Ukraine Cybersecurity for Critical Infrastructure Activity

Issuance Date:	September 8, 2021
Closing Date:	September 30, 2021
Closing Time:	Close of Business (17:30 Kyiv Time)

Subject: Request for Applications (RFA)
RFA-CSA-21-001
Community building and dialogue grant under the Community and Innovation program

Reference: Issued Under USAID Cybersecurity Critical Infrastructure Activity
Contract No. 72012120C00002

The USAID Cybersecurity Activity (2020-2024) is a program funded by USAID and implemented by DAI in coordination with six implementing partners from the US and Ukraine. The overall goal of the Activity is to reduce cybersecurity vulnerabilities in Critical Infrastructure (CI), and to transform Ukraine from a compromised, reactive cybersecurity actor to a proactive cybersecurity leader.

Ukraine's Cybersecurity system requires a single organizational platform working on behalf of all stakeholders to boost the cybersecurity industry of Ukraine; to work to develop and maintain an extensive national and international network of partners and collaborators in Business, Government, Academia, and Society for the benefit of Ukraine's cybersecurity sector.

This Notice of Funding Opportunity (NOFO) in the form of RFA solicits applications from qualified organizations for implementation of the Activity's Center for Cybersecurity Innovation (CCI) Community and Stakeholder Dialogue pillar. Specifically, this RFA targets established Ukrainian organizations capable of providing a platform to foster innovation and facilitate collaboration between government, business, academia, and a community of cybersecurity professionals to address the most pressing cybersecurity challenges. (See attached Program Description for a complete statement of goals and expected results).

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 (2 CFR 200 Subpart E for all US-based and for non-US based non-profit organizations, and the Federal Acquisition Regulation (FAR) Part 31 for for-profit organizations), 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 and the Standard Provisions for U.S. Nongovernmental Recipients will apply. See Annex 1 for Standard Provisions.

Subject to the availability of funds, DAI intends to award one grant or multiple grants, up to a maximum of $350,000. The expected duration of the grant (period of performance) is three years. DAI, as primary implementer of the USAID Cybersecurity Activity, reserves the right to fund any or none of the applications submitted.

This RFA consists of the following:

Section A – Grant Application Instructions
Section B – Special Grant Requirements
Section C – Selection Process
Section D – Program Description
Annexes

Applications must be received electronically via email**, no later than 22 days (September 30, 2021)** after the date of issuance indicated at the top of this cover letter at the place designated below for receipt of applications. Applications and modifications thereof shall be submitted in Microsoft Word or Excel and PDF to USAIDCybersecurity_Grants@DAI.com.

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

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.

Any questions concerning this RFA should be submitted in writing not later than 15 days prior to the closing date shown above to USAIDCybersecurity_Grants@DAI.com. Applicants should retain for their records one copy of all enclosures which accompany their application.

Thank you for your interest in the USAID Cybersecurity Activity.

Sincerely,

Tim Dubel
Chief of Party

Cybersecurity Center for Innovation

Table of Contents

Section A – Grant Application Instructions

1. Application Procedure

A. Completion and submission of applications

Eligibility Requirements

RFA applicants should meet the following eligibility criteria:

- Established non-government, not-for-profit organization
- Non-partisan
- More than 5 years of existence
- Experience managing multi-year, standard grants of over $150,000 (USD)
- Experience managing grants from international donors, preferably USAID
- Experience organizing large-scale, cross-sector and stakeholder dialogue and related events (forums, etc.)

Existing cybersecurity practice

Grants may not be awarded to:

Organizations excluded from federal procurement and non-procurement programs:

- Any entity whose name appears with an Active Exclusion on www.sam.gov;
- Any "Public International Organization" (PIO);
- Any entity affiliated with DAI Global LLC or any of its directors, officers, or employees.

Application Submission Requirements

- Applications must be submitted electronically to USAIDCybersecurity_Grants@DAI.com
- Applications must include :
  - Completed Application Form
  - Completed Grant Project Workplan (e.g. Gantt chart),
  - Projected Grant Budget and Budget Notes
  - CVs and BioData forms of all project team members
  - Completed Financial Capability Questionnaire and attachments
  - Statement of liability (part of application form)

Deadlines

Applications must be received at USAIDCybersecurity_Grants@DAI.com no later than September 30, 2021, as indicated in the cover letter. Applications and modifications thereof shall be submitted in Microsoft Word or Excel and PDF to USAIDCybersecurity_Grants@DAI.com.

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

Page Limitation: Applications should be specific, complete, presented concisely and shall not exceed 10 pages (exclusive of annexes).

Applications submitted in response to this RFA must include the following information:

1. Project Description: The purpose of this grant is to implement the community building and stakeholder dialogue pillar of CCI in an effort to foster innovation and facilitate collaboration between Government, Business, Academia, and professional Community to address the most pressing cybersecurity challenges.

2. Monitoring (Results and Benchmarks): The applicant should define, to the maximum extent possible at the application stage, results and benchmarks for monitoring the performance towards attainment of program objectives.

The following indicators shall be considered and projected while preparing an application under this RFA. Applicants are free to include the tools they will use to monitor project activities and evaluate project results:

- Number of events focused on supporting the building of a robust and developed cybersecurity community and relevant stakeholder dialogues
- Establishment of sub-group efforts with objectives related to building and sustaining cybersecurity innovation
- Development of partnerships to foster innovation in the cybersecurity sector

3. Sustainability: The applicant should describe how the project or its benefits will continue after grant funding ends. If this includes profitability, the application should specifically address its growth and marketing models and include projected revenue against expenses.

4. Personnel: The applicant should propose a limited number of key personnel who will be required to implement the work under this grant. This can be one or more persons who are full-time or contracted employees responsible for designing, implementing and/or managing key aspects of the grant project. Each applicant should provide detailed curriculum vitae or resumes that demonstrate the Key Personnel's ability to perform the duties outlined in the statement of work and in accordance with the evaluation factors found herein. DAI will evaluate the CV to determine the individual's knowledge, skills and abilities in the areas listed herein.

5. Organizational Capability: Each application shall include information that demonstrates the applicant's expertise and ability to meet or exceed the goals of this program.

6. Past Performance: Applicants should present any evidence of their past experience implementing grants for international donors, of work conducted under their cybersecurity practice, list of resource network, etc. A requirement for receiving grant funds is having managed grant agreements of a similar size and scope. Applicants should also list previous experience working with USAID or other international institutions on cybersecurity or related technical areas, should they possess it. Applicants may include descriptions of up to three (3) projects or other similar activities. However, this is not a requirement to receive funds. For each project, the entity should submit a reference up to a maximum of three (3) references, which should include: clients' names and telephone numbers who will serve as references.

7. Budget: All proposals must include a completed budget; see Section C for more details.

8. Cost Sharing Contribution: Details regarding the proposed cost sharing contribution by your organization must be included. Cost share is **not** a requirement for this RFA.

9. Other material: Applicants may also want to submit other material as attachments along with their applications such as letters of reference, newspaper clippings reporting on the organization's activities, brochures or other promotional material. However, attachments should be limited to 3 pages and they will not be returned to the applicants (exclusive of annexes).

C. Preparation Instructions – Financial and Administrative Documentation

1. **Completed Budget.** All budget lines must be clearly linked to specific project activities. Although DAI will support organization staff and operating costs that are necessary for reaching project goals, applicants should direct their resources primarily to project implementation, rather than organization operating costs. Supporting information shall be provided, as necessary, in sufficient detail to allow a complete analysis of each line item cost.

2. **Completed Financial Capability Questionnaire,** which includes:
    a. **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**
    c. **Organizational chart**

3. Documentation that the applicant has the ability to comply with the award conditions, taking into account all existing and currently prospective commitments of the applicant. The applicant must demonstrate its ability to segregate funds obtained from the award of a capital grant from other activities of the organization. A separate bank account is required should a grant award be made. (Documentation may include certification from the applicant's bank or a summary of previous awards, including type of funding, value, client, etc.)

4. Documentation that the applicant has a satisfactory record of integrity and business ethics. (Documentation may include references from other donors or clients and a summary of previous awards, including type of funding, value, client, etc.)

5. *Depending on size, type, and complexity of the grant, the following may also specifically be requested at this stage*:
    - *if applicable* – NICRA, or if no NICRA, the profit and loss statements which include detail of the total costs of goods and services sold, by information of the applicant's customary indirect cost allocation method, together with supporting computations of the basis for the indirect cost allocation method
    - cash flow, description of management structure, and/or oversight procedures, if available
    - copy of applicant's accounting manual
    - copy of applicant's operations manual
    - copy of purchasing policies and description of the applicant's purchasing system (for large grantees)

6. **Data Universal Numbering System (DUNS)** There is a mandatory requirement for the applicant to provide a DUNS number to DAI. The Data Universal Numbering System is

a system developed and regulated by Dun & Bradstreet (D&B) that assigns a unique numeric identifier, referred to as a "DUNS number" to a single business entity. Without a DUNS number, 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 DUNS number to DAI. Organizations who fail to provide a DUNS number will not receive an agreement and DAI will select an alternate awardee.

All U.S. and foreign organizations which receive a grant with a value of $25,000 and above **are required** to obtain a DUNS number prior to signing of the agreement. Organizations are exempt from this requirement if the gross income received from all sources in the previous tax year was under $300,000. DAI requires that grant applicants sign the self-certification statement if the applicant claims exemption for this reason.
For those required to obtain a DUNS number, see Annex 8- Instructions for Obtaining a DUNS Number - DAI'S Vendors, Subcontractors and Grantees.
For those not required to obtain a DUNS number, see Annex 9- Self Certification for Exemption from DUNS Requirement

B. Special Grant Requirements

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

Separate Account: The grantee must establish a separate account to house all funds provided under the grant, including all interest income.

Permitted Uses of Program Income: The Grantee must inform DAI of any program income generated under the grant and agrees to follow USAID's disposition requirements for such program income, in accordance with 2 CFR 200.307. 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 to support the Center for Cybersecurity Innovation, namely community building and stakeholder dialogue. 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 Agreement(s). The types of reporting required, along with the schedule of reporting, will depend on the grant type and project duration. Reporting forms will be provided to grant recipients. Types of reporting will include the following:

- **Project report** to be submitted during grant project implementation according to a schedule determined with DAI. This report will include a description of project activities and progress towards meeting the project goal; problems in project implementation; actions taken to overcome them; and plans on how the next phase of the project will be implemented.

- **Final project report** will describe how the project objectives and goals were reached, results of the project, and problems and solutions during implementation. This information should be presented in a manner suitable for presentation to the public.

- **Financial reports** will be submitted to DAI according to a schedule described in the grant agreement(s). Types of financial reports, as well as the schedule of reporting, will depend on the type of grant, length of project, and amount of grant funding. Financial reports will be required in order to receive grant installments. These reports will describe the amount of grant funds spent during the previous period, total amount spent to date, and amount remaining in each budget line item. In addition, all grant recipients are required to submit a detailed Final Financial Report.

Issuance of the final installment of grant funds is contingent upon DAI's receipt and acceptance of Final Financial and Final Program Reports.

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):
    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.

Other: As mentioned, subject to the availability of funds, a grant will be made available to an eligible organization for a value of up to $350,000 USD (all grants will be distributed in USD or local currency equivalent). Payment will be made according to a monthly or installment schedule, and in no event will more than 90% of the total agreed budget be disbursed prior to receiving and approving the Final Financial and Final Program Report.

C. Selection Process

Within 30 calendar days of the deadline for submitting applications, a review panel will convene. The review panel will include senior technical and operational representatives from DAI, and USAID, should they wish to participate. Applications will be evaluated on a rolling basis. Throughout the evaluation process, DAI shall take steps to ensure that members of the review

panel do not have any conflicts of interest or the appearance of such with regard to the organizations whose applicants are under review. An individual shall be considered to have the appearance of a conflict of interest if that person, or that person's spouse, partner, child, close friend or relative works for or is negotiating to work for or has a financial interest (including being an unpaid member of a Board of Directors) in any organization that submitted an application currently under the panel's review. Members of the panel shall neither solicit nor accept gratuities, favors, or anything of monetary value from parties to the awards.

All applications that meet the application requirements will be reviewed by the review panel. Verification of the application submission requirements will be conducted at the CCI Headquarters by the Director of Operations or other designated staff.

If suitable applications are received, an award will be made within approximately 45-180 days working days of the review panel meeting (or sooner) provided that the awardee (s) furnish (es) DAI with all the required documentation as itemized in Section A of this RFA and appropriate client approvals are also obtained, if necessary.

The applications will be evaluated according to the evaluation criteria set forth below. To the extent necessary (if 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 award. **Award will be made to responsible applicants whose applications offer the 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:

The following criteria should be adjusted as necessary to suit project needs.

1. Past performance and capability

- Is the applicant a recognized local organization with an established cybersecurity practice and vast network of relevant local stakeholders, including government, businesses, professionals, etc.

Very good = 30 points; good = 10 points; average = 5 points; poor = 0 points

2. Project justification and design

Is the design innovative, creative and realistic? Does the proposed staff have the experience for executing the activities included in the application? Can it reasonably be expected that the proposed technical approach will produce the expected results? Is the methodology for determining/measuring success of the grant sufficient, comprehensive, and clear?

Very good = 30 points; good = 15 points; average = 5 points; poor = 0 points

3. Cost effectiveness

Is the cost reasonable in terms of the expected results? The proposed costs make sense technically, which means that they are directly related to the proposed activity and that they are costs that are reasonable and necessary.

Very good = 10 points; good = 7 points; average = 5 points; poor = 0 points

4. Potential for sustainability

Does the implementer demonstrate how these activities will be sustained beyond the duration of the grant and their long-term impact?

Very good = 10 points; good = 7 points; average = 5 points; poor = 0 points

Signing of Grant Agreements

Upon USAID approval of the applicant, a Grant Agreement will be prepared. After DAI and the successful applicant have signed the Grant Agreement, DAI will provide training on financial management and reporting on grant funds. All reporting and contractual obligations will be explained to the grant recipients. Before receiving the first grant installment, ***all grant recipients must open a separate bank account*** as this is the only means by which grant funds will be transferred from DAI to the grant recipient.

D. Program Description

Background

The USAID Cybersecurity Activity is a program funded by USAID and implemented by DAI in coordination with six implementing partners from the US and Ukraine. The overall goal of the Activity is to reduce cybersecurity vulnerabilities in Critical Infrastructure (CI), and to transform Ukraine from a compromised, reactive cybersecurity actor to a proactive cybersecurity leader.

Through September 2024, the Activity will implement numerous programmatic initiatives designed to increase resilience and build capacity to prevent, detect, and respond to cyberattacks against critical infrastructure in Ukraine. To achieve this goal, the Activity is implementing the following components:

Component 1: Strengthening the cybersecurity enabling environment
This component will strengthen the cybersecurity resilience of Ukraine's CI sectors by addressing legislative gaps, promoting good governance, enabling collaboration between stakeholders, and supporting cybersecurity institutions. This component will also build the technical capacity of key sectors through increased access to cybersecurity technology and equipment.

Component 2: Developing Ukraine's cybersecurity workforce
This component of the Activity will address workforce gaps through interventions that develop new cybersecurity talent and build the capacity of existing talent. These interventions will address the entire workforce pipeline, the quality of education received by cybersecurity specialists, and industry training programs to rapidly upskill Ukraine's workforce to respond to immediate cybersecurity vulnerabilities.

Component 3: Building a resilient cybersecurity industry
A growing cybersecurity industry in Ukraine will contribute directly to national security and prosperity. This component will seek to build trust and collaboration between the public and private sectors to develop innovative solutions related to cybersecurity; spur investment and growth in the broader cybersecurity market in Ukraine through greater access to financing and market development efforts; support smaller cybersecurity companies to increase the number of local cybersecurity service providers; and offer mechanisms for Ukrainian firms to connect with industry partners to enable better access to innovations and business opportunities.

Increasing Ukraine's cybersecurity resilience requires integrated efforts across both the public and private sectors to generate and support innovative solutions and expertise needed to meet the demands of Ukraine's constantly evolving threat landscape. To achieve this, the Activity intends to launch a program currently entitled Center for Cybersecurity Innovation, otherwise known as CCI. The overall design of CCI includes multiple partners and is organized according to three pillars:

Cybersecurity Community Building and Stakeholder Dialogue	Visibility and Promotion of Ukrainian Cyber Solutions and Innovations	Supporting Cyber Innovations
Objective: community building and stakeholder dialogue to foster innovation and facilitate collaboration between government, business, academia, and the professional community to identify, explore and jointly address the most pressing cybersecurity challenges.	Objective: Increase visibility and opportunities for Ukrainian cyber solutions through internationalization and promotion of the industry and Ukraine as a trusted cybersecurity destination	Objective: Identify and support innovative cybersecurity innovations (concepts and research) and solutions (products, and services) from start-ups, service companies, researchers, independent teams, and others to address key cybersecurity challenges.
Outcomes: - A unified and proactive community of stakeholders contributing to improved cybersecurity - Tangible and sustainable initiatives to foster community and professional dialogue	Outcomes: - Increased opportunity for Ukrainian cybersecurity providers - Links to existing trade promotion and investment initiatives to highlight the cyber sector	Outcomes: - Greater coordination and mutual support across innovation stakeholders to identify and find solutions to cyber challenges - Viable (commercial or public sector) solutions to domestic and international application

Through these pillars, CCI will foster development of a multi-stakeholder community to identify priorities and champion needed reforms and partnerships, demonstrate that Ukraine is a viable and trusted partner in cybersecurity, and support an innovation environment and space for GOU stakeholders to engage with researchers, innovators, and other thought leaders to jointly address cybersecurity challenges and develop next generation cybersecurity solutions.

Specific to the first pillar, a priority is to engage multiple stakeholders with a perspective on cybersecurity – including the public and private sectors, academia, civil society, etc. Through this approach, the community is expected to self-organize, identify priorities, and form specific approaches to address those priorities. The Activity will support this community building effort.

Objective

This RFA solicits applications from qualified organizations for implementation of the CCI Community and Stakeholder Dialogue pillar. Specifically, this RFA targets established Ukrainian organizations with a focus on multi-stakeholder engagement and development of programs, reform initiatives, and policies through a proven approach to community development through dialogue. Interested organizations should be capable of providing a platform to foster such a dialogue and build community between government, business, academia, and a community of cybersecurity professionals to address the most pressing cybersecurity challenges.

Responsibilities/tasks:

The selected organization will be tasked with the following:

- Providing a platform for community building and stakeholder dialogue:
    - Identifying and connecting leaders of the emerging Ukrainian cybersecurity community across different stakeholders and sectors
    - Establishing and launching a mechanism/platform for regular discussions on cybersecurity challenges and for turning cybersecurity issues into opportunities, through concrete action.
- Creating a membership/community of regular participants in dialogue
- Planning and holding high-level, multi-stakeholder events, including seminars, conferences, roundtable discussions, etc.
- Sustaining the platform and activities beyond the period of performance of the grant.

The organization must have the resources to perform the above requirements, including having an established cybersecurity practice, qualified staff, and a vast network in order to attract participation in the above listed activities.

Expected Benchmarks, Milestones, and Outcomes:

Key anticipated approaches include the following:

A planned program of events and initiatives to build community, including:

- Facilitated multi-stakeholder events, including a clear agenda, productive engagement methodologies (exercises, expert speakers, etc), and specific outcomes and defined follow up actions
- Additional events to highlight specific issues, engage the community in a more tailored way, etc. These may include roundtables on key policy issues, technical solutions, etc.

Engaging key constituents:

- Support for self-organization of sub-groups, including cybersecurity professionals, or individuals with an interest or expertise in specific technical areas
- A methodology for ensuring that key constituent groups, in particular the public sector, and fully engaged and acting on initiatives proposed through community dialogue, such as policy changes, a reform action plan, etc.
- Specific and results oriented engagements with key partner organizations, including for example, business associations, policy groups (think tanks), etc.. These could include partnership agreements, joint events, etc.

The expected timeline and outcomes include:

Year 1:

- A final strategic program plan, including events and initiatives over a three-year period, with clearly defined outcomes
- A strategic communications plan in support of the above strategic program plan
- At least two major multi-stakeholder community building events
- A minimum of five supporting events, including, for example roundtables, policy discussions, guest speaker lectures, etc.

- A report of key inputs and outcomes of the strategic program plan

Years 2 and 3:

- For each year, a program of events (major and supporting) in support of the strategic program plan, as sell as supporting communication efforts
- Defined engagements with partner organizations
- Annual reports on the inputs and outcomes of the strategic program plan and communications efforts
- A final report indicating achievements in the area of community building and stakeholder dialogue, with a proposed action plan for sustainability and ongoing impact

Annex 1: Mandatory Standard Provisions

Standard Mandatory Provisions for Non-US, Non-Government Recipients
and Required as Standard Provisions Applicable to Non-US, Non-Government Recipients,
http://www.usaid.gov/policy/ads/300/303mab.pdf

ADS 303, http://www.usaid.gov/policy/ads/300/303.pdf

OMB Circular 122 "Cost Principles for Non-Profit Organizations,"
http://www.whitehouse.gov/omb/circulars/a122/a122.html

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, as applicable:

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.)

Annex 3: Application Form

Annex 3

A P P L I C A T I O N F O R M

I. THE APPLICANT

1. Name of applicant

(please include also acronyms, if any)

2. Address of applicant

(please include official address as well as postal address)

Official address:

Postal address:

3. VAT registration number

(if applicable)

4. Telephone

5. E-mail

6. Web site

7. Contact person

II. PROJECT INFORMATION

1. Title of proposed project

2. Location and duration

Location:

Duration: _____ months, from [month] 2021 to [month] [year]

3. Summary Budget

Total budget	(local currency)	(100%)
▪ Amount requested	(local currency)	(%)
▪ Applicant contribution	(local currency)	(0%)
▪ *Exchange rate used*	*1 USD = local currency*	*(date)*

III. PROJECT DESCRIPTION

1. Project summary

(Please provide a brief summary of your proposed project and necessary information on how grant funds will be used to advance the goal of fostering innovation through facilitated collaboration between Government, Business, Academia, and professional Community to address the most pressing cybersecurity challenges.
The summary must be no more than 2 pages and should clearly address what your project will accomplish related to this RFA. The applicant should also explain why and how the project will be implemented and demonstrate what phases of the company business plan or business model are associated with the specific grant funds used to implement this project.)

2. Project goal, activities and results

(All activities under grant should be described. For example, number of events, why that number is deemed necessary, specific examples of participants/target audience, purpose and intended outcome of event, how it is different from other types of events.)

a) What are the specific activities that you will undertake using these grant funds? What is the purpose of each and how does each tie to the goal of this grant project? How will you carry them out?

b) What are the specific expected results that your project will bring about?

3. Monitoring and evaluation

a) How will you know that your project was successfully implemented? What criteria will you use to measure the achievements of your project?
(Please include the tools you will use to monitor project activities and evaluate project results)

4. Sustainability

a) Describe how the activities in your project will be sustained after funding ends. How will the activities or results of your project continue?

5. Project activity schedule and timeline (work plan)

(Based on the activities listed in section III.2(b) above, please fill in the work plan using the template provided in Annex 4)

IV. PROJECT TEAM

Please list all project team members, including their position, role in the project, level of effort, and a short description of their assigned responsibilities. *(Insert as many lines as necessary).*

(Please attach CVs for key personnel involved in the project, using the template provided in Annex 6; also include a 1420 BioData Form to be filled out by all key personnel)

NO	NAME & SURNAME	POSITION	ROLE IN THE PROJECT	DESCRIPTION
1				
2				
3				
4				
5				
6				
7				
8				

V. APPLICANT CAPABILITY AND PAST PERFORMANCE

1. Organizational capability and resources

Annual income over the past three years, mentioning the names of your main financial contributors (where applicable)

YEAR	TOTAL ANNUAL INCOME (in USD)	MAIN FINANCIAL CONTRIBUTORS* If revenue, provide the category of revenue source (e.g. individual customers, enterprise companies, consulting, etc.)

a) Please describe the various resources at the disposal of your organization such as: equipment, offices etc.

2. Past performance

Please describe no more than three major projects in which your organization was involved over the past three years, using the table below.

a) Project title	
b) Duration (months)	
c) Year	
d) Location	
e) Role of your organization *(leader, partner)*	
f) Project objectives	

g) Project results	
h) Total budget (USD)	
i) Funding sources and types of funding (grants, contract, or other) *Please include contact information for funding sources.*	

VI. PROJECT BUDGET

Please provide a detailed budget for the entire duration of the project, using the template provided in Annex 5 as an example.

VII. STATEMENT OF LIABILITY

I, the undersigned, being the person responsible in the applicant organization for this project, certify that the information given in this application is true and accurate.

Name and surname:	
Position:	
Signature:	
Date and Place:	

Annex 4: Workplan

ANNEX 4

Name of applicant:

#	Objective	Activities	Expected result (output)	Location	Responsible person	Timeline (months)											
						1	2	3	4	5	6	7	8	9	10	11	12

Annex 5: Budget

See attached Excel.

Annex 6: BioData Form

CONTRACTOR EMPLOYEE BIOGRAPHICAL DATA SHEET

The Privacy Act Statement is found at the end of this form.

1. Name *(Last, First, Middle)*		2. Contractor's Name	
3. Employee's Address *(include ZIP code)*		4. Contract Number	5. Position Under Contract
		6. Proposed Salary	7. Duration of Assignment
8. Telephone Number *(include area code)*	9. Place of Birth	10. Citizenship (*If non-U.S. citizen, give visa status)*	

11. Names, Ages, and Relationship of Dependents to Accompany Individual to Country of Assignment

12. EDUCATION *(include all college or university degrees)*

NAME AND LOCATION OF INSTITUTION	MAJOR	DEGREE	DATE

13. LANGUAGE PROFICIENCY *(see Instruction on Page 2)*

LANGUAGE	Proficiency Speaking	Proficiency Reading

14. EMPLOYMENT HISTORY *(List last three (3) positions held by the individual)*

POSITION TITLE	EMPLOYER'S NAME AND ADDRESS POINT OF CONTACT &TELEPHONE #	Dates of Employment *(M/D/Y)*	
		From	To

15. SPECIFIC CONSULTANT SERVICES *(give last three (3) years). Continue on a separate sheet of paper, if required, to provide this information.*

SERVICES PERFORMED	EMPLOYER'S NAME AND ADDRESS POINT OF CONTACT	Dates of Employment *(M/D/Y)*	
		From	To

16. RATIONALE FOR PROPOSED SALARY *(Provide the basis for the salary proposed in Block 6 with supporting rationale for the market value of the position. Continue on a separate sheet of paper, if required) Salary definition – basic periodic payment for services rendered. Exclude bonuses,* profit-sharing arrangements, commissions, consultant fees, extra or overtime work payments, overseas differential or quarters, cost of living or dependent education allowances.

17. CERTIFICATION: To the best of my knowledge, the above facts as stated are true and correct.

Signature of Employee	Date

18. CONTRACTOR'S CERTIFICATION *(To be signed by responsible representative of Contractor)*

Contractor certifies in submitting this form that it has taken reasonable steps (in accordance with sound business practices) to verify the information in this form. Contractor understands that USAID may rely on the accuracy of such information in negotiating and reimbursing personnel under this contract. Certifications that are false, fictitious, or fraudulent, or that are based on inadequately verified information, may result in appropriate remedial action by USAID, taking into consideration all the pertinent facts and circumstances, ranging from refund claims to criminal prosecution.

Signature of Contractor's Representative	Date

Annex 7: Financial Capability Questionnaire

Annex 7

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 proposal. 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 '?

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: ☐

3. 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 (2 CFR 200 Subpart E "Cost Principles")?

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 8: Instructions for Obtaining a DUNS Number - DAI'S Vendors, Subcontractors and Grantees

There is a mandatory requirement for the applicant to provide a DUNS number to DAI. The Data Universal Numbering System is a system developed and regulated by Dun & Bradstreet (D&B) that assigns a unique numeric identifier, referred to as a "DUNS number" to a single business entity. Without a DUNS number, 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 APS is contingent upon the winner providing a DUNS number to DAI. Organizations who fail to provide a DUNS number will not receive an agreement and DAI will select an alternate awardee.

All U.S. and foreign organizations which receive a grant with a value of $25,000 and above are required to obtain a DUNS number prior to signing of the agreement.

Organizations are exempt from this requirement if the gross income received from all sources in the previous tax year was under $300,000. DAI requires that grant applicants sign the self-certification statement if the applicant claims exemption for this reason. Documentation with Instructions for Obtaining a DUNS Number or a Self Certification for Exemption from the DUNS Requirement can be obtained from the project issuing this APS.

Annex 9: Self Certification for Exemption from DUNS Requirement

Self-Certification for Exemption from DUNS Requirement

Legal Business Name:

Physical Address:

City:

Country:

Signature of Certifier:

Full Name of Certifier (First, Middle, Last):

Title:

Date of Certification:

The applicant/sub-award recipient whose legal business name is provided herein, certifies thatwe are an organization exempt from obtaining a DUNS number, as the gross income received from all sources in the previous tax year is under USD $300,000.

*By submitting this certification, the certifier attests to the accuracy of the representations and certifications contained herein. The certifier understands that s/he and/or the applicant/sub-award recipient may be subject to penalties, if s/he misrepresents the applicant/sub-award recipient in any of the representations or certifications to the Prime Contractor and/or the US Government.

The applicant/sub-award recipient agrees to allow the Prime Contractor and/or the US Government to verify the company name, physical address, or other information provided herein. Certification validity is for one year from the date of certification.

Annex 10: Application Checklist

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

- ☐ The application is submitted by email
- ☐ Applicable certifications and assurances are signed and included (see Annex 2)
- ☐ *If applicable*: The workplan is included (Annex 4)
- ☐ Budget is included
- ☐ The CVs and BioData Forms are included (Annex 6)
- ☐ The statement of liability is signed and stamped (last page of application form – Annex 3)
- ☐ Completed Financial Capability Questionnaire (Annex 7)
- ☐ 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.)
- ☐ Incorporation Papers or Certificate of Registration and Statute
- ☐ Organizational Chart
- ☐ Documentation that the applicant has the ability to comply with the award conditions, taking into account all existing and currently prospective commitments of the applicant. The applicant must demonstrate its ability to segregate funds obtained from the award of a capital grant from other activities of the organization. A separate bank account is required should a grant award be made. (Documentation may include certification from the applicant's bank or a summary of previous awards, including type of funding, value, client, etc.)
- ☐ Documentation that the applicant has a satisfactory record of integrity and business ethics. (Documentation may include references from other donors or clients and a summary of previous awards, including type of funding, value, client, etc..)
- ☐ Evidence of a DUNS Number or a Self-Certification for Exemption from DUNS Requirement (Annex 8 and 9).