Annual Program Statement (APS)

USAID Cybersecurity for Critical Infrastructure in Ukraine Activity

APS-CCI-003
Cybersecurity Enabling Environment Program

Issue Date: March 20, 2024
Final Closing Date: December 31, 2024
Questions Due By: on a rolling basis
Deadline for Submission: on a rolling basis
Submit Applications to: USAIDCybersecurity_Grants@dai.com
APS Reference No.: APS-CCI-003

To Interested Applicants:

The purpose of this Annual Program Statement (APS) is to solicit funding applications. The USAID Cybersecurity for Critical Infrastructure in Ukraine Activity (hereinafter referred to as "USAID Cybersecurity Activity" or "Activity"), implemented by DAI Global LLC ("DAI"), is seeking applications to propose creative and effective initiatives and solutions to strengthen the national preparedness, cybersecurity vulnerabilities and critical infrastructure (CI) of Ukraine in the cybersecurity sector. Conclusively, the APS process enables partners to propose partner-driven and sustainable solutions.

Under this APS, the Activity is awarding grants which will focus on achieving one or more of the following objectives:

1. **Component 1: Strengthen the Cybersecurity Enabling Environment** to create a safe and trusted environment to accelerate the development of people, processes, and technology in support of cybersecurity across critical infrastructure sectors and assets in Ukraine and
2. **Component 2: Develop Ukraine's Cybersecurity Workforce** to strengthen Ukraine as a sovereign nation built on a secure, protected, and dynamic economy supported by a talented pool of human capital and
3. **Component 3: Build a Resilient Cybersecurity Industry** to stimulate demand for and supply Ukrainian cybersecurity solutions and service providers to empower, equip, and finance cybersecurity entrepreneurs and businesses.

The grants will be awarded and implemented in accordance with the U.S. Agency for International Development (USAID) and U.S. Government grants under contract regulations, as well as the Activity's internal grants management policies and procedures.

Applications outside the geographic focus will not be considered. Applicants must demonstrate success in managing cultural and political considerations in the proposed focus country or region and in addressing the abovementioned development objectives.

The application process will consist of one (1) stage:

- Applicants shall submit an application package consisting of Annex A: Technical Approach Application, Annex B: Budget, and Annex C: Representations and Assurances as stated below in Section IV.
- Applicants shall prove eligibility based on the criteria detailed in Section III.
- Application evaluation is a competitive process. Received applications will be reviewed and evaluated based on the selection criteria in Section V.

Documents Required for Application Submission:

Applicants shall submit the following documents. Applications will be reviewed on a rolling basis.

1. **Annex A** – Technical Approach
2. **Annex B** – Detailed Budget Form
3. **Annex C** – Representations and Assurances:
    - Representation by a Corporation Regarding a Delinquent Tax Liability or a Felony Criminal Conviction (per AAPD 14-03)
    - Prohibition on Providing Federal Assistance to Entities that Require Certain Internal Confidentiality Agreements – Representation (May 2017)
4. **Certificate of Registration** with the Government of Ukraine

SECTION I – PROGRAM DESCRIPTION

The Annual Program Statement (APS) is developed to engage academia, science, and private sector players to enhance Ukraine's cyber resilience and describes the process for identifying, selecting, and awarding funds to partners.

The Annual Program Statement is soliciting applications from private, science, NGO, or academic players that target to strengthen the national cybersecurity system, build the capacity of the Government of Ukraine (GOU) entities in the area of cybersecurity, and ensure secure operations of operators of critical infrastructure (OCIs). Specifically, these applications should prioritize the following initiatives:

- addressing identified legislative gaps on the national level as well as sectoral ones e.g., public-private partnership, cyber insurance, risk assessment,
- suggested capacity building programs for GOU cybersecurity stakeholders and OCIs,
- strengthening collaboration between Ukrainian and international cybersecurity stakeholders,
- adopting best international practices in cybersecurity
- ad hoc surveys in cybersecurity, including secure by design, zero trust, etc.

1.1 PROGRAM OBJECTIVE

The overall goal of the APS is to reduce and potentially eliminate cybersecurity legislative gaps, to achieve convergence of Ukrainian and international approaches in the field of cybersecurity, and to promote European integration aspirations.

The objectives of the program are:

- strengthen cyber resilience through legislation development,
- implement international best practices in the area of cybersecurity,
- create legislative preconditions for the effective public-private partnership development in the field of cybersecurity
- strengthen collaboration between Ukrainian and International cybersecurity stakeholders.

1.2 ADMINISTRATION OF AWARD

Funding awarded under the APS is authorized pursuant to the Foreign Assistance Act of 1961 as amended and is subject to 2 CFR 700 and 2 CFR 200 – Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards.

Applicants may obtain copies of the referenced material at the following websites:

- 2 CFR 200: http://www.ecfr.gov/cgi-bin/text-idx?SID=0a5b7fee6378930cce72564449dd8bb7&mc=true&node=sp2.1.200.d&rgn=div6
- 2 CFR 700: https://www.ecfr.gov/current/title-2/subtitle-B/chapter-VII/part-700
- Standard Provisions for Non-U.S., Nongovernmental Recipients: https://www.usaid.gov/about-us/agency-policy/series-300/references-chapter/303mab

SECTION II – AWARD INFORMATION

Estimated Funding Level

DAI anticipates awarding grants for up to one year on a rolling basis. Grants are negotiated and awarded in U.S. dollars (USD) but will be paid in Ukrainian Hryvnias (UAH) at the exchange rate applicable and used by the program's financial accounting system when processing the payment. Grant awards will generally range from the UAH equivalent of USD 20,000 to 150,000. DAI expects to award multiple grants and may choose to fund the selected application(s) fully or incrementally. There is no limit on the number of applications an applicant may submit. Issuance of this APS in no way obligates DAI to award any grants, and applicants will not be reimbursed for any costs associated with preparing their applications.

Anticipated Start Date of Grants Award: April 2024

Period of Performance: The start date will be upon award, and the performance period will be up to one year.

Award Type:

Based on the evaluation results, the Activity will determine the value, duration, and type of grant based on the nature of the proposed concept note/grant activity and the applicant's financial and management capacity.

SECTION III – ELIGIBILITY INFORMATION

3.1 TYPES OF ENTITIES THAT MAY APPLY

Applicants must be a registered Ukrainian for-profit, not for-profit non-governmental organization (NGOs), business/trade association, think tank, and/or private enterprise formally registered, constituted, and recognized by and in good standing with appropriate Ukrainian governmental authorities and laws of Ukraine, and compliant with all applicable civil and fiscal regulations.

This APS is issued as a public notice to ensure that all interested and eligible organizations have a fair opportunity to submit funding applications. Eligible organizations could include foundations, non-governmental organizations (NGOs), private organizations affiliated with public academic institutions and international non-governmental organizations, higher educational institutions, private companies, or professional associations. Please note, for-profit organizations willing to forego profit may apply however restrictions on costs paid under grants to profit-making organizations apply – see section 3.3 "Ineligible Activities and Unallowable Costs".

Cost share is not required for eligibility purposes. Applicants are encouraged to contribute resources from their own private or local sources to implement this program where feasible.

3.2 ADDITIONAL ELIGIBILITY REQUIREMENTS

- As mentioned above in section 3.1, local organizations must be legally registered in accordance with the laws of the Government of Ukraine.
- Applicants must display sound management in the form of financial, administrative, and technical policies and procedures and present a system of internal controls that safeguard assets, protect against fraud, waste, and abuse; and support the achievement of program goals and objectives. The Activity will assess this capability prior to awarding a grant.
- Must support outcomes and results consistent with and linked to the Activity's objectives stated above.
- Applicants must sign the required certifications as part of their application package in response to this APS found in Annex C: Representations and Assurances to be considered acceptable applications.
- All domestic and foreign organizations receiving first-tier subcontracts/ purchase orders with a value of $30,000 and above are required to obtain a Unique Entity ID (SAM) before signing the agreement. All foreign entities receiving first-tier monetary grants (standard, simplified and FAAs) with a value equal to or over $25,000 and performing work outside the U.S. must obtain a Unique Entity ID (SAM) prior to signing the grant. All U.S. organizations receiving first-tier monetary grants of any value are required to obtain a Unique Entity ID (SAM); the exemption for under $25,000 applies to foreign organizations only. *(«Instructions for Obtaining a Unique Entity ID (SAM) for DAI`s Vendors, Subcontractors & Grantees» will provided to the successful applicants).*
- The Activity will work with the successful grantee to draft a marking and branding plan which will be annexed to the grant agreement.

3.3 INELIGIBLE ENTITIES AND UNALLOWABLE COSTS

The USAID Cybersecurity Activity will not award grants to the following entities:

- Any governmental and state-owned enterprises (SOE).
- Organizations from foreign policy restricted countries (Cuba, Iran, North Korea, Sudan and Syria);
- Any U.S. entity which is a "Private Voluntary Organization" (PVO) but has not registered as such with USAID.
- Any "Public International Organization" (PIO).
- Organizations who have active exclusives in SAM (sam.gov). In addition, organizations are not eligible for awards if they have members who appear in the U.S. Department of Treasury's List of Specially Designated Nationals (OFAC's Sanctions List) and Blocked Persons or who have been designated by the United Nations Security (UNSC) sanctions committee established under UNSC Resolution 1267 (1999) (the 1267 Committee) as an individual or organization linked to terrorism.
- Any entity affiliated with DAI and DAI subcontractors or any of its directors, officers, or employees.

Unallowable costs are further described in Subpart E – Cost Principles in 2 CFR 200 for non-profit organizations and FAR 31.2 "Cost principles for Commercial Organizations" for for-profit organizations. All costs must be reasonable, allocable, and allowable. Grant funds cannot be used for the following:

- Private ceremonies, parties, celebrations, or "representation" expenses.
- Purchases of restricted goods, such as certain agricultural commodities, motor vehicles (including motorcycles), pharmaceuticals and contraceptive items, pesticides, used equipment, U.S. Government excess property and fertilizers without the previous approval by the USAID CO.
- Prohibited goods under USAID regulations include but are not limited to military and surveillance equipment, police or law enforcement equipment, abortion equipment and services, weather modification equipment, luxury goods, and gambling equipment.
- Purchases of goods or services restricted or prohibited under the prevailing USAID source/nationality regulations per 22 CFR 228 and relevant Standard Provisions; or from countries or suppliers as may be identified by USAID's consolidated list of debarred, suspended, or ineligible subcontractors at https://sam.gov/content/home.

- Any purchases or activities deemed unnecessary to accomplish grant purposes as determined by DAI, including any grantee headquarters' expenses that are not directly linked to the implementation of the proposed program.
- Previous obligations and/or bad debts.
- Fines and/or penalties.
- Creation of endowments.
- Other costs unallowable under USAID and/or federal regulations, such as alcoholic beverages.
- Indirect costs such as but not limited to overhead or indirect fringe (unless the applicant has documented proof of such rates through audits or USAID-issued NICRA).

The USAID Cybersecurity Activity highly encourages applications from new organizations who meet the above eligibility criteria.

SECTION IV – APPLICATION AND SUBMISSION INFORMATION

The USAID Cybersecurity Activity will review proposals using a single-stage process.

SUBMISSION OF GRANT APPLICATION

All applicants are required to submit an application package consisting of four parts that is specific and complete. The four-part application includes:

(1) Detailed technical approach application (Annex A).
(2) Detailed budget breakdown with a proposed deliverables schedule (Annex B) which must be supported by budget backup documentation for cost realism.
(3) Signed Representations and Assurances (Annex C).
(4) A copy of your 'Certificate of Registration' with the Government of Ukraine.

Format of Application Submission

The chart below summarizes the format required for each portion of the application in order for it be considered complete:

What to Submit	Required Content	Required
1. Technical Approach Application	The narrative format is based on the application forms' sections I-VI and their respective guidance. Sections should address the program description and selected program objectives, detailed activities, anticipated projected results, how the work will help accomplish DAI's program goals, project activity schedule/timeline (workplan), and proposed personnel.	Word (see Annex A)
2. Detailed Budget • Budget Excel File (template provided) • Supporting Documentation	Applicant shall complete: - Excel budget table based off template provided; feel free to modify/tailor it to your technical approach. - Deliverables Schedule - Budget support documentation for the costs proposed in your budget	Excel (see Annex B)

3. Representations and Assurances, Other Statements of the Recipient and Solicitation Standard Provisions	See Annex C for more details – these forms need to be read and signed.	Signed (digitally or with ink) PDF copy
4. Certificate of Registration with the Government of Ukraine	A digital copy of your current registration status with the Government of Ukraine.	PDF copy

Review and Notification
Applications are reviewed on a rolling basis. The Activity will evaluate the application within 30 days of receipt.

Applicants will be notified if:

a. They are successful, and the Activity will host communications to provide additional guidance on the next steps or
b. They are rejected, or
c. The application was not aligned with or eligible for funding.

Final Determination

All applicants are subject to a pre-award financial and management review before final approval and award of grant funding. The Activity team will review an application to determine the final applicants selected for funding. If selected, the Activity team may decide to fund all or part of the application.

Submission Instructions

Applicants must submit full applications (with all the supportive documents) to: USAIDCybersecurity_Grants@dai.com in English. Please use **email subject** format as follows: Response to APS-CCI-003 – [Insert your Organization's Name]

OTHER IMPORTANT INFORMATION

Branding and Marking

All USAID-sponsored assistance awards are required to adhere to branding policies and revised marking requirements for grants and cooperative agreements in accordance with ADS 320. This includes visibly displaying the USAID Standard Graphic Identity that clearly communicates assistance is, "From the American people" on all programs, projects, activities, publications, public communications, and commodities provided or supported through USAID assistance awards. ADS 320 requires that included in the grant is a branding strategy that describes how the program, project, or activity is named and positioned, how it is promoted and communicated to beneficiaries and cooperating country citizens and identifies all donors and explains how they will be acknowledged. Activity will provide a template branding strategy that will be adapted in consultation with the applicant. ADS 320 may be found at the following website: https://www.usaid.gov/about-us/agency-policy/series-300/320.

Environmental Procedures

1. The Foreign Assistance Act of 1961, as amended, Section 117 requires that the impact of USAID's activities on the environment be considered and that USAID include environmental sustainability as a central consideration in designing and carrying out its development programs. This mandate is codified in Federal Regulations (22 CFR 216) and in USAID's Automated Directives System (ADS) Parts 201.5.10g and 204 (https://www.usaid.gov/about-us/agency-policy/series-200/204), which, in part, require that the potential environmental impacts of USAID-financed activities are identified prior to a final decision to proceed and that appropriate environmental safeguards are adopted for all activities. i.e.: environmental

compliance obligations under these regulations and procedures are specified in the following paragraphs of this APS.
2. In addition, the contractor/recipient must comply with host country environmental regulations unless otherwise directed in writing by USAID. In case of conflict between host country and USAID regulations, the latter will govern.
3. No activity funded under this grant will be implemented unless an environmental threshold determination, as defined by 22 CFR 216, has been reached for that activity, as documented in a Request for Categorical Exclusion (RCE), Initial Environmental Examination (IEE), or Environmental Assessment (EA) duly signed by the Bureau Environmental Officer (BEO). (Hereinafter, such documents are described as "approved Regulation 216 environmental documentation.")

Unique Entity ID (SAM)

The unique entity ID (SAM) requirement is already mentioned under **3.2 Additional Eligibility Requirements.**
The applicant shall be informed that the Unique Entity ID number submission is not required as part of the application process but, if required, will need to be provided before Activity will sign a grant agreement. Please notify the Activity if you have any problems applying for or receiving the Unique Entity ID number via email at USAIDCybersecurity_Grants@dai.com.

Certifications, Assurances, Other Statements of the Recipient and Solicitation Standard Provisions

Awards to U.S. organizations will be administered in accordance with 2 CFR 200 Subpart E, ADS 303 and USAID Standard Provisions for U.S. non-governmental organizations. For non-U.S. organizations, USAID Standard Provisions for non-U.S. non-governmental organizations would apply. See Annex C: Representations and Assurances.

SECTION V – APPLICATION REVIEW INFORMATION

5.1 APPLICATION REVIEW CRITERIA

Applications will be reviewed in terms of responsiveness to the APS, appropriateness of subject matter, and creativeness. Applicants are encouraged to demonstrate how their proposed work will contribute to the USAID Cybersecurity Activity goals.

#	Merit Review Category	Rating (Points)
1	**Relevance to GOU and CIOs needs (30%)** 1.1 Benefits are clearly elaborated to the GOU stakeholders and Critical Infrastructure Operators (CIOs) in the technical approach.	30
2	**Addressing critical challenges (20%)** 2.1. Strategy for how the suggested technical application will address current challenges the GOU stakeholders and Critical Infrastructure Operators (CIOs) face.	20
3	**Strength of technical approach and responsiveness to APS objectives (30%)** 3.1. Alignment with and contribution towards APS objectives. 3.2. Details of the proposed approach.	30

4	**Management & Institutional Capacity (20%)** 4.1. Demonstrated institutional capacity (technical, administrative, and financial). 4.2. Demonstrated experience in the relevant industry. 4.3. Past performance managing interventions of similar scope, complexity, and size. 4.4. Demonstrated long-term experience by key staff in capabilities where appropriate.	20
	Overall Rating (out of 100 points)	**100**

SECTION VI – AWARD AND ADMINISTRATION INFORMATION

Competition for this APS will be open for one year. At the discretion of Activity, applications received will be evaluated on a rolling basis through the duration of the year.

All grants will be negotiated in U.S. dollars (USD); however, payments will be issued in **Ukrainian hryvnia** (UAH) paid at the national bank's exchange rate on the date of payment**.** All costs funded by the grant must be allowable, allocable, and reasonable. Grant applications must be supported by a detailed and realistic budget.

Issuance of this APS and assistance with application development do not constitute an award or commitment on the part of the USAID Cybersecurity Activity, nor does it commit the USAID Cybersecurity Activity to pay for costs incurred in the preparation and submission of an application. Further, USAID Cybersecurity Activity reserves the right to accept or reject any or all applications received and reserves the right to ask further clarifications from the applicants. Applicants will be informed in writing of the decision made regarding their application.

(1) Post- Selection Information

Following selection of an awardee, as stated in Section IV: Application and Submission Information, DAI will inform the successful applicant by email and notify unsuccessful applicants concerning their status.

(2) General Information on Reporting Requirements

Program implementation reporting will be determined based on the outcome of the collaborative finalization of the planned program and the delineation of roles and responsibilities. An annual performance monitoring and evaluation plan will also be agreed upon using established baseline data and specific, measurable targets and indicators. Financial reporting will be in accordance with the requirements of the grant agreement.

SECTION VII – DAI CONTACTS

The point of contact for grant-related questions is: USAIDCybersecurity_Grants@dai.com.

Any prospective applicant desiring an explanation or interpretation of this APS must request it in writing and will be reviewed and answered on the rolling basis. Oral explanations or instructions given before award of a grant will not be binding. Any information given to a prospective applicant concerning this APS will be furnished promptly to all other prospective applicants as an amendment of this APS, if that information is necessary in submitting applications or if the lack of it would be prejudicial to any other prospective applicants.

SECTION VIII - OTHER INFORMATION

Issuance of this APS does not constitute an award or commitment on the part of DAI, nor does it commit DAI to pay for costs incurred in the preparation and submission of an application.

DAI reserves the right to fund any or none of the applications submitted. Further, DAI reserves the right to make no awards as a result of this APS.

LIST OF ANNEXES (attached/included in separate files):

Annex A. Technical Approach Application Form
Annex B. Detailed Budget Form
Annex C. Representations and Assurances

Annex A. Technical Approach Application Form

See attached Word file. Detailed instructions are included in each section of the application form.

Annex B. Detailed Budget Form

See attached Excel file. Edit at your convenience according to your proposed grant project.

Annex C. Representations and Assurances

Applicants may obtain copies of the referenced material at the following websites:

- 2 CFR 200: http://www.ecfr.gov/cgi-bin/text-idx?SID=0a5b7fee6378930cce72564449dd8bb7&mc=true&node=sp2.1.200.d&rgn=div6
- 2 CFR 700: https://www.ecfr.gov/current/title-2/subtitle-B/chapter-VII/part-700
- Standard Provisions for Non-U.S., Nongovernmental Recipients: https://www.usaid.gov/about-us/agency-policy/series-300/references-chapter/303mab
- Certifications, Assurances, Representations, and Other Statements of the Recipient - https://www.usaid.gov/about-us/agency-policy/series-300/references-chapter/303mav

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:

Part I – Certifications and Assurances

- Assurance of Compliance with Laws and Regulations Governing Non-Discrimination in Federally Assisted Programs.
- Certification Regarding Lobbying.
- Certification Regarding Terrorist Financing, Implementing Executive Order 13224.
- Certification of Recipient.

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 (***Annex C of this APS***)

Part V – Prohibition on Providing Federal Assistance to Entities that Require Certain Internal Confidentiality Agreements – Representation (May 2017) (***Annex C of this APS***)