



Shaping a more livable world.

Issuance Date: January 3, 2024
Closing Date: February 16, 2024
Closing Time: Close of Business (18:00 Kyiv Time)

Subject: Reissue of Request for Applications (RFA) RFA-CCI-002
Cyber Vouchers Administration Grant Program

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

To Interested Applicants:

The USAID Cybersecurity for Critical Infrastructure in Ukraine Activity (hereinafter referred to as “USAID Cybersecurity Activity” or “Activity”) under this Request for Applications (RFA), is seeking applications for funding highly experienced organization which will administrate Cyber Voucher Program developed by the Activity with the goal to stimulate the development of the cyber security market in Ukraine.

The USAID Cybersecurity for Critical Infrastructure in Ukraine Activity, implemented by DAI Global LLC, is designed to reduce cybersecurity vulnerabilities in critical infrastructure (CI) sectors and transform Ukraine from a compromised, reactive cybersecurity actor to a proactive cybersecurity leader. Recognizing the complexity of the threat posed by Russian hybrid warfare, the Activity has adopted a multi-sector approach that engages government, businesses, and academia to improve Ukraine’s cybersecurity for CI. Through three strategic objectives, the Activity is improving the enabling environment for cybersecurity, strengthening Ukraine’s cybersecurity workforce, and stimulating market development to promote Ukrainian cybersecurity products and services.

The USAID Cybersecurity for Critical Infrastructure in Ukraine Activity is planning to launch a Cyber Voucher Program in 2024 to stimulate the development of the cybersecurity market in Ukraine by offering new business opportunities for providers and affordable services to eligible businesses. In the long run, the Cyber Voucher Program will encourage businesses to spend more on cybersecurity through increased awareness and trust. The Activity’s Cyber Voucher program is in line with the National Cybersecurity Strategy of Ukraine, under the ‘development of safe, sustainable, and reliable cyberspace’ pillar’s raising public awareness of cybersecurity component.

Please refer to the detailed description of the program and expected achievements in Section D. Program Description of this RFA for more information.

Pursuant to 2 CFR 700.13, it is USAID’s policy to refrain from awarding 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. See Annex I for Standard Provisions.

DAI reserves the right to fund any or none of the applications submitted.

Subject to the availability of funds, DAI intends to award one grant per year to one organization/institution. The expected duration of DAI support or the period of performance is one year. DAI, as primary implementer of the USAID Cybersecurity Activity, reserves the right to fund any or none of the applications submitted.

For the purposes of this program, this RFA is being issued and consists of this cover letter and 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, not later than **February 16, 2024**, 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 **10 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,

Petro Matiaszek
Chief of Party

Cyber Voucher Administration Grant Program

Table of Contents

Section A – Grant Application Instructions	4
I. Application Procedure	4
A. Completion and submission of applications	4
B. Preparation Instructions – Technical.....	5
C. Preparation Instructions – Financial and Administrative Documentation.....	7
Section B. Special Grant Requirements	9
Section C. Selection Process	12
Section D. Program Description	14
Annex 1: Mandatory Standard Provisions	20
Annex 2: Certifications, Assurances, Other Statements of the Recipient.....	21
Annex 3: Application Form.....	22
Annex 4: Budget.....	26
Annex 5: CVs and BioData Forms	27
Annex 6: Financial Capability Questionnaire	28
Annex 7: Instructions for Obtaining an Unique Entity ID (SAM)	36
Annex 8: Self Certification for Exemption from Unique Entity ID (SAM).....	43
Annex 9: Application Checklist	44

Section A – Grant Application Instructions

I. Application Procedure

A. Completion and submission of applications

Eligibility Requirements

RFA applicants must meet the following requirements:

- non-governmental non-profit organization;
- non-partisanship;
- more than 5 years of existence;
- experience in managing grants from international donors, preferably from USAID;
- experience in managing projects/programs with a large number of participants;
- experience with managing complex market mechanisms;

Grants cannot be given to:

Organizations excluded from federal procurement programs and other programs:

- any organizations entered with the status of "Active Exclusion" in the www.sam.gov registry;
- any "Public international organizations" (PIOs);
- any entities affiliated with DAI Global LLC or any of its directors, officers or employees.

Application Submission Requirements

- Applications may be submitted to USAIDCybersecurity_Grants@DAI.com
- Applications must include:
 1. Completed Application Form (*Annex 3*)
 2. Projected Grant Budget (*Annex 4*)
 3. CVs of all project team members
 4. Completed Financial Capability Questionnaire (*Annex 6*) and attachments (e.g. *policies*)
 5. Representations and Assurances (*Annex 2*):
 - Representation by 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)

Deadlines

Applications must be received at USAIDCybersecurity_Grants@DAI.com not later than no later than February 16, 2024, 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 25 pages (exclusive of annexes).

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

I. Project Description: The applicant must provide a detailed description of the project, specifying its activities and results.

The purpose of this grant is to implement and manage the Cyber Voucher program (the Program), which envisions the provision of cybersecurity services to eligible Small and Medium Sized Businesses (SMBs) by local, small-scale providers. On one hand, The Program will provide SMBs (or service recipients) with trusted, accredited cybersecurity providers and monetary incentives to make services more affordable, and on the other, the Program will enable participating providers to acquire new clients and get experience in new industries. Ultimately, the goal of the Program is to elevate the level of cyber preparedness of Ukrainian businesses, which otherwise might not be aware of their cyber landscape or have the resources to improve their information security, by providing them with a safe starting point.

The Program envisions the use of an online platform, which will be developed prior to program launch and given to Program administrator to manage. The platform will essentially serve as the front end for potential Program participants, where they can get acquainted with up-to date information on the Program and register. The contractor which will be developing the platform will perform an onboarding for the administrator so that the organization can effectively use the tool.

At a minimum, the platform will serve the following functions:

- Display up-to-date information on the eligibility requirements for participants
- Display the available service under the program
- Display any rules and regulations which apply to participating in the program
- List the necessary documents for registration (service providers and recipients) and accreditation (service providers)
- Provide ability to create an online account or “user cabinet” for service providers and recipients
- Provide ability to service recipients to choose the desired service and submit a requisition
- Notify all eligible service providers about a new requisition
- Provide ability to for service providers to submit their bids / price proposals
- Provide ability for service recipients to view available offers for their requisition
- Provide ability to submit feedback; both service recipient to providers, and service provider to recipient

Essential duties and responsibilities the grantee is expected to have the capacity to perform (not limited to):

- Evaluating eligibility of applicants, i.e. gathering standard list of documentation and checking as per Activity’s guidelines (both service providers and recipients). Assisting applicants with any documentation related questions.

- Perform service provider accreditation for all services a provider desires to offer under the Program, which involves gathering additional documentation (references, proof of past performance), to ensure provider has the skill and capacity required.
- Operate the Cyber Voucher online platform. Platform developers will perform an onboarding for the grantee, with the grantee subsequently expected to operate the platform day-to-day. Technical support will be provided by the developer for at least the first 6 months of operation.
- Provide the necessary cybersecurity expertise. Service recipients will need to be guided by the administrator when they learn which services are available under the Program and which should they choose depending on their current cybersecurity landscape.
- Perform communication/promotional activities together with the Activity's communications team in order to attract participants and share success stories.
- Manage the financial side of the Program. As part of the grant budget, the grantee will be given a lump sum designated specifically for voucher disbursements. After any given instance of a performed service, grantee needs to ensure service recipient has paid its share of cost to service provider, and consequently the grantee makes the payment for the remainder of the price (voucher amount).

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.

This is not an exhaustive list (grantee is free to propose additional metrics), but at the very least the grantee must track the following (the online platform may have functionality to track some of these, details will be discussed with winning applicant at the contract signing stage):

- Total number of registered cybersecurity providers
- Total number of active cybersecurity providers (completed one or more services)
- Total number of registered SMBs (service recipients)
- Number of vouchers disbursed
- Total monetary amount disbursed
- Number each service was performed under the Program
- Other metrics as suggested by grantee

The Activity may add more metrics and/or adjust the ones given above.

3. Sustainability: The applicant should describe how the project or its benefits will continue after grant funding ends. The Activity has analyzed several potential sustainability scenarios. The applicant needs to provide a short summary of how the program may run after the end of grant.

4. Personnel: Each applicant should provide, as part of their application, a detailed curriculum vitae that demonstrates 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.

In addition to the responsibilities listed in section 1 above, the applicant must have the staff to perform these duties. If the applicant does not have relevant staff employed at the time of submission of the

application, relevant positions must be accounted for in the budget (i.e., hire the missing personnel with grant funds for the duration of the program). The two positions required by the Activity are

- Accountant or financial manager, preferably with experience in dealing with USAID grants and a large volume of transactions.
- Senior project manager, who will act as the primary contact with the Activity for the duration of the grant. The manager is required to maintain day-to-day communication with the Activity and able to provide updates on the running of the Cyber Voucher program whenever requested.

Beyond the positions listed above, the grantee is free to propose their vision of the personnel they believe will be sufficient to implement the program and reflect this accordingly in the budget.

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.

As a rough estimate which can be used when developing the budget, the Program envisions around 100-150 vouchers to be disbursed over one year of operations. Grantee needs to have capacity to review, verify, and make timely payments so that operation of the Program is not hindered by lack of administrative capacity.

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 related areas. 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. Applicants may include a cost-sharing component if they desire, however, this is not a requirement for obtaining a grant under 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 5 pages.

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. See attached Annex 4 for the budget form. 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 can 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. **Unique Entity ID (SAM)** There is a mandatory requirement for the applicant to provide a Unique Entity ID (SAM) to DAI. Without an Unique Entity ID (SAM), 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 an Unique Entity ID (SAM) to DAI. Organizations who fail to provide an Unique Entity ID (SAM) 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 an Unique Entity ID (SAM) 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 an Unique Entity ID (SAM), see Annex 7- Instructions for Obtaining an Unique Entity ID (SAM)- DAI'S Vendors, Subcontractors and Grantees. For those not required to obtain an Unique Entity ID (SAM), see Annex 8- Self Certification for Exemption from Unique Entity ID (SAM) Requirement.

Section 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: 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 200.307. 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), immediately above shall apply automatically. Grantees who are commercial organizations may not apply 1) to their program income.

Use of Funds: Funds provided under any grant awarded shall be used exclusively to maintain enough staff to effectively perform all necessary duties and responsibilities as the administrator of the Cyber Voucher program and make the voucher payments themselves. Methodologies and policies will be developed with the successful applicant to optimize the process on how the grants funds shall be used. 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. 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:

- **Interim Program report** to be submitted during project implementation according to a schedule determined by 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.
- **Interim Financial reports** will be submitted to DAI according to a schedule described in the grant agreements. 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.

- **Final program 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.

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 not be used to finance any of the following:

1. Goods or services which are to be used primarily to meet military requirements or to support police or other law enforcement activities,
2. Surveillance equipment,
3. Equipment, research and/or services related to involuntary sterilization or the performance of abortion as a method of family planning,
4. Gambling equipment, supplies for gambling facilities or any hotels, casinos or accommodations in which gambling facilities are or are planned to be located,
5. Activities which significantly degrade national parks or similar protected areas or introduce exotic plants or animals into such areas, or
6. Establishment or development of any export processing zone or designated area where the labor, environmental, tax, tariff, and/or safety laws of the country in which such activity takes place would not apply.
7. Pharmaceuticals,
8. Pesticides,
9. Logging equipment,
10. Luxury goods (including alcoholic beverages and jewelry),
11. Establishing or expanding any enterprise that will export raw materials that are likely to be in surplus in world markets at the time such production becomes effective and that are likely to cause substantial injury to U.S. producers,

12. Activities which would result in the loss of forest lands due to livestock rearing, road construction or maintenance, colonization of forest lands or construction of dams or other water control structures,
13. Activities which are likely to have a significant adverse effect on the environment, including any of the following (to the extent such activities are likely to have a significant adverse impact on the environment):
 - i.) Activities which may lead to degrading the quality or renewability of natural resources;
 - ii.) Activities which may lead to degrading the presence or health of threatened ecosystems or biodiversity;
 - iii.) Activities which may lead to degrading long-term viability of agricultural or forestry production (including through use of pesticides);
 - iv.) Activities which may lead to degrading community and social systems, including potable water supply, land administration, community health and well-being or social harmony.
14. Activities which are likely to involve the loss of jobs in the United States due to the relocation or expansion outside of the United States of an enterprise located in the United States, or
15. Activities which the Grantee is aware are reasonably likely to contribute to the violation of internationally or locally recognized rights of workers,
16. Activities to support the production of agricultural commodities for export from Malawi when such commodities would directly compete with exports of similar United States agricultural commodities to third countries and have a significant impact on United States exporters.

Other: As mentioned, the grant will be made available to eligible organization in grant amount up to 800,000 USD (all grants will be distributed in local currency equivalent), out of which at least 500,000 USD will be solely designated for paying out the voucher amounts to service providers. Payment to grantee 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.

Section C. Selection Process

Within 30 working 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. 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 USAID Cybersecurity Critical Infrastructure Activity Headquarters by the Director of Operations or other designated staff.

If suitable applications are received, one or more awards will be made within 60 working days of the review panel meeting provided that the awardee (s) furnish (es) DAI with all the required documentation as itemized in Section A of this RFA.

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:

1. Past performance and capability;

The applicant's past experience and capabilities in conducting projects of a similar nature.

Does the applicant have substantial experience with implementing large projects or programs involving day-to-day interaction with program participants/users, in particular in the field of IT or cybersecurity. Does the applicant have experience with implementing grant projects/programs financed by international donor organizations (USAID preferred)

Very good = 50 points; good = 20 points; average = 5 points; poor = 0 points

2. Project justification and design;

Does the proposed staff have experience in carrying out the activities specified in the request? Can the proposed technical approach reasonably be expected to produce the expected results? Is it clear that applicant either already has or is reasonably able to secure the required personnel which will meet the capacity and expertise requirements of the grant?

Very good = 40 points; good = 20 points; average = 5 points; poor = 0 points

3. Cost effectiveness;

- Is the cost reasonable in terms of the expected results?

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

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, 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.

Section D. Program Description

Background

The USAID Cybersecurity for Critical Infrastructure in Ukraine Activity (Activity), implemented by DAI Global LLC, is designed to reduce cybersecurity vulnerabilities in critical infrastructure (CI) sectors and transform Ukraine from a compromised, reactive cybersecurity actor to a proactive cybersecurity leader. Recognizing the complexity of the threat posed by Russian hybrid warfare, the Activity has adopted a multi-sector approach that engages government, businesses, and academia to improve Ukraine's cybersecurity for CI. Through three strategic objectives, the Activity is improving the enabling environment for cybersecurity, strengthening Ukraine's cybersecurity workforce, and stimulating market development to promote Ukrainian cybersecurity products and services.

The USAID Cybersecurity for Critical Infrastructure in Ukraine Activity is planning to launch a Cyber Voucher Program in 2024 to stimulate the development of the cybersecurity market in Ukraine by offering new business opportunities for providers and affordable services to eligible businesses. In the long run, the Cyber Voucher Program will encourage businesses to spend more on cybersecurity through increased awareness and trust. The Activity's Cyber Voucher program is in line with the National Cybersecurity Strategy of Ukraine, under the 'development of safe, sustainable, and reliable cyberspace' pillar's raising public awareness of cybersecurity component.

Similar programs were implemented in several other countries. In Scotland, the Cyber Resilience Voucher Scheme provided up to a GBP 1,500 for eligible small and medium sized businesses (SMBs) in order to develop a cyber action plan, and consequently check the adherence of firms' cyber systems according to an established government standard. In Australia, SMBs have an opportunity to get directly connected with one of cyber security research teams at participating universities and have them solve their unique issue, with projects eligible for up to AU\$ 15,000. UK offered Cyber Security Innovation Vouchers worth up to GBP 5,000 to SMBs, which covered assessment and testing of firms' cyber security.

Objective

The main goal of the program is to stimulate the development of the cyber security market in Ukraine. This will be achieved through two primary objectives which correspond to both sides of the market:

- Provide new business opportunities for service providers (sellers) by matching them with SMBs which require CS services. The "new" here does not simply mean an additional client, but potentially new work experience altogether for providers who have not worked with critical infrastructure entities previously.
- Encourage SMBs (buyers) to spend more on cybersecurity in the long term by making them more aware of their cyber landscape and providing them with a guided jump start into evaluating and elevating their cyber preparedness.

The scope of the program was defined by the Activity's goals and the challenges faced by SMBs and service providers:

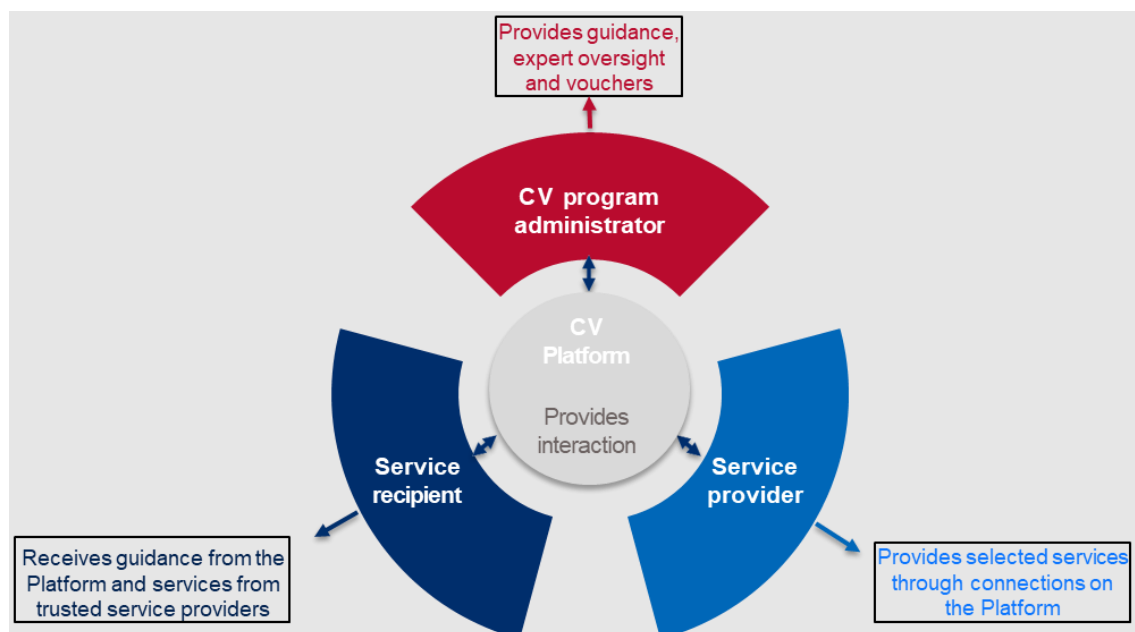
SMBs (service recipients)

- The target service recipient is a private sector SMB in one of the industries designated as critical infrastructure. These entities typically have no or very low understanding of their cybersecurity, and even if there is sufficient knowledge, usually do not have available funding to develop and maintain an adequate cybersecurity framework. A major barrier in these cases is inability to navigate the cybersecurity space and a lack of understanding where to start and who to trust.
- Through the program, the service recipient will get access to accredited and trusted providers, receive plain-language guidance by the Platform, and get financial support (in the form of vouchers) which will make services more affordable. In the long run, this is likely to lead to an increase in cybersecurity expenditure by businesses.

Service providers (sellers)

- The target service provider is either an individual entrepreneur (FOP) or an SMB. Such providers typically do not have access to a wide audience of clients and are limited in how they can promote themselves and reach new customers. They have confirmed experience with providing select services but might lack hands on experience with best practices and methodologies.
- Through the program, the service provider will get access to a pool of potential customers, an opportunity to increase their portfolio, establish new business relationships, and have ability to gain experience in a variety of industries while having access to best practices and ability to consult with an experienced cybersecurity professional.

At its core, the program offers discounted cybersecurity services to SMBs and access to “ready” clients to service providers. Both end user groups will interact with the online platform, where certain steps of their journey will be automated and streamlined. The platform will be maintained and run by an administrator organization. The administrator will be responsible for the day-to-day operation of the program, providing guidance and expert oversight of both SMB and service provider journeys.



SMBs (service recipients)

1. Register on the online platform
2. Select service with guidance from administrator
3. Sign contract with provider
4. Receive the service with oversight of administrator
5. Assess the provider and provide feedback to administrator
6. Pay discounted price, administrator covers voucher amount

Service providers (sellers)

1. Register on the online platform and pass accreditation for select services
2. Participate in competitive bidding process
3. Sign contract with recipient
4. Deliver the service with access to best practices and methodologies
5. Receive payment (voucher amount from administrator, rest from service recipient)
6. Receive evaluation and reference letter

Target cybersecurity services to be covered by program

To guide the service recipients through their journey of building cybersecurity and information security capabilities, target services will be split in to two tiers:

Tier I: InfoSec diagnostics and investigation services

- NIST Cyber Security Framework compliance assessment
- ISO/IEC 27001 compliance assessment
- Preparation for financial statements audit from IT standpoint– ITGC assessment
- Cabinet of Ministers of Ukraine Resolution #518 compliance assessment
- NBU Resolution #95 compliance assessment
- GDPR compliance assessment
- InfoSec current state diagnostics and recommendations development
- InfoSec breaches discovery (IT environment compromise assessment)
- Digital crimes investigation (digital forensic)
- Vulnerability assessment of IT environment

Tier 2: InfoSec development and testing services; outsourcing

NIST Cyber Security Framework requirements implementation	Incident detection and response outsourcing
ISO/IEC 27001 requirements implementation	Outsourcing of InfoSec function (CISO as a service)
GDPR requirements implementation	InfoSec awareness program outsourcing
Preparation for financial statements audit from IT standpoint– ITGC implementation	Vulnerability management outsourcing
InfoSec documentation framework development	Application security testing outsourcing
InfoSec processes and related controls implementation	Infosec internal audit outsourcing
InfoSec strategy development	InfoSec risk management outsourcing
IT continuity practices development and implementation	
InfoSec Awareness / Cyber-Hygiene practices and materials development	
Penetration testing by social engineering methods	
Penetration testing to IT environment	
Cabinet of Ministers of Ukraine Resolution #518 requirements implementation	
NBU Resolution #95 requirements implementation	
Security testing of mobile applications code	
Security testing of web applications code	
Application security testing	

Requirements for Service Providers

Eligibility requirements for service providers are split into two groups:

Qualification requirements – requirements that should be met in order to enroll to in the program. The goal of these requirements is checking the good standing of each service provider and mostly relate to their legal status and involvement in prohibited or risky practices.

- Legal status check
 - No bankruptcy proceedings
 - Not under liquidation
 - No engagement in corruption
 - No outstanding conviction for a crime
 - Must submit full ownership information if provider is a legal entity
- Excluded parties screening
 - Not under sanctions
 - Not an excluded party
 - No links with Russia
 - Additional USAID/DAI checks

Accreditation requirements – requirements that should be met in order for a provider to be eligible to perform different services under the program. These requirements are aimed at the checking provider's experience, as well as relevant operational and technical capacities required for the provision of specific services.

- For individual entrepreneurs (FOPs):
 - Capacity statement – basic information about applicant's qualifications and capacities relevant to delivery of services under program (e.g., education, service portfolio, track record)
 - Control statement – information about relationships with Russian entities
 - Extract from Corporate Register
 - Full scope certificate from the Bankruptcy Register
 - Non-conviction certificate
 - Affidavit – necessary declarations, acknowledgment of conformity with qualification requirements, other program rules
- For legal entities:
 - Capacity statement – CVs of key staff, service portfolio, track record
 - Control statement – ownership information / shareholder structure, relationships to Russian entities
 - Company charter
 - Extract from Corporate Register
 - Full scope certificate from Bankruptcy Register
 - Certificate from Corruption Offences Register
 - Non-conviction certificates of key officials
 - Affidavit

Vouchers and Contracting

The portion of the service price which will be covered by a voucher will vary depending on the type of service, and whether it is the first or repeating instance of an SMB purchasing a service through the Cyber Voucher Program. Additional factors may be considered and implemented closer to program launch. Preliminarily, the activity envisions that the amount covered by a single voucher should not exceed \$5,000, with average voucher amount in the \$1,000-\$2,000 range. The price of any given service will depend on several factors, including the size and type of an SMB, and complexity of its systems.

Once a service recipient makes a request for a service, eligible service providers which were previously registered and accredited by the Program are able to submit their bids. Grantee is expected to provide cybersecurity expertise and advise service recipients on whether received offers from service providers are adequate and do not deviate significantly from market rates. Once a service recipient selects the provider, the two parties will proceed to contracting just as they would outside of the program.

Annex 1: Mandatory Standard Provisions

The Mandatory Standard Provisions are provided separately as a PDF document.

Mandatory Standard Provisions for Non-US Nongovernmental Recipients:

<https://www.usaid.gov/sites/default/agency-policy/303mab.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, 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

Application Form	
USAID Cybersecurity for Critical Infrastructure in Ukraine Activity	
I. ORGANIZATION DETAILS	
1) Organization name and ID [Tax ID or USREOU (Ukrainian state registry legal entity identifier)]:	
[full legal name]	
[Tax ID or USREOU]	
2) Date organization was founded and registration status:	
[Current registration status]	
3) Contact information:	
[Contact Information— Contact name, title, address, telephone, e-mail, etc. The contact person (agent) is responsible for communications between the Activity and the applicant. This applies to all aspects of the grant application, from initial submission through negotiation and award. The agent must have full authority and responsibility to act on behalf of the applicant. The agent should be someone who will be directly involved with the grant activity and has a proven, established relationship with the APPLICANT]	
Key contact person(s) and title:	
Office address:	Office phone:
Mobile:	
Email:	Website:
4) Describe the organization, its purpose, and past related experience:	
[Describe the organization and its activities—This section should introduce the applicant and its background: how it was formed, its mission or purpose, major accomplishments in the area of the targeted activity, current activities, past related experience, and clients. This section must not exceed 1 page in length]	
5) List contact information for three (3) references from previous firms, organizations, or donor agencies (U.S. and other) that your organization has collaborated with in the last two years:	

[References—List three donors, partner organizations, or community leaders that can provide references for your organization’s ability to successfully carry out the financial, administrative, and technical requirements of the grant activity. Briefly describe your relationship to the reference and the nature and duration of your work together. If the reference is a previous donor, list the activity and location of the activity(s) they funded. Be sure to provide complete information, including a point of contact, with telephone and email]

Firm or Organization	Nature of Relationship or Title of Project, Location	Start & End Dates of Collaboration	Contact Person
			Name & Position: Email: Tel:
			Name & Position: Email: Tel:
			Name & Position: Email: Tel:

II. TECHNICAL PROPOSAL

I) Location:

Location:	<i>[Location]</i>
Date ready to begin:	<i>[month, and year]</i>

2) Budget Summary (Total Cost)

From Annex 4, provide the final total estimated cost of your proposed application in USD.

Budget Category	Grant Resources (in USD)
Total Estimated Costs (in USD)	\$

III. PROJECT DESCRIPTION

(ADJUST THIS ENTIRE SECTION AS NECESSARY)

I) Project summary

(This section should present your technical approach of your proposed project summary and how grant funds will be used to advance selected objectives. The summary must **be no more than 5 pages** and should clearly address what your project will accomplish related to product development, marketing, expansion and/or improvement that will have an impact on the overall cybersecurity market in Ukraine. 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) Monitoring and evaluation

(Please include the tools you will use to monitor project activities and evaluate project results)

3) Sustainability

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

IV. PROPOSED PERSONNEL

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

(Please attach CVs for key personnel involved in the project)

No	NAME & SURNAME	TITLE	ROLE IN THE PROJECT	DESCRIPTION
1				
2				
3				
4				

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.)

2) Past performance		
<i>Please describe no more than three major projects in Ukraine in which your organization was involved over the past three years, using the table below.</i>		
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)		
VI. STATEMENT OF LIABILITY AND DISCLOSURE OF RELATIONSHIPS		
<p>I, the undersigned, being the person responsible as the applicant submitting this application under the organization [Insert Name of Organization] for this grant, certify that the information given in this application is true and accurate, and that the organization, [Insert Name of Organization], is not affiliated with DAI, DAI subcontractors or any of its directors, officers, or employees.</p>		
	Name and surname:	
	Title/Position:	
	Signature:	
	Date:	

Annex 4: Budget

The budget template is provided separately as an Excel document.

Annex 5: CVs and BioData Forms

Send your CVs in arbitrary form.

Annex 6: Financial Capability Questionnaire

Annex 6

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 comply with 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 U.S. Federal Cost principles as described in 2 CFR 200 Subpart E?

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 (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 7: Instructions for Obtaining a Unique Entity ID (SAM)- DAI'S Vendors, Subcontractors and Grantees

INSTRUCTIONS FOR OBTAINING AN Unique Entity ID (SAM) DAI'S VENDORS, SUBCONTRACTORS & GRANTEEES

Note: There is a Mandatory Requirement for your Organization to Provide a Unique Entity ID (SAM) to DAI

I. SUBCONTRACTS/PURCHASE ORDERS: All domestic and foreign organizations which receive first-tier subcontracts/ purchase orders with a value of \$30,000 and above are required to obtain a Unique Entity ID (SAM) prior to signing of the agreement. *Your organization is exempt from this requirement if the gross income received from all sources in the previous tax year was under \$300,000. Please see the self-certification form attached.*

II. MONETARY GRANTS: All foreign entities receiving first-tier monetary grants (standard, simplified and FOGs) 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 of the grant. All U.S. organizations who are recipients of 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.

NO SUBCONTRACTS/POs (\$30,000 + above) or MONETARY GRANTS WILL BE SIGNED BY DAI WITHOUT PRIOR RECEIPT OF AN UNIQUE ENTITY ID (SAM).

Note: The determination of a successful offeror/applicant resulting from this RFP/RFQ/RFA is contingent upon the winner providing a Unique Entity ID (SAM) to DAI. Organizations who fail to provide a Unique Entity ID (SAM) will not receive an award and DAI will select an alternate vendor/subcontractor/grantee.

Background:

Summary of Current U.S. Government Requirements - Unique Entity ID (SAM)

Effective April 4, 2022, entities doing business with the federal government will use the Unique Entity Identifier (SAM) created in SAM.gov. The Unique Entity ID (SAM) is a 12-character alphanumeric value managed, granted, and owned by the government. This allows the government to streamline the entity identification and validation process, making it easier and less burdensome for entities to do business with the federal government.

Entities are assigned an identifier during registration or one can be requested at SAM.gov without needing to register. Ernst and Young provides the validation services for the U.S. Government. The information required for getting a Unique Entity ID (SAM) without registration is minimal. It only validates your organization's legal business name and address. It is a verification that your organization is what you say it is.

The Unique Entity ID (SAM) does not expire.

Summary of Previous U.S. Government Requirements – DUNS

The Data Universal Numbering System (DUNS) is a system developed and managed by Dun and Bradstreet that assigns a unique nine-digit identifier to a business entity. It is a common standard worldwide and was previously used by the U.S. Government to assign unique entity identifiers. This system was retired by the U.S. Government on April 4, 2022 and replaced with the Unique Entity Identifier (SAM). After April 4, 2022 the federal government will have no requirements for the DUNS number.

If the entity was registered in SAM.gov (active or inactive registration), an Unique Entity ID (SAM) was assigned and viewable in the entity registration record in SAM.gov prior to the April 4, 2022 transition. The Unique Entity ID (SAM) can be found by signing into SAM.gov and selecting the Entity Management widget in your Workspace or by signing in and searching entity information.




Instructions detailing the process to be followed in order to obtain an Unique Entity ID (SAM) for your organization.

THE PROCESS FOR OBTAINING AN UNIQUE ENTITY ID IS OUTLINED BELOW:

- I. Have the following information ready to request an Unique Entity ID (SAM)
 - a. Legal Business Name
 - b. Physical Address (including ZIP + 4)
 - c. SAM.gov account (this is a user account, not actual SAM.gov business registration).
 - i. **As a new user**, to get a SAM.gov account, go to www.sam.gov.
 1. Click “Sign In” on the upper right hand corner.
 2. Click on “Create a User Account”

An official website of the United States government [Here's how you know](#)

LOGIN.GOV SAM.GOV






sam.gov is using Login.gov to allow you to sign in to your account safely and securely.

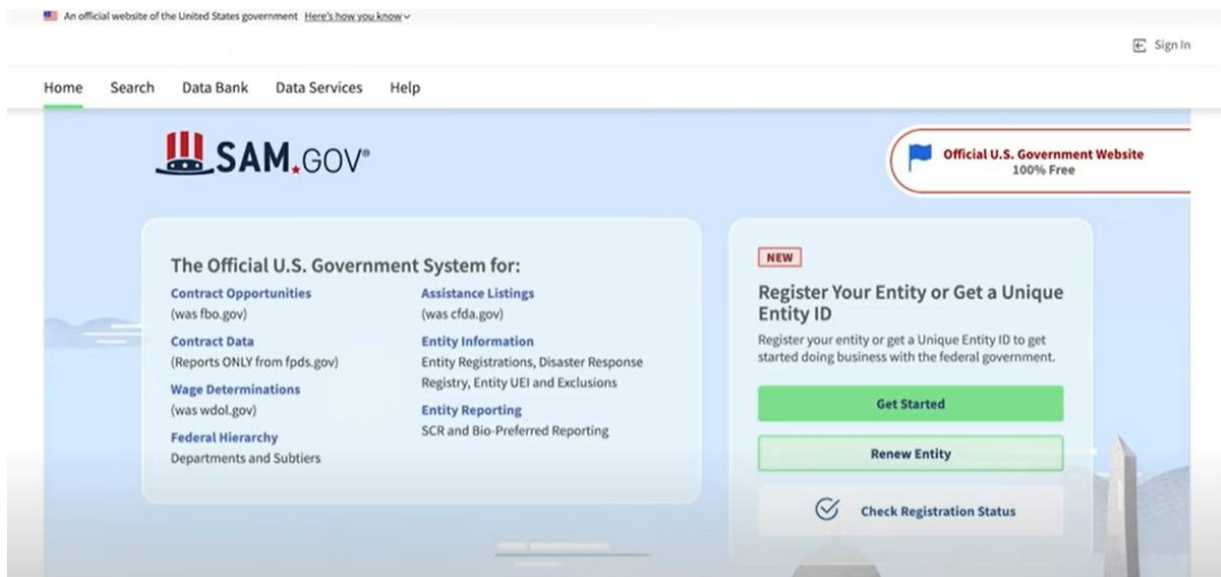
Email address

Password Show password

Sign in

 Create an account

3. Choose Account Type:
 - a. Create an Individual User Account to perform tasks such as register/update your entity, create and manage exclusion records or to view FOUO level data for entity records.
 - b. Create a System User Account if you need system-to-system communication or if performing data transfer from SAM to your government database system. Complete the requested information, and then click “Submit.”
 4. Click “DONE” on the confirmation page. You will receive an email confirming you have created a user account in SAM.
 5. Click the validation link in the email that contains the activation code within 48 hours to activate your user account. If the email link is not hyperlinked (i.e., underlined or appearing in a different color), please copy the validation link and paste it into the browser address bar. You can now register an entity.
- NOTE: Creating a user account does not create a registration in SAM, nor will it update/renew an existing registration in SAM.
2. Once you have registered as a user, you can get an Unique Entity ID by selecting the “Get Started” button on the SAM.gov home page.



3. Select “Get Started” on the Getting Started with Registration page.

4. Select “Get Unique Entity ID” on the Get Started page.

5. Enter Entity Information.



- a. If you previously had a DUN Number, make sure your Legal Business Name and Physical Address are accurate and match the Entity Information, down to capitalization and punctuation, used for DUNS registration.

6. When you are ready, select “Next”

7. Confirm your company’s information.



- a. On this page you will have the option to restrict the public search of this information. “Allow the selected record to be a public display record.” If you uncheck this box, only you and the federal government users will be able to search and view the entity information and entities like DAI will not be able to independently verify that you have an Unique Entity Identifier (SAM).

Allow the selected record to be a public display record.

If you feel displaying non-sensitive information like your registration status, legal business name and physical address in the search engine results poses a security threat or danger to you or your organization, you can restrict the public viewing of you record in SAM’s search engine. However, your non-sensitive registration information remains available under the Freedom of Information Act to those who download the SAM public data file. [Learn more about SAM public search results](#)

8. When you are ready, select “Next”

9. Once validation is completed, select “Request UEI” to be assigned an Unique Entity ID (SAM). Before requesting your UEI (SAM), you must certify that you are authorized to conduct transactions under penalty of law to reduce the likelihood of unauthorized transactions conducted for the entity.



Request UEI

You have completed validation. Select **Request UEI** to be assigned a Unique Entity ID.

VERIFIED MATCH:

US TEST COMPANY 999 ● Public

DUNS UNIQUE ENTITY ID:
362267515

PHYSICAL ADDRESS
3501 CORPORATE PKWY
CENTER VALLEY, PA 18034
US

Before requesting your UEI, please certify that you are authorized to conduct transactions under penalty of law to reduce the likelihood of unauthorized transactions conducted for my entity. Then select **Request UEI**.

I certify that I am authorized to conduct transactions on behalf of the entity.

Request UEI

10. The Unique Entity ID will be shown on the next page. SAM.gov will send an email confirmation with your Unique Entity ID.



Receive UEI

Congratulations! You have been assigned the following Unique Entity ID.

EH4HG9MLR7Q6

VERIFIED MATCH:

US TEST COMPANY 999 ● Public

DUNS UNIQUE ENTITY ID:
362267515

SAM UNIQUE ENTITY ID:
EH4HG9MLR7Q6

PHYSICAL ADDRESS
3501 CORPORATE PKWY
CENTER VALLEY, PA 18034
US

You have finished getting your Unique Entity ID, select **Done** to return to your workspace.

To continue with registration, select **Continue Registration**.

[Continue Registration](#) [Done](#)

11. If you need to view the Unique Entity ID from SAM in the future or update the organization’s information, sign into SAM.gov and go to “Entity Management” widget.

SAM.GOV Requests Notifications Workspace Sign Out

Home Search Data Bank Data Services Help

Workspace

Entity Management
What do I need for registration? [Get Started](#)

Entity Registration

0	0	0	0
ACTIVE	DRAFT	WORK IN PROGRESS	SUBMITTED

Next Update Due: Due in Next 30 days: 0 Entity Registrations

Unique Entity ID

1	0
ACTIVE	DRAFT

System Accounts

1	0	0	0	0
ACTIVE	DRAFT	CHANGE REQUEST	PENDING	DEACTIVATED

Profile

Downloads Saved Searches Following

Pending Requests
No pending requests [See All](#)

Notifications
No available notifications [See All](#)

Add A New Role
Select on the options below to request a new role. If you need a role that you do not see below, contact an administrator for your organization directly.

Select a Role

Annex 8: Self Certification for Exemption from Unique Entity ID (SAM) Requirement

Self-Certification for Exemption from Unique Entity ID (SAM) For Subcontractors and Vendors

Legal Business Name: _____

Physical Address: _____

Physical City: _____

Physical Foreign Province (if applicable): _____

Physical Country: _____

Signature of Certifier _____

Full Name of Certifier (Last Name, First/Middle Names): _____

Title of Certifier: _____

Date of Certification (mm/dd/yyyy): _____

The sub-contractor/vendor whose legal business name is provided herein, certifies that we are an organization exempt from obtaining an **Unique Entity ID (SAM)**, 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 sub-contractor/vendor may be subject to penalties, if s/he misrepresents the sub-contractor/vendor in any of the representations or certifications to the Prime Contractor and/or the US Government.

The sub-contractor/vendor 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 9: Application Checklist

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

- The application is submitted in electronic format.
- Applicable certifications and assurances are signed and included (see Annex 2)
- Budget is included
- CVs and BioData Forms are included (Annex 5)
- The statement of liability is signed and stamped (last page of application form – Annex 3)
- Completed Financial Capability Questionnaire (Annex 6)
- 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 Unique Entity ID (SAM) or a Self-Certification for Exemption from Unique Entity ID (SAM) Requirement.