



USAID Critical Infrastructure Digitization and Resilience (CIDR)

Request For Proposals (RFP)

No. REQ-BET-22-0006

Call for Proposals for GAP Analysis, Vulnerability Assessment, and implementing an Information Security Management System (ISMS) at the Ministry of Agriculture, Forestry, and Water Economy in North Macedonia

Issue Date: Issue Date: August 30, 2023

WARNING: Prospective Offerors who have received this document from a source other than the CIDR Project at DAI, 7600 Wisconsin Avenue, Bethesda, MD, 20814, should immediately contact **CIDR_Procurement@dai.com** and provide their name and mailing address in order that amendments to the RFP or other communications can be sent directly to them. Any prospective Offeror who fails to register their interest assumes complete responsibility in the event that they do not receive communications prior to the closing date.

DAI conducts business under the strictest ethical standards to assure fairness in competition, reasonable prices and successful performance or delivery of quality goods and equipment. DAI does not tolerate corruption, bribery, collusion or conflicts of interest. Any requests for payment or favors by DAI employees should be reported as soon as possible to ethics@dai.com or by visiting www.dai.ethicspoint.com. Further, any attempts by an offeror or subcontractor to offer inducements to a DAI employee to influence a decision will not be tolerated and will be grounds for disqualification, termination and possible debarment. See provision No. 9 for more details.

Table of Contents

1. Introduction and Purpose.....	4
1.1 Purpose.....	4
1.2 Issuing Office.....	4
1.3 Type of Award Anticipated	4
2. General Instructions to Offerors.....	4
2.1 General Instructions.....	4
2.2 Proposal Cover Letter	5
2.3 Questions regarding the RFP.....	5
3. Instructions for the Preparation of Technical Proposals	5
3.1 Services Specified.....	6
3.2 Technical Evaluation Criteria.....	6
4. Instructions for the Preparation of Cost/Price Proposals	7
4.1 Cost/Price Proposals.....	7
5. Basis of Award	7
5.1 Best Value Determination	7
5.2 Responsibility Determination.....	7
6. Inspection & Acceptance.....	8
7. Compliance with Terms and Conditions	8
7.1 General Terms and Conditions	8
7.2 Prohibited Technology	8
7.3 Source and Nationality.....	8
7.4 Unique Entity ID (SAM)	8
8. Anti-Corruption and Anti-Bribery Policy and Reporting Responsibilities	9
9. Attachments.....	10
9.1 Attachment A: Scope of Work for Services or Technical Specifications	10
9.2 Attachment B: Proposal Cover Letter	14
9.3 Attachment C: Price Schedule	15
9.4 Attachment D: Instructions for Obtaining an Unique Entity ID (SAM)Number - DAI'S Vendors, Subcontractors	16
9.5 Attachment E: Self Certification for Exemption from Unique Entity ID (SAM)Requirement	25
9.6 Attachment F: Past Performance Form.....	27
9.7 Attachment G: Representations and Certifications of Compliance	28
List of Optional Attachments.....	29
9.8 Attachment H: Proposal Checklist.....	29

Synopsis of the RFP

RFP No.	REQ-BET-22-0006
Issue Date	Wednesday, August 30, 2023
Title	Call for Proposals for GAP Analysis, Vulnerability Assessment, and implementing an Information Security Management System (ISMS) at the Ministry of Agriculture, Forestry, and Water Economy in North Macedonia
Issuing Office & Email/Physical Address for Submission of Proposals	Email submissions required. Please submit proposals to: CIDR_Procurement@dai.com
Deadline for Receipt of Questions	Questions regarding scope or RFP are due by 5:00pm EST on Wednesday, September 6, 2023.
Deadline for Receipt of Proposals	Proposals are due by 5:00pm EST on Friday, September 22, 2023.
Point of Contact	CIDR_Procurement@dai.com
Anticipated Award Type	Firm Fixed Price
Basis for Award	An award will be made based on the Trade Off Method. The award will be issued to the responsible and reasonable offeror who provides the best value to DAI and its client using a combination of technical and cost/price factors.

1. Introduction and Purpose

1.1 Purpose

DAI, the implementer of the USAID-funded Critical Infrastructure Digitization and Resilience (CIDR) project, invites qualified Information and Communications Technology (ICT) consultant companies **based in North Macedonia** with experience implementing ISO 27001 Information Security Management Systems (ISMS) to submit proposals to support the Ministry of Agriculture, Forestry, and Water Economy under the Government of North Macedonia with conducting a GAP analysis, vulnerability assessment, assets identification and classification, risk assessment, developing Risk Treatment Plan, Information Security Management System Implementation based on ISO 27001:2022, and identifying and carrying out capacity building technical assistance activities to increase cyber hygiene.

1.2 Issuing Office

The Issuing Office and Contact Person noted in the above synopsis is the sole point of contact at DAI for purposes of this RFP. Any prospective offeror who fails to register their interest with this office assumes complete responsibility in the event that they do not receive direct communications (amendments, answers to questions, etc.) prior to the closing date.

1.3 Type of Award Anticipated

DAI anticipates awarding a Firm Fixed Price Subcontract. This award type is subject to change during the course of negotiations.

A Firm Fixed Price Subcontract is: An award for a total firm fixed price, for values more than \$150,000, for the provision of specific services, goods, or deliverables and is not adjusted if the actual costs are higher or lower than the fixed price amount. Offerors are expected to include all costs, direct and indirect, into their total proposed price.

2. General Instructions to Offerors

2.1 General Instructions

“Offeror”, “Subcontractor”, and/or “Bidder” means a firm proposing the work under this RFP. “Offer” and/or “Proposal” means the package of documents the firm submits to propose the work.

Offerors wishing to respond to this RFP must submit proposals, in English, in accordance with the following instructions. Offerors are required to review all instructions and specifications contained in this RFP. Failure to do so will be at the Offeror’s risk. If the solicitation is amended, then all terms and conditions not modified in the amendment shall remain unchanged.

Issuance of this RFP in no way obligates DAI to award a subcontract or purchase order. Offerors will not be reimbursed for any costs associated with the preparation or submission of their proposal. DAI shall in no case be responsible for liable for these costs.

Proposals are due no later than **5:00pm EST on Friday, September 22, 2023**. Proposals must be submitted via email to CIDR_Procurement@dai.com. Email submissions must state the RFP number and title of the activity in the subject line of the email, and technical and cost proposals should be submitted in the same email. Late offers will be rejected except under extraordinary circumstances at DAI’s discretion.

Late offers will be rejected except under extraordinary circumstances at DAI’s discretion.

The submission to DAI of a proposal in response to this RFP will constitute an offer and indicates the Offeror's agreement to the terms and conditions in this RFP and any attachments hereto. DAI reserves the right not to evaluate a nonresponsive or incomplete proposal.

2.2 Proposal Cover Letter

A cover letter shall be included with the proposal on the Offeror's company letterhead with a duly authorized signature and company stamp/seal using Attachment B as a template for the format. The cover letter shall include the following items:

- The Offeror will certify a validity period of 60 days for the prices provided.
- Acknowledge the solicitation amendments received.

2.3 Questions regarding the RFP

Each Offeror is responsible for reading and complying with the terms and conditions of this RFP. Requests for clarification or additional information must be submitted in writing via email to CIDR_Procurement@dai.com by **5:00pm EST on Wednesday, September 6, 2023**. If you do not have a question but would like to register your interest and receive a copy of the Questions and Answers, please send an email to CIDR_Procurement@dai.com. No questions will be answered by phone.

Any verbal information received from a DAI or CIDR employee or other entity shall not be considered as an official response to any question regarding this RFP.

Copies of questions and responses will be distributed in writing to all prospective bidders who are on record as having received this RFP after the submission date specified in the Synopsis above.

3. Instructions for the Preparation of Technical Proposals

Technical proposals shall be sealed in a separate envelope from cost/price proposals and shall be clearly labeled as "VOLUME I: TECHNICAL PROPOSAL".

Technical proposals shall include the following contents:

1. Technical Approach - Description of the proposed services which meets or exceeds the stated technical specifications or scope of work.
 - The proposal must show how the Offeror plans to complete the work and describe an approach that demonstrates the achievement of timely and acceptable performance of the work.
 - This description should take the form of a narrative format in a Word document with a Gantt chart that reflects the anticipated timeline for completion of each task and sub-task.
2. Management approach – Description of the Offeror's staff assigned to the project. The proposal should describe how the proposed team members have the necessary experience and capabilities to carry out the Technical Approach.
 - For all named staff, the management approach should include their qualifications, including # of years of experience, areas of expertise, and education qualifications.
 - Qualified staff should have ISO 27001 (Lead) implementer and ISO 27001 (Lead) Auditor certifications.
3. Past Performance – Provide a list of at least three (3) recent awards of similar scope and duration. The information shall be supplied as a table and shall include the legal name and address of the organization for which services were performed, a description of work performed, the duration

of the work and the value of the contract, description of any problems encountered and how it was resolved, and a current contact phone number of a responsible and knowledgeable representative of the organization. See Attachment F.

3.1 Services Specified

For this RFP, DAI is in need of the services described in Attachment A.

3.2 Technical Evaluation Criteria

Each proposal will be evaluated and scored against the evaluation criteria and evaluation sub-criteria, which are stated in the table below. Cost/Price proposals are not assigned points, but for overall evaluation purposes of this RFP, technical evaluation factors other than cost/price, when combined, are considered significantly more important than cost/price factors.

Evaluation Criteria	Maximum Points
Technical Approach: -Does the proposal clearly explain and respond to the requirements of the activity as outlined in the scope? -Does the proposal indicate the necessary stakeholders that will need to be involved and a clear plan for engaging them? -Does the proposal include a Gantt chart that clearly outlines a timeline for proposed steps to accomplish the activity?	40 points
Management Approach: -Does the organization have sufficiently qualified staff who can undertake the scope of work? Do qualified staff have ISO 27001 (Lead) implementer and ISO 27001 (Lead) Auditor certifications? -Does the proposed approach and timeline fulfill the requirements of executing the scope of work in a timely and efficient manner? - Does the offeror have the ability to be in-country consistently for the duration of the assessment of the MoA ICT infrastructure as well as that of several of the 40 branch offices located throughout the country?	30 points
Past Performance: -Does the organization have a track record of successfully conducting similar work? Are three examples included?	30 points
Total:	100 points

4. Instructions for the Preparation of Cost/Price Proposals

4.1 Cost/Price Proposals

Cost/Price proposals must be submitted as a separate attachment in the email submission and must be clearly labeled as “Cost/Price Proposal – Volume 2”.

Cost/Price proposals shall be sealed in a separate envelope from technical proposals and shall be clearly labeled as “VOLUME II: COST/PRICE PROPOSAL”.

- Provided in Attachment C are instructions for obtaining a template for the Price Schedule for **firm-fixed price awards**. Offerors shall complete the template including as much detailed information as possible.
- This RFP includes several tasks that are independent of each other. Offerors shall provide a cost proposal for each task as it is listed in the table in Attachment A of this RFP. CIDR reserves the right to choose to implement all, or any of the listed tasks from the services provided by the Offeror.
- Offerors must include detailed budget notes and assumptions for all expenses included in the budget. These notes can either be included as a separate tab on the budget, or as a separate Word document.
- It is important to note that Value Added Tax (VAT) shall be included on a separate line. These services are not eligible for VAT exemption under the DAI prime contract. The Subawardee is responsible for all applicable taxes and fees, as prescribed under the applicable laws for income, compensation, permits, licenses, and other taxes and fees due as required.

5. Basis of Award

5.1 Best Value Determination

DAI will review all proposals, and make an award based on the technical and cost evaluation criteria stated above, and select the offeror whose proposal provides the best value to DAI. DAI may also exclude an offer from consideration if it determines that an Offeror is "not responsible", i.e., that it does not have the management and financial capabilities required to perform the work required.

Evaluation points will not be awarded for cost. Cost will primarily be evaluated for realism and reasonableness. DAI may award to a higher priced offeror if a determination is made that the higher technical evaluation of that offeror merits the additional cost/price.

DAI may award to an Offeror without discussions. Therefore the initial offer **must contain the Offeror's best price and technical terms**.

5.2 Responsibility Determination

DAI will not enter into any type of agreement with an Offeror prior to ensuring the Offeror's responsibility. When assessing an Offeror's responsibility, the following factors are taken into consideration:

1. Provide evidence of the required business licenses to operate in the host country.
2. Evidence of an Unique Entity ID (SAM) (explained below and instructions contained in Attachment D).
3. The source, origin and nationality of the products or services are not from a Prohibited Country (explained below).
4. Having adequate financial resources to finance and perform the work or deliver goods or the ability to obtain financial resources without receiving advance funds from DAI.
5. Ability to comply with required or proposed delivery or performance schedules.

6. Have a satisfactory past performance record.
7. Have a satisfactory record of integrity and business ethics.
8. Have the necessary organization, experience, accounting and operational controls and technical skills.
9. Have the necessary production, construction and technical equipment and facilities if applicable.
10. Be qualified and eligible to perform work under applicable laws and regulations.

6. Inspection & Acceptance

The designated DAI Project Manager will inspect from time to time the services being performed to determine whether the activities are being performed in a satisfactory manner, and that all equipment or supplies are of acceptable quality and standards. The subcontractor shall be responsible for any countermeasures or corrective action, within the scope of this RFP, which may be required by the DAI Chief of Party as a result of such inspection.

7. Compliance with Terms and Conditions

7.1 General Terms and Conditions

Offerors agree to comply with the general terms and conditions for an award resulting from this RFP. The selected Offeror shall comply with all Representations and Certifications of Compliance listed in Attachment G.

7.2 Prohibited Technology

Bidders MUST NOT provide any goods and/or services that utilize telecommunications and video surveillance products from the following companies: Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company, or any subsidiary or affiliate thereof, in compliance with FAR 52.204-25.

8.3 Source and Nationality

Under the authorized geographic code for its contract DAI may only procure goods and services from the following countries.

Geographic Code 935: Goods and services from any area or country including the cooperating country, but excluding Prohibited Countries.

8.4 Unique Entity ID (SAM)

There is a **mandatory** requirement for your organization to provide an Unique Entity ID (SAM) to DAI. Without an Unique Entity ID (SAM), DAI cannot deem an Offeror “responsible” to conduct business with and therefore, DAI will not enter into a subcontract/purchase order or monetary agreement with any organization. The determination of a successful offeror/applicant resulting from this RFP/RFQ/RFA is contingent upon the winner providing an Unique Entity ID (SAM) to DAI. Offerors who fail to provide Unique Entity ID (SAM) will not receive an award and DAI will select an alternate Offeror.

All U.S. and foreign organizations which receive first-tier subcontracts/ purchase orders with a value of \$30,000 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 Offerors sign the self-certification statement if the Offeror claims exemption for this reason.

For those required to obtain an Unique Entity ID (SAM), see Attachment D - Instructions for Obtaining an Unique Entity ID (SAM)- DAI’S Vendors, Subcontractors

For those not required to obtain a Unique Entity ID (SAM), see Attachment E: Self Certification for Exemption from Unique Entity ID (SAM) Requirement

8. Anti-Corruption and Anti-Bribery Policy and Reporting Responsibilities

DAI conducts business under the strictest ethical standards to assure fairness in competition, reasonable prices and successful performance or delivery of quality goods and equipment. **DAI does not tolerate the following acts of corruption:**

- Any requests for a bribe, kickback, facilitation payment or gratuity in the form of payment, gift or special consideration by a DAI employee, Government official, or their representatives, to influence an award or approval decision.
- Any offer of a bribe, kickback, facilitation payment or gratuity in the form of payment, gift or special consideration by an offeror or subcontractor to influence an award or approval decision.
- Any fraud, such as mis-stating or withholding information to benefit the offeror or subcontractor.
- Any collusion or conflicts of interest in which a DAI employee, consultant, or representative has a business or personal relationship with a principal or owner of the offeror or subcontractor that may appear to unfairly favor the offeror or subcontractor. Subcontractors must also avoid collusion or conflicts of interest in their procurements from vendors. Any such relationship must be disclosed immediately to DAI management for review and appropriate action, including possible exclusion from award.

These acts of corruption are not tolerated and may result in serious consequences, including termination of the award and possible suspension and debarment by the U.S. Government, excluding the offeror or subcontractor from participating in future U.S. Government business.

Any attempted or actual corruption should be reported immediately by either the offeror, subcontractor or DAI staff to:

- Toll-free Ethics and Compliance Anonymous Hotline at (U.S.) +1-503-597-4328
- Hotline website – www.DAI.ethicspoint.com, or
- Email to Ethics@DAI.com
- USAID's Office of the Inspector General Hotline at <https://oigportal.ains.com/eCasePortal>

By signing this proposal, the offeror confirms adherence to this standard and ensures that no attempts shall be made to influence DAI or Government staff through bribes, gratuities, facilitation payments, kickbacks or fraud. The offeror also acknowledges that violation of this policy may result in termination, repayment of funds disallowed by the corrupt actions and possible suspension and debarment by the U.S. Government.

9. Attachments

9.1 Attachment A: Scope of Work for Services or Technical Specifications

BACKGROUND

The Critical Infrastructure Digitalization and Resilience (CIDR) program is a five-year program funded by the United States Agency for International Development (USAID) and implemented by DAI Global LLC (DAI). The CIDR program supports the governments of countries within USAID's Europe and Eurasia (E&E) portfolio in assisting critical infrastructure entities to: incorporate cybersecurity best practices into organizational operations, planning, and procurement; prioritize cybersecurity investment needs; select appropriate mandatory or voluntary standards and corresponding security controls; and establish the basis for region-wide cybersecurity information sharing.

The Offeror will support the Ministry of Agriculture, Forestry, and Water Economy to improve their cybersecurity and increase resilience to cyberattacks by (1) conducting a GAP and Vulnerability Analysis and Risk Assessment and (2) implementing an Information Security Management System at the MoA that would be in line with the international standard for information security ISO 27001:2022. The Offeror will also identify and carry out capacity building technical assistance activities to strengthen cyber hygiene and institutionalize cybersecurity best practices.

OBJECTIVES

The Offeror will support the CIDR program by conducting the GAP analysis and risk assessments as well as leading the implementation of an Information Security Management System at the MoA, including providing long-term (two years in total) advisory support to MoA for the implementation and usage of ISO 27001 as an international standard to manage information security in the organization. This activity will ensure a risk-based approach to cybersecurity.

TASKS

The Offeror is anticipated to support the following tasks outlined below:

	Description of tasks	Description of Outputs and Duration
1	GAP Analysis	Approx. two months
1.1	GAP Security Assessment with maturity level	GAP Assessment with maturity level
1.2	Development of detailed roadmap to ISMS implementation	Detailed roadmap that includes descriptions of key projects and technologies for envisaged security architecture
2	Risk Analysis	Approx. four months, and review after approximately one year

2.1	Asset inventory and classification	Registers of Assets with classification (Asset inventory to be conducted initially and once more as a review after approximately one year)
2.2	Assessment of technical infrastructure	Report on technical vulnerabilities and misconfigurations (Assessment of technical infrastructure to be conducted initially and once more as a review after approximately one year)
2.3	Vulnerability Risk Assessment	Vulnerability Risk Assessment and findings report to be conducted initially within the first two months and once more as a review after approximately one year.
2.4	Risk treatment plan	<p>Risk Treatment plan with identified critical and urgent needs for improvements in equipment, network, and services, including:</p> <ul style="list-style-type: none"> • Detailed proposal with technical specifications for services and equipment that may be purchased. • Develop proposal for qualitative conditions to ensure trusted and reliable vendors and suppliers are being used. • List of necessary ICT specialist profiles (or managed outsourced services) for procured equipment installation and running over the two-year period. • Review and proposal for improvements in the organizational structure of the MoA related to cybersecurity to ensure that ICT and cybersecurity issues, needs and incidents are adequately and timely identified, handled, and reported to the senior management. <p><i>It is expected that the Offeror, as part of this task, will conduct thorough research and take into account external sources, including reports and other documents related to the cybersecurity of the organization as well as meetings with current technical support providers.</i></p> <p>(Risk treatment plan as part of repeating activity included in the ISMS is to be conducted initially and once more as a review after approximately one year)</p>
3	Information Security Management System Implementation	Approx. five months, and review approximately after one year

3.1	Statement of applicability	Development of Statement of applicability document, to be reviewed after approximately one year as part of the annual review process.
3.2	Creation of Security policies	Creation of security Policies, including but not limited to: policies on Information Security, Data Protection, Data Retention, Asset Management, Information Classification and Handling, Information Security Awareness and Training, Access Control, Risk Management, Incident Response, Acceptable Use, Physical Security, Remote Working, Clear Desk and Screen, Backup, Business Continuity, Change Management, Antivirus and Malware, Third Party Security Monitoring and Logging, Continuous Improvement, Network Security, as well as others applicable to the organization and scope of work.
3.3	Creation of Security Procedures	<p>Security Procedures, including Management Procedure on the termination or change of employment, as well as at minimum the following procedures on: awareness of users against malicious code, management of removable media, disposal of media, handling and storage of information, exchange of information, protecting information related to the interconnection of business information systems, monitoring the use of the system, registration of users, safe use of mobile computing and communications, teleworking, Cryptographic Key Management, change control, Incident Management, identifying legal, regulatory and contractual requirements</p> <p>Initial creation of security procedures, followed by a review after approximately one year as part of the annual review process.</p>
3.4	Implementation of controls	Initial implementation of controls and review after approximately one year as part of the annual review process.
3.5	Business continuity plans	<p>Development of Business Continuity Plans and Disaster Recovery Plans that should be adjusted to the organization's unique , operational environment, and risk profile.</p> <p>Business continuity plans should include at minimum the following activities and deliverables: Business Impact Analysis (BIA), Risk Assessment and Management, Business Continuity Strategy, Business Continuity Plans.</p> <p>BCP to be developed initially and reviewed after approximately one year as part of the annual review process.</p>
3.6	Improvement mechanisms	KPI Indicators, Audit report

		Initial activity to be reviewed after approximately one year as part of the annual review process.
3.7	Management review	<p>Management review report</p> <p>Initial activity to be reviewed after approximately one year as part of the annual review process.</p>
4	Capacity Building Trainings	Approx. three months
4.1	Provision of capacity building training(s) for selected groups.	<p>Trainings should be geared toward the following groups at minimum: Risk owners, Business continuity team, Disaster Recovery, owners of documented policies and procedures, Incident Management, Unit Managers, Asset owners, Internal Auditors, and Change Managers.</p> <p>Offerors should include official training for two staff members at the beneficiary agency for ISO 27001 Implementer, and two staff members for ISO 27001 Auditor, with at least one included certification attempt per participant included in the price.</p>
4.2	Cybersecurity awareness training for MoA employees	<p>Topics for the trainings should cover at minimum the following:</p> <ul style="list-style-type: none"> • Security Policy • The use of passwords • Protection against viruses • The proper use of the Internet • The risks associated with E-mail (spam, phishing, malicious code) • The backup and storage of data • Social engineering (phishing) • Managing Security Incidents • Using encryption • The security of laptops and PDAs • The use of private files/systems at work • Respect for intellectual property • Problems related to access control • The individual role and responsibilities

9.2 Attachment B: Proposal Cover Letter

[On Firm's Letterhead]

<Insert date>

TO: Click here to enter text.
Development Alternatives, Inc.

We, the undersigned, provide the attached proposal in accordance with **RFP**-Click here to enter text.-Click here to enter text. issued on Click here to enter text.. Our attached proposal is for the total price of <Sum in Words (\$0.00 Sum in Figures) >. I certify a validity period of Click here to enter text. days for the prices provided in the attached Price Schedule/Bill of Quantities. Our proposal shall be binding upon us subject to the modifications resulting from any discussions.

Offeror shall verify here the items specified in this RFP document.

We understand that DAI is not bound to accept any proposal it receives.

Yours sincerely,

Authorized Signature:

Name and Title of Signatory: Click here to enter text.

Name of Firm: Click here to enter text.

Address: Click here to enter text.

Telephone: Click here to enter text.

Email: Click here to enter text.

Company Seal/Stamp:

9.3 **Attachment C: Price Schedule**

Please contact CIDR_Procurement@dai.com to request a copy of the Firm Fixed Price budget template.

9.4 Attachment D: Instructions for Obtaining a Unique Entity ID (SAM) Number - DAI'S Vendors, Subcontractors

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

Note: There is a Mandatory Requirement for your Organization to Provide an 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 an 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 an 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 an 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 an Unique Entity ID (SAM) to DAI. Organizations who fail to provide an 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 an 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

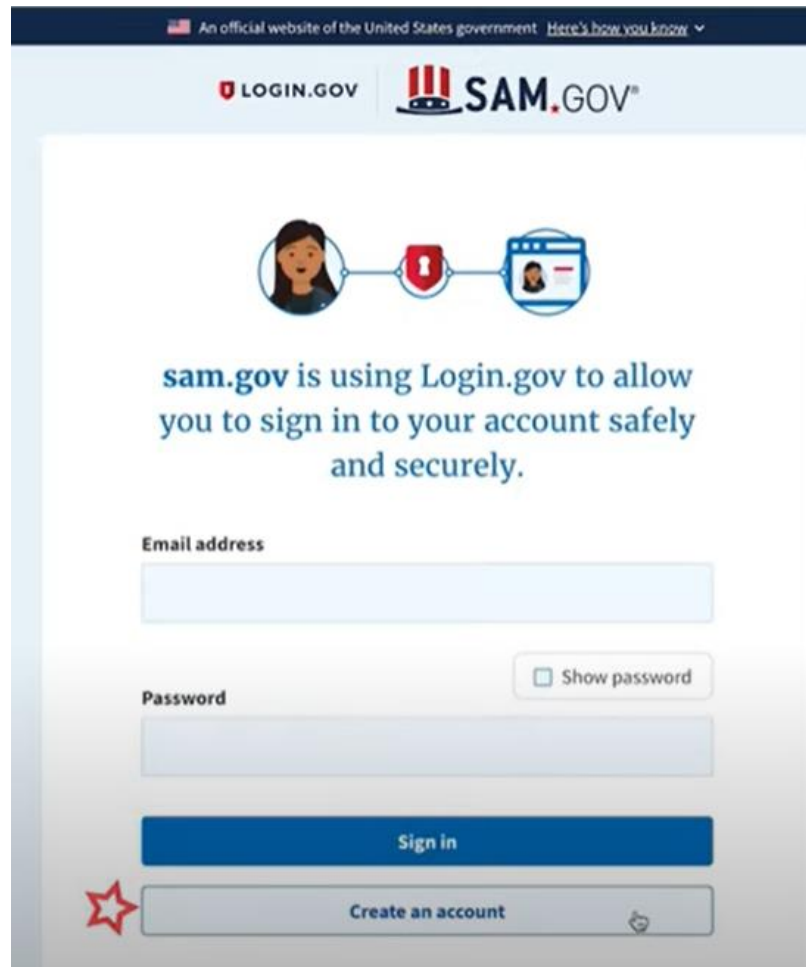
The Data Universal Numbering System (DUNS) is a system developed and managed by Dun and Bradstreet that assigns a unique nine-digit identifier to a business entity. It is a common standard world-wide and was previously used by the U.S. Government to assign unique entity identifiers. This system was retired 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 begin on the next page.

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

1. 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”



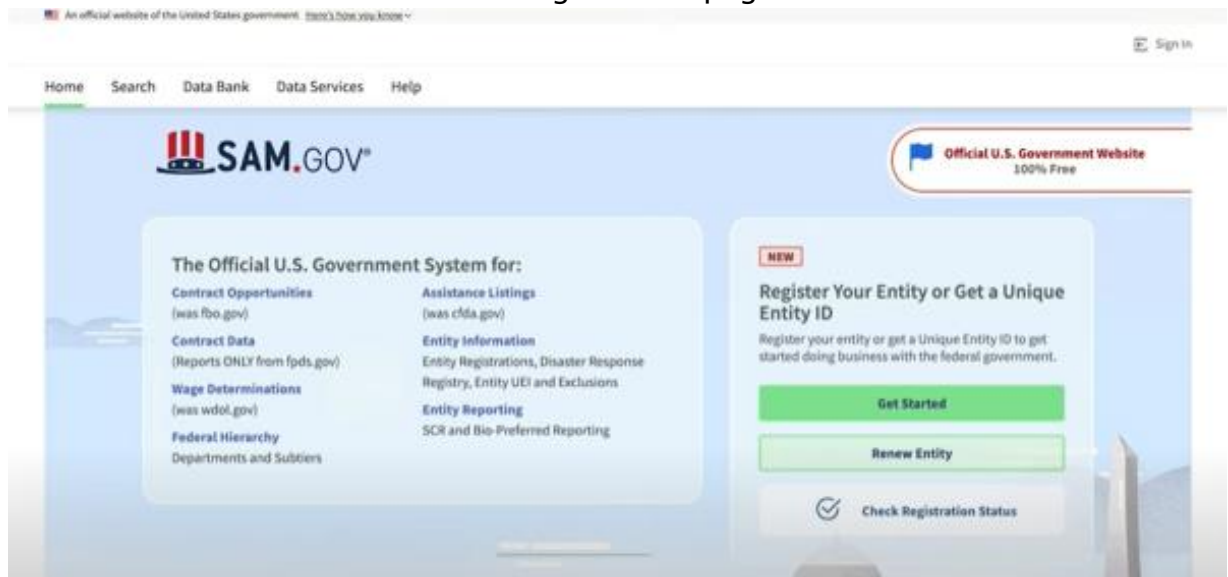
3. Choose Account Type:
 - a. Create an Individual User Account to perform tasks such as register/update your entity, create and manage exclusion records or to view FOUO level data for entity records.
 - b. Create a System User Account if you need system-to-system communication or if performing data 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.

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

SAM.GOV

Requests Notifications Workspace Sign Out

Home Search Data Bank Data Services Help

Getting Started with Registration

This the official U.S. government website for entity registration. Entity registration is FREE.

Entity Information Home

Before You Get Started

Before you start your registration, there are a few steps you must complete first. Review these steps to help ensure you set aside enough time to complete your registration.

- 1 Request a DUNS Number
- 2 Prepare Your Data
- 3 Get a Login.gov Account
- 4 Submit and Finish

1 Request a DUNS Number

All entities wishing to do business with the federal government must have a unique entity identifier (UEI). Currently, the DUNS number, which is a unique nine-character identification number provided by Dun & Bradstreet (D&B) free of charge, is the official UEI. D&B assigns UEI (DUNS) for each physical location of a business. Requesting a UEI (DUNS) takes about 10 minutes. Receiving a UEI (DUNS) takes 1-2 business days (under normal circumstances) when using the D&B web form.

[Go to D&B web form](#)

NEW

Register Your Entity or Get a Unique Entity ID

Register your entity or get a Unique Entity ID to get started doing business with the federal government.

Get Started

Renew Entity

Check Registration Status

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

Entity Management

Get Started

Register Entity

An entity registration allows you to bid on government contracts and apply for federal assistance. As part of entity registration, we will assign you a Unique Entity ID (SAM).

Comprehensive and current entity information is an essential part of the federal award process. It is important to prepare your information and allow sufficient time to understand and accurately complete your registration. You only need to complete and manage it here to remain eligible for federal awards.

You must renew your registration every 365 days for it to remain active.

Register Entity

Get Unique Entity ID (SAM)

If you only conduct certain types of transactions, such as reporting as a sub-awardee, you may not need to complete an entity registration. Your entity may only need a Unique Entity Identifier.

You can get a Unique Entity ID (SAM) for your organization without having to complete a full entity registration.

Get Unique Entity ID

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.

Workspace

Entity Management

What do I need for registration?

[Get Started](#)

Entity Registration



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

Unique Entity ID



System Accounts



Profile



John Doe
john.doe@gsa.gov



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 ▼

GSA

9.5 Attachment E: 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.

9.6 Attachment F: Past Performance Form

Include projects that best illustrate your work experience relevant to this RFP, sorted by decreasing order of completion date.

Projects should have been undertaken in the past three years. Projects undertaken in the past six years may be taken into consideration at the discretion of the evaluation committee.

#	Project Title	Description of Activities	Location Province/ District	Client Name/Tel No	Cost in US\$	Start-End Dates	Completed on schedule (Yes/No)	Completion Letter Received? (Yes/No)	Type of Agreement, Subcontract, Grant, PO (fixed price, cost reimbursable)
1									
2									
3									
4									
5									

9.7 Attachment G: Representations and Certifications of Compliance

1. Federal Excluded Parties List - The Bidder Select is not presently debarred, suspended, or determined ineligible for an award of a contract by any Federal agency.
2. Executive Compensation Certification- FAR 52.204-10 requires DAI, as prime contractor of U.S. federal government contracts, to report compensation levels of the five most highly compensated subcontractor executives to the Federal Funding Accountability and Transparency Act Sub-Award Report System (FSRS)
3. Executive Order on Terrorism Financing- The Contractor is reminded that U.S. Executive Orders and U.S. law prohibits transactions with, and the provision of resources and support to, individuals and organizations associated with terrorism. It is the legal responsibility of the Contractor/Recipient to ensure compliance with these Executive Orders and laws. Recipients may not engage with, or provide resources or support to, individuals and organizations associated with terrorism. No support or resources may be provided to individuals or entities that appear on the Specially Designated Nationals and Blocked persons List maintained by the US Treasury (online at www.SAM.gov) or the United Nations Security Designation List (online at: http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml). This provision must be included in all subcontracts/sub awards issued under this Contract.
4. Trafficking of Persons – The Contractor may not traffic in persons (as defined in the Protocol to Prevent, Suppress, and Punish Trafficking of persons, especially Women and Children, supplementing the UN Convention against Transnational Organized Crime), procure commercial sex, and use forced labor during the period of this award.
5. Certification and Disclosure Regarding Payment to Influence Certain Federal Transactions – The Bidder certifies that it currently is and will remain in compliance with FAR 52.203-11, Certification and Disclosure Regarding Payment to Influence Certain Federal Transactions.
6. Organizational Conflict of Interest – The Bidder certifies that will comply FAR Part 9.5, Organizational Conflict of Interest. The Bidder certifies that is not aware of any information bearing on the existence of any potential organizational conflict of interest. The Bidder further certifies that if the Bidder becomes aware of information bearing on whether a potential conflict may exist, that Bidder shall immediately provide DAI with a disclosure statement describing this information.
7. Prohibition of Segregated Facilities - The Bidder certifies that it is compliant with FAR 52.222-21, Prohibition of Segregated Facilities.
8. Equal Opportunity – The Bidder certifies that it does not discriminate against any employee or applicant for employment because of age, sex, religion, handicap, race, creed, color or national origin.
9. Labor Laws – The Bidder certifies that it is in compliance with all labor laws.
10. Federal Acquisition Regulation (FAR) – The Bidder certifies that it is familiar with the Federal Acquisition Regulation (FAR) and is in not in violation of any certifications required in the applicable clauses of the FAR, including but not limited to certifications regarding lobbying, kickbacks, equal employment opportunity, affirmation action, and payments to influence Federal transactions.
11. Employee Compliance – The Bidder warrants that it will require all employees, entities and individuals providing services in connection with the performance of an DAI Purchase Order to comply with the provisions of the resulting Purchase Order and with all Federal, State, and local laws and regulations in connection with the work associated therein.

By submitting a proposal, offerors agree to fully comply with the terms and conditions above and all applicable U.S. federal government clauses included herein, and will be asked to sign these Representations and Certifications upon award.

List of Optional Attachments

9.8 Attachment H: Proposal Checklist

Offeror: _____

Have you?

☐ Submitted your proposal to DAI electronically to CIDR_Procurement@dai.com as specified in General Instructions above?

Does your proposal include the following?

- ☐ Signed Cover Letter (*use template in Attachment B*)
- ☐ Separate Technical and Cost proposals labeled as Volume I and Volume II respectfully.
- ☐ Proposal of the Product or Service that meets the technical requirements as per Attachment A
- ☐ Response to each of the evaluation criteria
- ☐ Documents use to determine Responsibility
- ☐ Evidence of a Unique Entity ID (SAM)OR Self Certification for Exemption from Unique Entity ID (SAM)Requirement
- ☐ Past Performance (*use template in Attachment F*)