



Critical Infrastructure Digitization and Resilience (CIDR) Program

Request For Proposals (RFP)

No. REQ-BET-23-0080

Kosovo: Cybersecurity Rapid Incident Response Services

Issue Date: September 1, 2023

WARNING: Prospective Offerors who have received this document from a source other than DAI 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. Any amendments to this solicitation will be issued and posted on DAI's website and Devex and Offerors are encouraged to check these websites periodically.

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	8
4.1 Cost/Price Proposals.....	8
5. Basis of Award	8
5.1 Best Value Determination	8
5.2 Responsibility Determination.....	8
6. Inspection & Acceptance.....	9
7. Compliance with Terms and Conditions	9
7.1 General Terms and Conditions	9
7.2 Prohibited Technology	9
8.3 Source and Nationality.....	9
8.4 Unique Entity ID (SAM)	10
8. Anti-Corruption and Anti-Bribery Policy and Reporting Responsibilities	10
9. Attachments.....	12
9.1 Attachment A: Scope of Work for Services or Technical Specifications.....	12
9.2 Attachment B: Proposal Cover Letter	14
9.3 Attachment C: Price Schedule for Firm Fixed Price	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.....	26
9.7 Attachment G: Representations and Certifications of Compliance	27
List of Optional Attachments.....	28
9.8 Attachment H: Proposal Checklist.....	28

Synopsis of the RFP

RFP No.	REQ-BET-23-0080
Issue Date	Friday, September 1, 2023
Title	Kosovo: Cybersecurity Rapid Incident Response Services
Issuing Office & Email Address for Submission of Proposals	Issuing Office: DAI Global LLC All proposals must be submitted electronically to: CIDR_Procurement@dai.com
Deadline for Receipt of Questions	5:00pm EST on Friday, September 8, 2023
Deadline for Receipt of Proposals	5:00pm EST on Friday, September 22, 2023
Point of Contact	CIDR_Procurement@dai.com
Anticipated Award Type	Cost Reimbursable
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 Critical Infrastructure Digitization and Resilience (CIDR) program, invites qualified offerors to submit proposals to provide the services listed in Attachment A: Scope of Work. Specifically, DAI seeks offerors to provide bids for cybersecurity rapid incident response services to Government of Kosovo stakeholders, either remotely or on-site, with travel requirements being determined by the nature of the incident.

The successful service provider must meet the following qualifications:

- a. Have a proven track record of providing on-demand reactive cybersecurity incident response, and recovery services to essential service providers or critical infrastructure operators.
- b. Have a team of experienced cybersecurity professionals with expertise in incident response, remediation, and recovery.
- c. Have a robust incident response plan and playbook, preferably based on CISA Cybersecurity Incident & Vulnerability Response Playbook.¹
- d. Have the ability to deploy resources quickly and efficiently.

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 Cost Reimbursable contract. Under this contractual arrangement, CIDR will reimburse the selected service provider for all eligible and documented costs incurred in the delivery of the on-demand reactive crisis response and recovery services. These costs may include direct labor and travel expenses (if any), and other reasonable and necessary expenditures directly related to the execution of the contract. This subcontract type is subject to change during the course of negotiations.

A Cost Reimbursable Subcontract is: An award where the subcontractor is reimbursed for actual reasonable, allowable, and allocable costs up to a maximum ceiling value of the subcontract agreement.

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

¹https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

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**, and must be submitted electronically to CIDR_Procurement@dai.com. 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 non-responsive 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 by the deadline of 5:00pm EST on Friday, September 8, 2023 as specified in the Synopsis above. No questions will be answered by phone. Any verbal information received from a DAI staff member 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 submitted separately from cost/price proposals and shall be clearly labeled as "VOLUME I: TECHNICAL PROPOSAL".

Technical proposals shall include the following contents:

- Cover Letter:** See Attachment B: Proposal Cover Letter for instructions.
- Executive Summary:** A concise overview of the proposed approach, team composition, and key qualifications.
- Technical Approach:** The proposal should include a detailed explanation of the methodologies, tools, and techniques that will be utilized to address the objectives outlined in Attachment A: Scope of Work. Furthermore, the technical approach should include the following:
 - **Service Level Agreement (SLA):** The technical approach should include a comprehensive Service Level Agreement (SLA) that outlines the specific service commitments and performance expectations, and response time between the service provider and the

beneficiary entities. Offerors should include their own SLA templates. Also, the SLA should address data confidentiality, non-disclosure and security, and any service guarantees or penalties for non-compliance with the agreed-upon service levels.

- **Rules of engagement:** The technical approach should incorporate rules of engagement, clearly specifying the roles and responsibilities of both the service provider and the beneficiary team, as well as procedures for communication, information sharing, and collaboration during incident response activities. Offerors should include their own Rules of Engagement template. In the case of engagement activities with the Government of Kosovo, the provider should take into consideration the rules set in MIA/AIS Administrative Instruction No. 02/2010 for Information Security Management.²
 - **Incident Response Plan and Playbook:** The technical approach should include an incident response plan and playbook, preferably based on CISA Cybersecurity Incident & Vulnerability Response Playbook.
- d. **Management Approach (Team composition and qualifications).** The proposal should include a team with a well-rounded composition of expertise and roles that will effectively perform the required services. The team composition needs to be supported with documentation of the team's relevant experience (CVs), certifications, and expertise in incident response, cybersecurity, and critical infrastructure protection.
- e. **Past Performance:** At least three professional references highlighting capabilities and performance in similar engagements from the last five years.

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 more important than cost/price factors.

Evaluation Criteria	Evaluation Sub-criteria (if needed)	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 local support and		40 points

² <https://mpb.rks-gov.net/ap/desk/inc/media/F189A604-27A2-402A-A8DC-484EFF75F11F.pdf>

<p>stakeholders that will need to be involved and a clear plan for engaging them?</p> <p>-Does the proposal include a detailed Gantt chart that clearly outlines a timeline for proposed steps to accomplish the activity?</p> <p>-Does the proposal include the requested Service Level Agreement and Rules of Engagement?</p>		
<p>Management Approach:</p> <p>-Does the organization have sufficiently qualified staff who can undertake the scope of work?</p> <p>-Does the proposed approach fulfill the requirements of executing the scope of work in a timely and efficient manner?</p>		20 points
<p>Past Performance:</p> <p>-Does the organization have a track record of successfully conducting cybersecurity rapid incident response activities?</p> <p>Are three examples included of cybersecurity rapid incident response contracts?</p>		40 points
Total Points		100 points

4. Instructions for the Preparation of Cost/Price Proposals

4.1 Cost/Price Proposals

Cost/Price proposals shall be submitted separately from technical proposals and shall be clearly labeled as “VOLUME II: COST/PRICE PROPOSAL”.

The *anticipated* budget ceiling for this award is **\$180,000.00**. Please contact the CIDR Procurement team at CIDR_Procurement@dai.com for a copy of the template.

1. **Budget:** Offerors shall complete a detailed budget including as much information as possible, including labor costs, travel costs, indirect costs, and other associated costs with proposed activities.
2. **Budget Notes:** Detailed budget notes must accompany the cost proposal. These notes should explain each cost included in the budget and can be in the form of a Word document or as a tab included in the Excel budget template.
3. **VAT:** It is important to note that *if applicable*, Value Added Tax (VAT) shall be included on a separate line. These services are eligible for VAT exemption for Kosovo-based companies under the DAI prime contract. **For those companies based in Kosovo or with subsidiaries in Kosovo, the budget ceiling of \$180,000 is exclusive of VAT. For companies based outside of Kosovo or for those without subsidiaries in Kosovo, the ceiling is inclusive of VAT, if applicable.** The Subcontractor 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. Consortiums can submit proposals in response to this solicitation, but all members of the consortium must be in compliance with the requirements in the RFP, including source and nationality requirements in section 8.3.

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. We request Offerors to comply with the terms of source and nationality requirements as stated in the RFP.

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

DAI must verify the source and nationality of goods and services and ensure (to the fullest extent possible) that DAI does not procure any goods or services from prohibited countries listed by the Office of Foreign Assets Control (OFAC) as sanctioned countries. OFAC sanctioned countries may be searched within the System for Award Management (SAM) at www.SAM.gov. The current list of countries under comprehensive sanctions include: Cuba, Iran, North Korea, Sudan, and Syria. Goods may not transit through or be assembled in comprehensive sanctioned origin or nationality countries nor can the vendor be owned or controlled by a prohibited country. DAI is prohibited from facilitating any transaction by a third party if that transaction would be prohibited if performed by DAI.

By submitting a proposal in response to this RFP, Offerors confirm that they are not violating the Source and Nationality requirements of the goods or services being offered and that the goods and services comply with the Geographic Code and the exclusions for prohibited countries outlined above.

8.4 Unique Entity ID (SAM)

There is a **mandatory** requirement for your organization to provide a Unique Entity ID (SAM) to DAI. Without a 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 a 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 a Unique Entity ID (SAM) prior to signing of the agreement. Offerors can submit a proposal without a Unique Entity ID, but this number must be obtained before an agreement can be signed. 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 a Unique Entity ID (SAM), see Attachment D - Instructions for Obtaining a 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 hotline@usaid.gov.

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

Kosovo: Cybersecurity Rapid Incident Response Services

A. BACKGROUND AND JUSTIFICATION

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.

B. OBJECTIVES

CIDR is seeking services from qualified service providers of reactive crisis response and compromise recovery to support the Government of Kosovo with priority assistance requests to address potential cybersecurity incidents that could pose threats to its essential services. Key stakeholders include, but are not limited to, the Cybersecurity Agency (CSA) and other CSA constituents such as Operators of essential services and Digital service providers.

The selected service provider will be responsible for providing immediate, remote or on-site assistance (as determined by the nature of the incident) and technical expertise in rapidly diagnosing, remediating, and recovering from cybersecurity incidents/attacks.

C. SCOPE OF WORK

This Scope of Work outlines requirements for the provision of on-demand reactive cybersecurity incident response and recovery services within the designated timeframe of **October 1, 2023, to September 31, 2024**. During this period, the selected service provider will collaborate closely with the CIDR Kosovo team and the Government of Kosovo's point of contact (POC) to address cybersecurity incidents/attacks. The service provider's expertise demonstrated through their technical proficiency, extensive experience, and adherence to industry best practices, will play a crucial role in ensuring effective triage, diagnosis, remediation, and recovery in the event of cybersecurity incidents. Please note that language requirements for communication during field work and reporting include English and Albanian.

On-demand acknowledgement by and engagement of the service provider should commence no more than a maximum of three (3) hours counted from the moment when the request has been sent by the CIDR Kosovo Team, regardless of whether the incident requires remote or on-site support. The service provider must enable redundant communication channels with the CIDR Kosovo team, and an online helpdesk or a ticketing system is required.

For high-level trust, the service provider is obligated to sign a non-disclosure agreement related to the victim organization prior to starting with any activity. Victim organizations will mandatorily sign consent forms and official request letters prior to CIDR activation the rapid response mechanism. CIDR will make these rules known and available to all parties involved.

Cybersecurity Rapid Incident Response Services

1. **Conduct Initial Triage:** Upon request from the POC, confirm the incident and type, providing an initial assessment of the severity and impact of cyber incidents or events affecting essential services, leading to a comprehensive understanding of the incident's nature and potential consequences.
2. **Rapid Technical Diagnostic:** In close coordination with the POC, the service provider will support the affected critical infrastructure entity teams to perform a thorough and expedited technical analysis to identify the root cause, extent, and potential vulnerabilities associated with the incident, ensuring attacker containment and rapid and accurate response.
3. **Recovery:** The service provider will offer actionable technical advice to enable prompt remediation and recovery efforts, considering the specific needs and context of the incident and removing attacker control from the affected environment, regaining administrative control, and hardening controls to prevent future breaches.

It is possible to use proprietary technology stack during remote incident response, as long as technologies are **not** from prohibited countries and/or prohibited technologies) and explicit prior consent **must** be obtained in writing from the beneficiary.

When handling sensitive information, the selected Offeror is required to adhere strictly to Kosovo's laws (Such as:: <https://gzk.rks-gov.net/ActDetail.aspx?ActID=18616> - Law on Protection of Personal Data). Before transferring any data, explicit consent must be obtained from the beneficiary.

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: Budget Template

Please contact CIDR_Procurement@dai.com for a copy of the DAI cost reimbursable budget template.

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

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 A 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 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 A UNIQUE ENTITY ID IS OUTLINED BELOW:

1. Have the following information ready to request a 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®

Illustration showing a person icon connected to a shield icon, which is connected to a computer monitor icon.

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

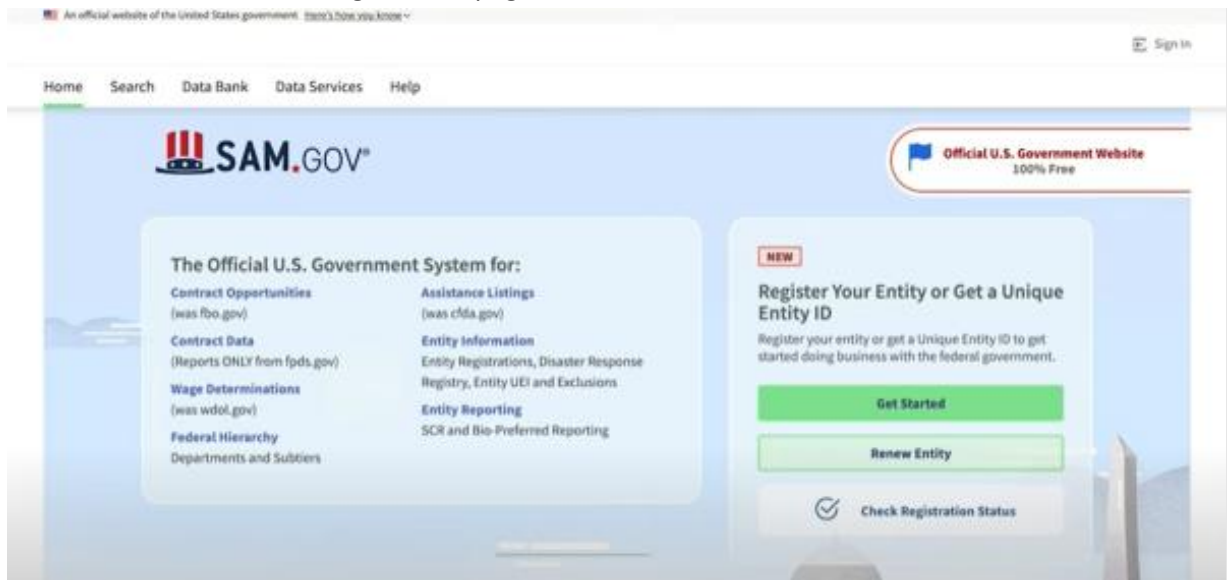
Create an account

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.”

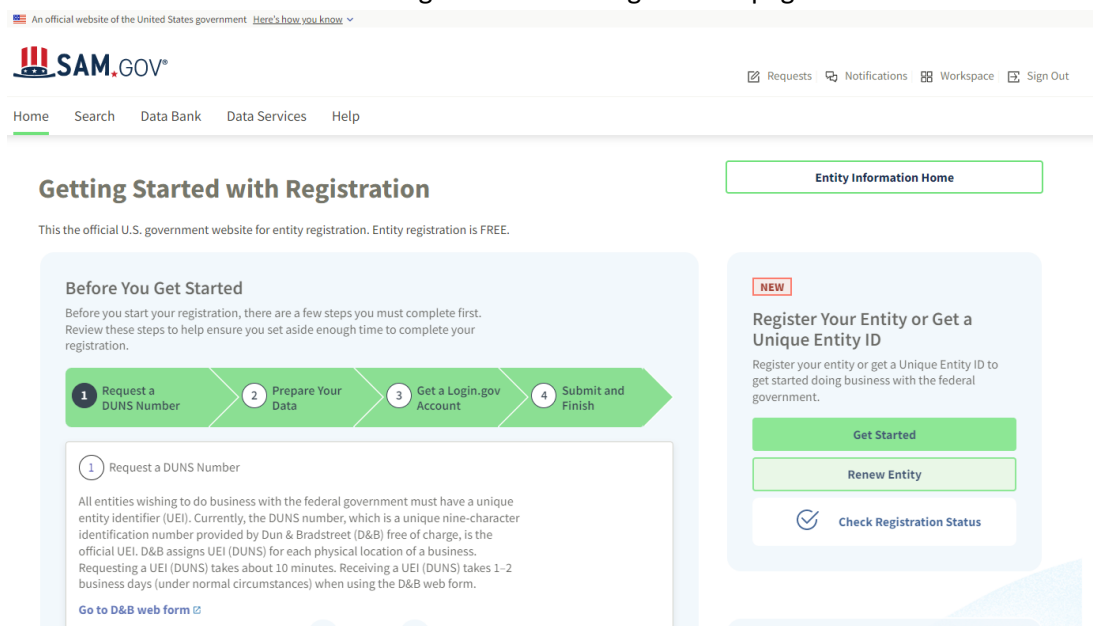
4. Click “DONE” on the confirmation page. You will receive an email confirming you have created a user account in SAM.
5. Click the validation link in the email that contains the activation code within 48 hours to activate your user account. If the email link is not hyperlinked (i.e., underlined or appearing 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.

< 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).



8. When you are ready, select "Next"
9. Once validation is completed, select "Request UEI" to be assigned a 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.

1

2

3

4

Enter Entity Information

Validate Information

Request UEI

Receive UEI

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 DUNS Requirement For Subawardees 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 a DUNS number, as the gross income received from all sources in the previous tax year is under USD \$300,000.

***By submitting this certification, the certifier attests to the accuracy of the representations and certifications contained herein. The certifier understands that s/he and/or the subawardee/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 or Subcontract
1									
2									
3									
4									
5									

9.6 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

9.7 Attachment H: Proposal Checklist

Offeror: _____

Have you?

☐ Submitted your proposal to DAI to the electronic address as specified in General Instructions?

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 included that are used 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*)