Opportunity Details

Notice ID	Related Notice	Active/Inactive
FA8600-23-S-C056-0003		**Active**
Notice Status	Department/Ind. Agency	Sub-Tier
Published	**DEPT OF DEFENSE**	**DEPT OF THE AIR FORCE**
Office		
FA8600 AFLCMC PK		

Looking for contract opportunity help?

APEX Accelerators are an official government contracting resource for small businesses. Find your local APEX Accelerator for free government expertise related to contract opportunities.

APEX Accelerators are funded in part through a cooperative agreement with the Department of Defense.

The APEX Accelerators program was formerly known as the Procurement Technical Assistance Program (PTAP).

General Information

Contract Opportunity Type	Updated Published Date
Combined Synopsis/Solicitation (Updated)	**Dec 01, 2023 03:57 PM**
Date Offers Due	Inactive Policy
Jan 12, 2024 05:00 PM EST	**15 days after response/Contract Award Date**
Inactive Date	Initiative
Jan 27, 2024	**None**
Allow Vendors to Add/remove from Interested Vendors List	Allow Vendors to View Interested Vendors List
Yes	**No**

Classification

Original Set Aside	Product Service Code
	R702-SUPPORT- MANAGEMENT: DATA COLLECTION
Place of Performance	
, USA	

NAICS Code(s)

NAICS Code	NAICS Definition
518210	Computing Infrastructure Providers, Data Processing, Web Hosting, and Related Services

Description

Number: FA8600-23-S-C056

Commercial Solutions Opening Type: This is the initial announcement under Call 3. This will be a Two-Step Call solicitation.

NOTE: Word Copy of the Final Call is attached to this announcement. There are formatting limitations within SAM.gov. In the event there is a discrepancy between this posting and the attached word document, the word document shall control.

First Step: WHITE PAPER DUE DATE AND TIME: White Papers will be accepted until 12 January 2024 at 1700 ET. White Papers may be submitted at any time during this period. White Papers received after specified date and time will be considered late in accordance with FAR 52.212-1(f). Interested Vendors can submit clarifying questions to AFLCMC by 7 December 2023. AFLCMC will publish all received questions and AFLCMC's responses (anticipated 13 December 2023) prior to the White Paper submission date. All submissions (questions and white papers) shall be made to the designated Submission POCs below.

Second Step: PROPOSAL DUE DATE AND TIME: In accordance with this Call, AFLCMC will down select vendors from the first step to submit a Step 2 proposal. Proposal due date and time will be provided in a separately issued Requests for Proposal (RFPs) sent to offers that submit a Solution Brief and Pricing Proposal that meet or exceed evaluation criteria contained in this Call.

Submission POC: White Papers must be submitted via email to the Contracting Points of Contact (POCs):
Contracting Officer Name: Neal Duiker
Email: neal.duiker@us.af.mil
Contract Specialist Name: Kimberly Conley
Email: kimberly.conley.3@us.af.mil
 FULL TEXT – CALL 3
(Project Vulcan Forge)

    1. Overview

This Commercial Services Opening (CSO) Call is intended to be as streamlined as possible to allow for the exploration of modern solutions to support a variety of critical national security systems. Air Force Life Cycle Management Center (AFLCMC) invites vendors to submit innovative and novel technical solutions which address all aspects of Digital Infrastructure (DI), focusing on the user story focus areas below. This requires delivering an enduring, secure, robust, efficient, responsive, agile, elastic and extensible DI solution spanning all classification levels.

Many AFLCMC projects operate in varying classification environments, including highly classified environments (collateral, Sensitive Compartmentalized Information, and Special Access Program). Though some DI Focus Areas may require unclassified work, respondents should be aware that to be eligible for any contract/instrument award, vendors must be cleared to work, or have the ability to be cleared to work, in highly classified environments. If vendor intends to perform classified work at their facility (or subcontractor or sub-awardee's facility), they will need to provide a Facility Accreditation Letter (FAL) for each facility to the Contracting Officer/Agreements Officer by no later than (NLT) contract award (anticipated March 2024).

 This CSO Call may result in the award of a FAR-based contract, an Other Transaction Agreement (OTA) under 10 USC 4021, or an Other Transaction for Prototype Project pursuant to 10 USC 4022. AFLCMC intends to follow the processes identified in the Data Operations CSO unless otherwise noted or annotated in this Call. AFLCMC is not obligated to make any awards as a result of this Call and all awards are explicitly subject to the availability of funds and successful negotiations. The Government is not responsible for any monies expended by any vendor prior to

<u>the issuance of any awarded contract/agreement.</u>

AFLCMC reserves the right to modify the solicitation requirements of this CSO Call at its' sole discretion.

_____

1. Digital Infrastructure (DI) Technology Focus Areas

1. General Information: AFLCMC designed an Azure cloud-based software DevSecOps environment supporting multiple USAF programs (hereafter referred to as Crucible). The Crucible environment contains cloud resources at the IL5 (Controlled Unclassified Information), IL6 (Secret) and IL6+(Secret Special Access Program) classifications. Enrolled USAF programs work within separate, segregated enclaves with multiple security enclaves (ex. Program A has its own IL5, IL6 and IL6+ environment separate from Program B's enclaves). Further, Programs access the Crucible environment from varying USAF networks. AFLCMC designed the Crucible environment to permit future USAF programs not currently enrolled to access and establish enclaves to meet specific mission needs. When new programs enroll, the Crucible environment may need to peer to a new network. Therefore, Crucible requires sufficient security controls and artifacts to obtain an authority to operate (ATO). AFLCMC is seeking innovative and novel technical solutions focusing on the four user stories/focus areas described in paragraphs B, C, D, and E below.

2. User Story 1 – Personnel and Environmental Onboarding:

User Story: Currently, Crucible relies on a personnel heavy onboarding process that requires existing access to Crucible environments. There are approximately six hundred (600) users currently enrolled within the Crucible environment. AFLCMC intends to scale enrollment to one thousand (1,500-2,000) users within twelve (12) months. The existing onboarding process is personnel heavy with significant manual processes resulting in a lengthy and inefficient use of resources. Further, the existing onboarding processes are not sufficiently documented nor easily accessible in all of Crucible's various enclaves. AFLCMC's limited onboarding resources waste precious time re-inventing onboarding processes or searching within environments leading to weeks/months delays (hereafter Personnel Onboarding). AFLCMC needs an automated process compatible within all Crucible environments. Onboarding challenges include properly setting up personnel with Azure Virtual Desktops with varying features and digital resources (hereafter Environment Onboarding). This process is also personnel intensive and inefficient. Furthermore, AFLCMC struggles to estimate costs associated with personnel and environment onboarding. These costs are billed to enrolling programs. Given the inconsistencies, delays and inefficiencies, cost estimates lack fidelity and significant unexpected charges.

Outcomes Desired: AFLCMC seeks an automated Personnel and Environment Onboarding process improving on all user pain points articulated above. Designed process must work in all Crucible enclaves at all classification levels and expedites onboarding for new users to, at maximum, a week with a goal of a day. The Personnel and Environmental Onboarding processes must be sufficiently robust to address common onboarding needs while simultaneously eliminating "one off" processes. Solutions must be designed to integrate with existing platform software identified in the attached Addendum. Further, onboarding workflow shall include high-fidelity pricing estimates so enrolling programs can properly estimate and commit funds. This onboarding process will be user initiated and provide clear pricing guidelines that accurately reflect projected costs to within +/- 10% per user. Without sacrificing flexibility, the Crucible onboarding process will offer several default environment offerings for all users intended to meet the needs of 90-95% of all users. Standard Environment Onboard offerings shall easily offer CPU and GPU compute, personal and shared storage up to 100 TB, access to Atlassian products (Jira, Confluence, Bitbucket, etc.), a variety of software solutions (Microsoft Office, Visual Studio, Python, Java, Adobe, etc.), operating systems (Windows, Linux, macOS), and access (Azure Virtual Desktops or Kubernetes). The onboarding process should be executed through automated processes which minimizes physical paperwork and email-initiated actions and maintained by USG personnel. If future onboarding changes are needed, AFLCMC desires a solution that can be adapted by USG personnel. Further, onboarding processes shall contain a tool for onboarding personnel to

continuously monitor process from kick-off through completion (ex. Kanban). This tool shall permit evaluation of efficiency metrics to identify further process improvements. Vendors must be capable of operation within IL5, IL6, and IL6+ environments. At minimum, Vendors should include training and reach back support for Government operation of the designed tool. Future contract/agreement awards could include training and reach back support for Government management of the tool up to vendor full operational support.

Focus Areas Sought: Continuous Integration (CI)/Continuous Development (CD) software pipeline, Infrastructure as Code (IaC)

Anticipated Delivery Date: 120 days after receipt of order (ARO)

3. User Story 2 – Security Documentation Tool:

  User Story: Crucible is designed to enroll new USAF programs with specific software applications running in program-specific enclaves. This dynamic and elastic environment makes it difficult to appropriately document the environment. As Crucible enrolls additional USAF programs, new software, applications and enclaves creates a security documentation gap. Specifically, in order to maintain compliance with cyber security measures, AFLCMC needs to have sufficient documentation defining what software, applications and enclaves operate within Crucible at any given time in order to maintain an ATO, pass security audits or permit peering into new USAF/DoD networks. Current security policies are not adequately documented and lack a singular reference point of contact. Moreover, current security policies conflict each other and USAF guidance. Confusion over security policies often cause delays and unnecessary work. Specifically, for programs requiring peering into existing networks, AFLCMC lacks the appropriate body of evidence (BOE) needed to obtain permission to connect the network. Further, security documentation of onboarded personnel prevents users approved on one network from using an approved peered network. Lastly, Crucible has access controls limiting users to enclaves/environments specifically authorized. However, without updated security documentation, programs and vendors lack confidence that sensitive data is properly secured to prevent leaks/spills. As Crucible scales to add more users and programs, AFLCMC needs updated security documentation and process improvements to maintain ATO for all customers.

Outcomes Desired: To support Crucible, AFLCMC desires an automated tool/process to update security documentation for Crucible's changing environment. This tool must also document security protocols and identify/deconflict existing security policies. and implementation of security policies that maintain pace with Crucible's changing nature. Solutions must be designed to integrate with existing platform software identified in the attached Addendum. This automated tool shall update security documentation for added software, applications and/or enclaves to maintain the BOE for continuous ATO. Further, the tool should be maintained by automated processes that accurately map Crucible security configurations as outlined in the JSIG Appendix C and the Crucible specific Plan of Action and Milestones (POA&M). Documentation should be updated continuously and accurately reflect the state of Crucible within one week of a change. Vendors should design or utilize a tool and process to produce artifacts/documentation easily accessible to government security and program management personnel, including any underlying data/metadata used to generate the deliverables. Access Control policies should be updated and maintained to ensure proper access to Crucible environments for over 1,600 users, and more than 25 different user teams, with appropriate measures to permit USG personnel to validate proper segregation, limiting risks to leaks/spills or inadvertent access by unauthorized users. An ideal solution will improve connections to peer networks (ie IL6+ to IL6+) by rapidly updating and producing BOE documentation to obtain Authority to Connect (AtC). AFLCMC desires a solution that can be adapted by USG personnel. Vendors must be capable of operation within IL5, IL6, and IL6+ environments. Future contract/agreement awards could include training and reach back support for Government management of the tool up to vendor full operational support.

Focus Areas Sought: Software defined perimeter enabling classified data processing, Continuous Integration (CI)/Continuous Development (CD) software pipeline, Infrastructure as Code (IaC)

Anticipated Delivery Date: 120 days ARO

4. User Story 3 – Resource Utilization Tool/Automation:

User Story: AFLCMC desires to make the Crucible environment affordable for maximum USAF use. Cost barriers for

future enrollment consist of fluctuating Personnel & Environmental Onboarding, Security Documentation and Management Overhead costs. Management overhead includes the costs associated with making engineering changes within Crucible (establishing unique enclaves), purchasing of license/applications/tools, and setting up user accounts. As it pertains to Management Overhead costs, AFLCMC does not have a mechanism to view and monitor utilization of enclaves, applications, software, etc. Most Crucible processes rely heavily on Crucible personnel to both initiate and manage the process without adequate insight on utilization. Crucible administrators onboard users and environments as requested by each using program, creating a large back log of environmental engineering changes. This has resulted in an environment that is heavy on management and support personnel thereby driving up per-developer costs. Any environment changes require personnel heavy engineering changes which often require a month or more to accomplish. With a utilization tool, Crucible administrators could possibly recapitalize or reassign existing, unused/underused licenses/applications/enclaves. This should reduce the engineering backlog and reduce overhead costs. AFLCMC anticipates this problem exacerbating as more users/programs onboard into Crucible.

Outcomes Desired: AFLCMC seeks an automated tool that offers user utilization insights for varying enclaves/licenses/applications/tools/etc. Solutions must analyze usage of and integrate with existing platform software identified in the below Addendum. The solution must provide sufficient utilization details to allow Crucible administrators insights to advise users/programs on ways to reutilize/recapitalize on unused/underused licenses/applications/enclaves. Through utilization insights, AFLCMC desires to reduce administrative overhead costs to 30% or less of the total cloud cost (including compute & store, software, etc.) through reduced engineering change backlogs, reduced new licensure costs and repurposing existing infrastructure to meet new needs. The solution may include tools to identify cloud resources that may be incurring unnecessary costs, identify compute and storage cost drivers, and provide forecasting data for budgeting and planning. Key to any solution will be accurate collection of data on resource usage within Crucible. AFLCMC desires vendors use best data analytic practices when designing this tool. Finally, resource utilization tool should provide greater user self-service in Crucible for the following areas: software onboarding, data repository creation, requesting compute and storage resources, tracking of purchased resources usage, environment creation, and containerization. AFLCMC desires a solution that can be adapted by USG personnel. Solutions must be capable of operating in IL5, IL6, and IL6+ environments. Future contract/agreement awards could include training and reach back support for Government management of the tool up to vendor full operational support.

Focus Areas Sought: Continuous Integration (CI)/Continuous Development (CD) software pipeline, Infrastructure as Code (IaC)

Anticipated Delivery Date: 180 days ARO

5. User Story 4 – Data Platform:

User Story: AFLCMC desires to improve data sharing and analytics within the Crucible environment. Crucible users comprise different specific weapon platforms with unique and common requirements. However, based on the varying classification caveats among these users, and various intellectual property concerns, utilizing programs operate within segregated enclaves. Stringent security requirements and separation of environments limit access to data and modern software tools. Software libraries are both limited in quantity and generally do not reflect the most recent versions. Most work in Crucible is directed toward individual programs of records which limits the amount of common code and datasets that make modern data analytics possible. Further, Crucible users are often duplicating work because no common repositories exist for data sets, applications or common execution practices. Transferring of data tends to be a slow and often manual process. These challenges often prevent Crucible weapon system users from accessing and exploiting data analytics necessary to unlock insights to improve and optimize performance, unveil underlying trends, and detect features to meet program specific needs. AFLCMC believes a cohesive data platform running within the Crucible environment can help programs/systems focus on missional and operational problem sets. Moreover, creating a data platform with common repositories allows for a common thread among Crucible users. By allowing programs to utilize common data sets, implementations and/or algorithms, Crucible users can maximize efficiencies and reduce duplication of efforts.

Outcomes Desired: AFLCMC seeks tools and processes to build out a common data platform to operate within the Crucible environments. Solutions must cover any component of the dataflow to include parsing and documenting data formats, sharing and access control of data, data normalization and preprocessing, data analytics, data tagging, synthesizing data, data visualization, and optimization of data resources. Solutions must be easily adaptable to specific weapon systems needs without significant duplication of effort. Therefore, base data platform features should be sufficiently containerized for immediate deployment in varying user enclaves. The solution must drive data sharing using Application Programming Interfaces (APIs). Through parsing and documenting data formats, AFLCMC desires to make data easier to work with by third party vendors. Sharing and access control of data should make data more accessible to all programs within Crucible. Data analytic tools should be standalone and capable of operating in isolated environments. Data tagging and synthesizing should make the creation of domain specific datasets more feasible. Solutions may include, but are not limited to the following forms: creation of repositories for fundamental datatypes, datasets, and algorithms; dataflows that automatically generate documentation on data formats; dataflows for streaming data and transferring large datatypes; packaging code libraries for creation of deep learning, large language models, and other complex data analytic applications; data simulation and automatic data tagging tools for dataset generation; and tools for scheduling and queueing shared data resources. Cross-domain solutions and compute and storage hardware solutions are not within the scope of this user story. AFLCMC desires a solution that can be adapted by USG personnel. Solutions must be capable of operating in IL5, IL6, and IL6+ environments. Future contract/agreement awards could include training and reach back support for Government management of the tool up to vendor full operational support.
Focus Areas Sought: Machine Learning (ML) and Artificial Intelligence (AI) data factories, Big Data capability (data warehousing, data lakes, restructured data engineering)
Anticipated Delivery Date: 120 days ARO

_____

3. Call Description, Instructions to Vendors, and Evaluation Criteria
Overview: This call will be a two-step call. White papers may be submitted at any time prior to the due date and time specified in this Call. Vendors are responsible for monitoring SAM.gov for any amendments to this Call that may have updated information. White Papers will be evaluated against the criteria detailed below. After the submitted white papers have been evaluated by AFLCMC, vendors will be notified if they have been selected to submit a full proposal for Step 2.

- Step 1: White Paper due date and time is 12 January 2024 at 1700 ET. AFLCMC will review Step 1 White Papers and down select vendors based on the below evaluation criteria. Interested Vendors can submit clarifying questions to AFLCMC by 7 December 2023. AFLCMC will publish all received questions and AFLCMC's responses (anticipated 13 December 2023) prior to the White Paper submission date.

- Online Industry Day: Down selected vendors will receive an invitation to participate in an online Industry Day wherein AFLCMC will offer additional insights/information on the above user stories. If selected to submit a full proposal, AFLCMC, at its sole discretion, reserves the right to request a presentation or discussion with Government personnel about the White Paper.

- Step 2: Proposal due date and time will be provided in Requests for Proposal (RFPs) sent to offers that submit a Solution Brief and Pricing Proposal that meet or exceed evaluation criteria contained in this Call.

Overarching Instructions: AFLCMC reserves the right to award against each user story independently of one another. Vendors shall propose to each user story independently under one response. (For example, company X may submit a proposal for user story 1 & 3 in their response, while company Y may submit a proposal to only user story 4 in their respective response.) Vendors may propose to all, some, or one of the user stories. AFLCMC will not give preferential treatment for responding to a higher quantity of user stories, so vendors are encouraged to focus on areas where they can add the most benefit. User story responses will be evaluated and down selected for

continuation into step two (2) independently of one another. (For example, AFLCMC reserves the right to suggest company X move forward into step two for their response to user story 1, but not user story 3). Only one response (which may address multiple user stories) will be accepted from each vendor.

As a reminder, responses must be UNCLASSIFIED. AFLCMC will not accept classified proposals under this Call.

STEP 1 INSTRUCTIONS: Below is the required structure and required content for proposal submission for this Call. Vendor responses shall be submitted to Mr. Neal Duiker, at neal.duiker@us.af.mil & Ms. Kimberly Conley, at kimberly.conley.3@us.af.mil, NLT 1700 (ET) on 12 January 2024 at 1700 ET via email in either PDF, Word, or PowerPoint file types and shall include the following:

Part 1 - Cover Page: Vendor's cover page must include the following information:

1. Vendor Name
2. Vendor Address
3. Vendor technical, programmatic, and contracts points of contact (PoC)
4. List whether your organization qualifies as any of the following in accordance with FAR Part 19: Small Business (SB), Small Disadvantaged Business (SDB), Woman-Owned Small Business (WOSB), HUBZone Small Business, Veteran-Owned Business, Service-Disabled Veteran Owned Small Business (SDVOSB), Historically Black College or University (HBCU) and Minority Institution
5. DD254 Info
   1. CAGE Code
   2. Cognizant Security Office
      1. Name
      2. Address
      3. Phone Number

Part 2 - Questionnaire Responses: Vendors shall address all the following questions:

a. Which user story(ies) is your organization responding to?
   1. Personnel and Environmental Onboarding: (Y/N)
   2. Security Documentation Tool: (Y/N)
   3. Resource Utilization Tool/Automation: (Y/N)
   4. Data Platform: (Y/N)

b. Does your organization have experience with Microsoft Azure? Y/N

c. Provide a list of general classification levels and additionally proscribed categories from the below options that your organization has utilized for past projects. (UNCLASSIFIED / CUI / SECRET / SECRET SAR / TOP SECRET/ TOP SECRET SAR / TOP SECRET SCI) Note: Do not provide any classified information regarding past projects on your white paper submission, to include contract/agreement numbers (PIIDs).

d. AFLCMC problems require solutions that work in both Windows and Linux environments. Is/are the solutions your organization put forward compatible with both Windows and Linux? (Y/N)

e. AFLCMC problems may require solutions that necessitate an vendor to be familiar with coding languages. Does your organization have experience or expertise with any coding languages? AFLCMC has specific interest in Modern C++ (17+), Java11, and Python3. (Three sentence max)

f. AFLCMC problems may require solutions that necessitate an vendor to be familiar with data analytics libraries. Does your organization have experience or expertise with data analytics libraries such as scikit-learn, pytorch, numpy, pandas, R, or Julia. (Three sentence max)

g. Does your company have experience with any of the tools from the Addendum including Jira, Terraform, Helmfile, Backstage, OSCAL, Gitlab, or Jenkins? (Three sentence max)

h. Has your software been evaluated or accredited for use on government AFNET? (Y/N)

Part 3 - User Story Response(s): Independent from the above responses, an vendor may submit responses to one, some, or all the user stories detailed in part 2 above. Each response should be written so that they can be evaluated

individually by the Government. Vendors shall submit a response to each user story they wish to provide a solution for, not to exceed three (3) pages per user story (Times New Roman, 12 pt font) plus a title page each. The User Story Response(s) must include the following

1. A suggested technical solution, including a definition of a minimum viable product (MVP) covering a potential proof of concept.
2. A rough transition to work plan
3. Any ground rules/assumptions on which your solution is based
4. A rough order of magnitude (ROM) price estimate for your solution
5. An estimated timeline (Period of Performance) to get to the vendor-defined MVP
6. One or multiple examples of experience related to the user story/focus area (Demonstrated experience with highly secured IT systems, classified networks, and/or special access programs is preferred).

Proposals received in response to the CSO shall be evaluated in accordance with evaluation factors specified below using a scientific, technological, or other subject-matter expert peer review process.

STEP 1 WHITE PAPER EVALUATION CRITERIA: The Government will review the vendor's White Paper to determine if it has the potential to meet AFLCMC's needs based on the following criteria, which are listed in equal order of importance:

1. E – Experience: Has the vendor demonstrated experience in the user story areas? Does vendor have demonstrated experience as or with Appendix A software/tools?
    1. AFLCMC identifies specific tooling, software and/or applications for User Stories 1, 2 & 3. AFLCMC will evaluate vendor familiarity with these identified tool sets. Evaluators will review White Papers and identify experience working with these addendum items. The Crucible environment operates with in the Azure Government cloud platform. Therefore, all awardable vendors must demonstrate experience and knowledge working within Azure.
2. A – Access: Is the vendor eligible for security access to AFLCMC programs? AFLCMC work requires vendors work within an IL5, IL6 and IL6+ environment.
    1. Evaluators will assess whether vendors maintain adequate security approval to work within these environments. Vendors unable to operate per these security instructions will be deemed not awardable.
3. P – Price: Is the ROM price reasonable for the proposed scope of work and in relation to the independent government estimate?
    1. Interested vendors are required to provide a rough order of magnitude (ROM) for their solution brief. The competition review team will evaluate and assess whether ROM prices are reasonable based on:
        1. the solution offered in comparison to the user stories, and
        2. the ROM in relation to the IGE
4. T – Technical: Will offered technical solution help solve AFLCMC's user stories and intent for the proposed focus areas?
    1. Vendors are required to produce a suggested technical solution, including a definition of a minimum viable product (MVP) to solve AFLCMC's user story problem sets. The Competition review team will evaluate whether the proposed MVP provides a novel and executable solution to the user story challenges and stated intent sections contained within the call.

STEP 2 INSTRUCTIONS: The Government will invite select vendors to submit full proposals based on favorable evaluation results of White Papers approximately 30 days of the White Paper submission date. Solution Briefs and Pricing Proposals will be requested via a Request for Proposal (RFP) letter by the Contracting Officer and will contain separate submission instructions and applicable due dates and timelines. The Government will address any Organizational Conflict of Interest (OCI) concerns on a case-by-case basis with any vendor invited to submit a Step 2

proposal. For any OCI issues, instructions will be included within the Step 2 RFP.

After vendors are notified of the status of their Step 1 White Paper, an online industry day or technical interchange meeting will be scheduled for vendors selected for Step 2 proposals, tentatively scheduled for 9 February 2024.

Vendors invited into Step 2 will receive additional information from AFLCMC detailing the problems generally described in the above user stories. This additional information is sensitive and cannot be provided during Step 1. AFLCMC expects Step 2 vendors to tailor their proposals to meet these specific requirements.

Unsuccessful vendors will be notified by the Government, either via email or letter, to inform them that the proposed effort is not of interest to the Government at this time. Upon request from an unsuccessful vendor, the Government will provide a brief explanation of the reason for not requesting a Step 2 proposal, but will not entertain any questions from unsuccessful vendors.

Step 2 Proposal Review, Evaluation and Selection Process:

Each user story proposal will be evaluated by the Government and stand on its own technical merit. Proposals will be evaluated in accordance with the following evaluation criteria:

1. T- Technical:

1. The ability for the Government to transition the deliverables to future Government needs. Any proposed restriction on technical data or computer software will be considered; however, AFLCMC will prefer solutions granting USG sufficient data rights to manage technical solutions.
    • AFLCMC envisions sufficient data rights to mean having sufficient tools, technical data and ability to integrate automated tooling into other software/environments. Further, AFLCMC desires the ability to modify and/or integrate uniquely developed scripts, APIs and/or plug-ins.
    • The USG wants the ability to utilize USG partners to maintain and adapt the solution as needed. This requires adequate training and access to the necessary tools. As stated within the call, the USG will favor solutions in which the USG would have the adequate data/tools to meet this specific objective.

2. Does the solution meet and/or resolve USG user story challenges? AFLCMC will prefer solutions offering the greatest benefit regarding scaling, throughput, and data management capabilities.
    • USG will evaluate final solutions against how the solution resolves the user story challenges. Within each user story, AFLCMC identifies several specific challenges and intended outcomes. Final solutions will be rated on how effectively the solution addresses these challenges within the USG environment. Further, the competition review team will evaluate how the final solution meets both the MVP identified in the Step 1 White Paper and the intended outcomes identified within the user stories.
    • Further, the USG will evaluate how the solution optimizes and meets the scaling, throughput and data management capabilities needed to effectively meet AFLCMC's needs.

3. Is the vendor's proposed solution feasible within the time constraints of anticipated award?
    • Within the Project Vulcan Forge call, AFLCMC identifies specific timespans per user story. AFLCMC will evaluate the viability of the final solution in comparison to the anticipated delivery dates. AFLCMC will favor solutions that closely align to the anticipated delivery dates.

4. Does the vendor have relevant past experience in implementing technical solutions in highly secure environments? The Government in its sole discretion reserves the right to also consider the vendor's past performance on other efforts.
    • AFLCMC will evaluate a vendor's experience implementing solutions within highly secure environments. Crucible operates within IL5, IL6 and IL6+ enclaves. Awardable vendors must demonstrate relevant experience working in highly secure environments.

2. P - Price: The proposed price will be evaluated for reasonableness.

- AFLCMC will review the final price proposal in relation to both the scope of work proposed by the final solution and the independent government estimate.

No other criteria will be used.

Based on the Government's evaluation, proposals will be categorized as Awardable or Not Awardable (see definitions below). The selection of one or more sources for award will be based on the Government's evaluation, as well as importance to agency programs and funding availability.

1. Awardable: Proposal is recommended for acceptance if sufficient funding is available.
2. Not Awardable: Even if sufficient funding existed, the proposal should not be funded.

NOTE: The Government reserves the right to award all, some, one, or none of the proposals. When the Government elects to award only a part of a proposal, the selected part may be categorized as Awardable, though the proposal as a whole may not merit such a categorization.

If a vendor is determined to be awardable and chooses to proceed to contract/agreement award, AFLCMC and the vendor will enter into contract/agreement negotiations. Prior to award of a contract/agreement, the Contracting Officer/Agreements Officer will make a price reasonableness determination.

DEBRIEFINGS:

For unsuccessful vendors in either Step 1 or Step 2, the Government will conduct written, post-award debriefings upon request in accordance with FAR 52.212-1(l) and this Call. Debriefings will address the evaluation factors contained herein only. Debriefings will not include a comparison of submissions.

ADDITIONAL INFORMATION:

1. This CSO Call may result in the award of a FAR Part 12 contract or an Other Transaction Agreement (OTA) under 10 USC 4022 (also referred to as an Other Transition for Prototype or OTP). The awarded contract type shall be either Firm Fixed Price (FFP) or Fixed Price Incentive (FPI) in accordance with FAR Part 12.

2. The Government will be the sole decision authority on whether to pursue a FAR Part 12 Contract, an OTA, or no award at all. The Government reserves the right to award some, all, or none of the proposals received in response to this Call based on mission requirements and the availability of Government funds. The Contracting/Agreements Officer reserves the right to negotiate directly with the vendor on the terms and conditions prior to execution of the resulting contract/agreement on behalf of the Government. Be advised that only a Contracting/Agreements Officer has the authority to enter into, or modify, a binding contract/agreement on behalf of the United States Government.

3. This Call could result in the potential award of a follow-on production or solution integration contract or OTA.

4. Vendors must possess all required personnel security clearances, facility clearances, and other infrastructure requirements necessary to perform any proposed classified work in accordance with a Contract Security Classification Specification (DD Form 254) without reliance on Government resources. If vendor intends to perform classified work at their facility (or subcontractor or sub-awardee's facility), they will need to provide a Facility Accreditation Letter (FAL) for each facility to the Contracting Officer/Agreements Officer by no later than NLT contract/instrument award (anticipated by March 2024).

5. DFARS 252.239-7017 - NOTICE OF SUPPLY CHAIN RISK (DEC 2022):

(a) Definitions. "Supply chain risk," as used in this provision, means the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production,

distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system (10 U.S.C. 3252).

(b) In order to manage supply chain risk, the Government may use the authorities provided by section 10 U.S.C. 3252. In exercising these authorities, the Government may consider information, public and non-public, including all-source intelligence, relating to an vendor and its supply chain.

(c) If the Government exercises the authority provided in 10 U.S.C. 3252 to limit disclosure of information, no action undertaken by the Government under such authority shall be subject to review in a bid protest before the Government Accountability Office or in any Federal court.

6. Proprietary Information: Information constituting a trade secret, commercial or financial information, confidential personal information, or data affecting national security must be clearly marked. It shall be treated in confidence to the extent permitted by law. This restriction does not limit the Government's right to use information contained if it is obtained from another source without restriction. AFLCMC assumes no liability for disclosure or use of unmarked data and may use or disclose such data for any purpose. If an vendor is awarded a contract as a result of or in connection with the submission of proprietary data in the proposal, the Government shall have the right to duplicate, use or disclose the data to the extent provided in the resulting contract/agreement.

Proposals containing data that is not to be disclosed to the public for any purpose or used by the Government except for evaluation purposes shall include the following legend on the cover page:

"This proposal includes data that shall not be disclosed outside the Government and supporting personnel and shall not be duplicated, used or disclosed—in whole or in part – for any purpose other than to evaluate this proposal. If, however, a contract is awarded to this vendor as a result of – or in connection with – the submission of this data, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction. The data subject to this restriction are contain in sheets [insert numbers or other identification of sheets]."

Each restricted data sheet should be marked as follows:

Use or disclose of data contained on this sheet is subject to the restriction on the title page of this proposal.

7. Data Rights: For vendors invited to provide a phase 2 proposal, all proposal submissions shall include Data Rights Assertions, if applicable. This will be an essential element of each proposal submission. Special Licensing Agreements may be negotiated upon request. AFLCMC reserves the right to negotiate data rights as part of the Contracting/Agreement process.

8. Export-Controlled Items: Depending on the proposal subject matter, an awarded contract may be subject to Export Control (International Traffic in Arms (ITAR) 22 CFR 120-131, or Export Administration Regulations (EAR) 15 CFR 710-774). If the effort is subject to export controls, then a Certified DD Form 2345, Military Critical Technical Data Agreement, will be required to be submitted with proposals. DFARS 252.225-7048, "Export Controlled Item (JUN 2013)" clause shall be contained in all resulting contracts.

9. Supplier Performance Risk System (SPRS): In order to receive a DoD Contract, every vendor will be required to perform a Basis NIST SP 800-171 DoD Assessment. That process is described here. Once the Basic NIST 800-171 DoD Assessment is complete, each vendor will need to follow the instructions contained within this page to enter the results in SPRP on the PIEE website.

10. Telecommunications: All OTAs or contracts awarded under this Call will contain prohibitions on the use of certain telecommunications devices in accordance with DFARS 52.204-25.

11. Eligible Vendor: This is an unrestricted solicitation and open to all vendors. Small businesses are encouraged to propose. Vendors are encouraged to complete the Annual Representations and Certification in the System for Award Management (SAM) as soon as possible.

12. You may be ineligible for award if all requirements of this solicitation are not met on the White Paper and proposal (when applicable).

Attachment/Links

Attachments

Document	File Size	Access	Updated Date
Vulcan Forge CSO Call final.docx	0.015625KB	public	2023-12-01T15:57:42.252+00:00

Links

Display Name	Updated Date

Contact Information

Primary Point of Contact

Neal Duiker (Contracting/Agreements Officer)

neal.duiker@us.af.mil

Secondary Point of Contact

Kimberly Conley

kimberly.conley.3@us.af.mil

History

Contract Opportunity Type	Updated Date
Combined Synopsis/Solicitation (Original)	Dec 01, 2023 03:57 PM
Special Notice (Original)	Feb 09, 2023 07:47 PM

Interested Vendors List