Request for Information

Continuous Diagnostics and Mitigation Optimization and Integration Support

TAC-17-44964

This action is intended to be competed under the Transformation Twenty One Total Technology Next Generation multiple award, indefinite delivery, indefinite quantity contract using fair opportunity procedures in accordance with Federal Acquisition Regulation 16.505. This request for information (RFI) is issued solely to determine the availability of verified Service-Disabled Veteran-Owned Small Businesses (SDVOSBs) and Veteran Owned Small Businesses (VOSBs) that are capable of providing the services identified in the attached Performance Work Statement (PWS).

This RFI is for planning purposes only and shall not be considered an Invitation for Bid, Request for Task Execution Plan, Request for Quotation or a Request for Proposal. Additionally, there is no obligation on the part of the Government to acquire any products or services described in this RFI. Your response to this RFI will be treated only as information for the Government to consider. You will not be entitled to payment for direct or indirect costs that you incur in responding to this RFI. This request does not constitute a solicitation for proposals or the authority to enter into negotiations to award a contract. No funds have been authorized, appropriated or received for this effort. Interested parties are responsible for adequately marking proprietary, restricted or competition sensitive information contained in their response. The Government does not intend to pay for the information submitted in response to this RFI.

The North American Industry Classification System (NAICS) for this requirement is 541512 with a size standard of $27.5 million. A company that is not a VIP registered and verified SDVOSB or VOSB (https://www.vip.vetbiz.gov/) should not respond to this notice.

Provide the following: Summary describing your technical approach to meet the requirements which shall include Items 1 - 20 below. Generic capability statements will not be accepted or reviewed. ***Offerors shall be aware that the file size for email submissions is 5MB and zip files cannot be submitted.***

Respondents shall include the following in their submissions:

- Name of Company:
- Cage Code and DUNS Number:
- Address:
- Point of Contact /Company Representative:
- Phone Number:
- Email Address:

- Any applicable schedules (General Services Administration (GSA), Mission Oriented Business Integrated Services (MOBIS), Veterans Technology Services (VETS) Government wide Acquisition Contract (GWAC), etc.);
- If there are any vendor questions regarding the requirement, the Contracting Office will coordinate a comprehensive response and post to Federal Business Opportunities Page (FedBizOps).

Your response must address capabilities specific to the services required in the attached PWS and must include the following:

1. Provide a summary of your technical capability to meet the PWS requirements.
2. Corporate experience or expertise in performing these services and specific examples or references. Specific examples or references provided must include the agency, point of contact, dollar value, and contract number.
3. The intent and ability to meet set-aside requirements for performance of this effort, if set-aside, as set forth in Veterans Affairs Acquisition Regulation (VAAR) 852.219-10 (JUL 2016) (Deviation) VA Notice of Total SDVOSB Set-Aside or VAAR 852.219-11 (JUL 2016) (DEVIATION) VA Notice of Total VOSB Set-Aside, respectively. Please note that in accordance with 13 CFR §125.6 limitations on subcontracting requirements, demonstrate how you will not pay more than 50% of the amount paid by the Government to it to firms that are not similarly situated. Your response shall include information as to available personnel and financial resources; full names of proposed team members and the PWS requirements planned to be subcontracted to them, which must include the prime planned percentage or the names of the potential team members that may be used to fulfill the set aside requirement.
4. Has the draft PWS provided sufficient detail to describe the technical requirements to be performed under this effort.

   _____ YES ____ NO (if No, answer question 5)

5. If “NO”, please provide your technical comments/recommendations on elements of the draft PWS that may contribute to a more accurate proposal submission and efficient, cost effective effort.
6. Do you have an in-depth understanding of the VA’s specific CDM solution architecture and tool configuration, to include details on how the tools interact with each other? If yes, detail your understanding.
7. Do you have demonstrated experience implementing and integrating the specific tools that make up the VA’s specific CDM solution at organizations with over 500,000 endpoints? If yes, detail the organizations and how these tools were deployed.
8. Do you have demonstrated experience planning, deploying, configuring and integrating the DHS CDM Dashboard solution, including integration with the Federal dashboard? If yes, detail the work performed.
9. Do you currently have a team of engineers on-boarded within the VA with suitability and elevated network privileges (to include knowledge of their eToken

and One Time Password devices) that can implement and manage CDM tools within the VA environment? If yes, detail the work performed.

10. Are you knowledgeable on VA's processes to obtain suitability clearance and elevated privileges for staff to support this effort? If yes, detail the work performed.
11. Has your organization coordinated deployment and integration efforts across a geographically disperse environment the size of the VA, in support of a large enterprise cyber security solution? If yes, detail the work performed.
12. Detail your experience implementing the DHS CDM tool suite within the VA environment. If yes, detail the work performed.
13. Do you have an extensive understanding of the roles and responsibilities of the different groups within the VA that currently support the CDM project? If yes, explain the roles that all VA stakeholders take in the implementation and management of the CDM toolset. If yes, detail the work performed.
14. Do you have an extensive understanding of the VA's network topology and existing CDM ancillary hardware configurations? If yes, provide a specific explanation of how the CDM hardware is deployed and managed throughout the organization. If yes, detail the work performed.
15. Do you have an extensive understanding of the VA's change control procedures, to include approval processes, points of contact, and timelines? If yes, detail the work performed.
16. Do you have experience performing updates or patches within the VA environment, and specifically with the CDM tools? IF yes, describe the complete process for the request from initiation to execution. If yes, detail the work performed.
17. Do you have an established contractor lab facility, infrastructure and tools to support fully functional, system, integration, and performance testing for the CDM tools? If yes, detail the work performed.
18. Do you have established and proven operations and maintenance processes within the VA to support the CDM specific infrastructure to include tiered service desk with hands-on experience maintaining the VA's CDM solution? If yes, detail the work performed.
19. Has your organization supported executive-level reporting (i.e., dashboards) that provide current information on an organization's cyber security posture that is of similar size and complexity of the VA or at the VA? If yes, detail the work performed.
20. Do you have demonstrated experience working with CDM tool OEM's including knowledge of their service catalogs, experience with their troubleshooting best practices and escalation procedures? If yes, detail the work performed.

Responses are due to David Sette, Contract Specialist, David.Sette@va.gov and Summer Spalliero, Contracting Officer, Summer.Spalliero@va.gov no later than 12:00 P.M. Eastern Time on July 21, 2017.