DEFENSE FINANCE AND ACCOUNTING SERVICE

Request for Information (RFI)
Personally Identifiable Information (PII) Detection, Remediation, and Reporting Tool

Version 1.3
01/31/2020

A. BACKGROUND

DFAS is seeking to learn from Industry what cost effective commercial off the shelf (COTS) software products can meet DFAS' need for a Personally Identifiable Information (PII) detection and remediation tool within the agency.

DFAS seeks to learn about vendors who have COTS software capabilities that can detect PII data that is stored or loaded within the agencies' internal infrastructure Information Technology (IT) systems. The capability should discover content in motion and at rest residing within file shares, databases, and SharePoint data repositories. The capability should allow configurable actions to be taken upon any offending data such as blocking, deleting, moving, quarantining, encrypting, or redacting content. The software should include reporting capabilities to include logging all incidents with details to allow for auditing capabilities.

DFAS may, as a result of the information provided in response to this request for information, invite individual vendors to participate in industry presentations to further demonstrate their capabilities, experiences, and expertise with their solutions. Participation will be by invitation-only, and may require additional data submissions.

All information contained in this RFI is preliminary, as well as subject to modification, and is not binding to the Government. The Government will not reimburse vendors for any information submitted in response to this request. The determination of a procurement strategy, based in part upon submissions by interested parties, is solely within the discretion of the Government.

Instructions for Vendors:
Please review and provide responses to questions outlined below in Section C.

B. OBJECTIVES

DFAS is seeking Industry responses regarding commercial off the shelf software that is capable of providing protection with regards to PII detection and remediation functionality. DFAS also is interested in learning what other functionality and capabilities such software provides. DFAS is also interested in whether such software is part of an integrated Information Assurance system that the vendor offers. With respect to the need for PII detection and remediation functionality, DFAS has the following listing of items the software would need to be able to address:

A. Scan the following content in motion or at rest: file shares, databases, SharePoint
B. Take corrective action: block, delete, move, quarantine, encrypt, or redact content
C. Scan all major file types, including doc, docx, xls, xlsx, ppt, pptx, pdf, txt, htm, html, asp, aspx, and optionally mdb and accdb

D. Scan for PII, including social security numbers, bank account info, credit card numbers, birth dates, and addresses
E. Allow for customized scanning rules. For example, the ability to create a rule that looks for regular expressions and a combination of terms, as well as allowing the exclusion of certain acceptable values.
F. Provide interface for handling incidents. The user interface should clearly show at a minimum the name and location of the files that fail as well as who loaded the files and when. It is preferred that the software also provide a snippet of the text in which the offending data is discovered.
G. Provide summary reports, including number and type of incidents. It should also allow for filtering of incidents by location or date and allow data to be exported to Excel.
H. Preferred environment: Windows Server 2016. Microsoft SQL Server 2016. SharePoint 2016
I. Software must adhere to DoD security standards.
J. Software must also be Section 508 compliant.
K. CAC/PKI authentication is also be a requirement as well as role based permissions.

C. RFI QUESTIONS

We seek Industry feedback and comment on the following questions:

1. Are all modern versions of SharePoint supported (2013, 2016, 2019, online, O365)?
2. Is your product 508 compliant? DoD Section 508 policies requires products to be accessible to people with disabilities. https://dodcio.defense.gov/DoDSection508.aspx
3. Are product version updates (major and/or minor) available during the period of performance with no additional cost?
4. If hardware/infrastructure is refreshed, is the licensing transferrable to the new hardware/infrastructure?
5. If hardware/infrastructure is replaced, can the current software configuration/setup be saved and easily imported on to the new hardware?
6. DoD agencies are required to fix critical/high vulnerabilities within 30 days. Does your organization have mechanisms and procedures in place to ensure vulnerabilities related to this product are addressed in a timely manner?
7. Have you conducted penetration testing on your software?

8. Have you resolved all deficiencies discovered during penetration testing?
9. Do you continue to conduct penetration testing on all new releases?
10. Do you resolve all deficiencies discovered during penetration testing within 15 days of discovery?
11. Do you have a robust quality control program for software releases?
12. Do you follow generally accepted industry standards for software testing and deployment?
13. Do you follow the Software Development Life Cycle process?
14. Do you follow the agile methodology for software development?
15. The security of our computing environment is isolated to military and government agencies. Can the product(s) setup and operate without reaching out across the internet to any outside entities?
16. Do you have a subscription based licensing?
17. Do you have perpetual licensing?
18. Are you able to provide a Rough Order of Magnitude (ROM) for subscription based licensing and/or perpetual licensing?
19. Does your product conduct PII scanning of SharePoint content at rest?
20. Does your product conduct PII scanning of SharePoint content on demand, such as during the upload or content saving process (Real-Time Scan)?
21. Does your product conduct PII scanning of databases at rest?
22. Does your product conduct PII scanning of databases on demand such as during the data commit process to the database?
23. Does your product conduct PII scanning of unstructured content (i.e. shared drives) at rest?
24. Does your product conduct PII scanning of unstructured content (i.e. shared drives) on demand, such as during the save process of a file?
25. Does your product remediate PII in SharePoint such as quarantine, redact, or encrypt?
26. Does your product remediate PII in databases such as quarantine, redact, or encrypt?
27. Does your product remediate PII in unstructured content such as quarantine, redact, or encrypt?
28. Does your product have a limit to how many content items it can scan?
29. Does your product include an incident management system to manage alerts, findings, and actions necessary?
30. Does your product provide comprehensive metrics for PII scan results and incident management?
31. Does your company provide setup or ramp-up services for your product?

32. Does your company provide free training for your product?
33. Does this operate in a Microsoft Windows Server and SQL environment?
34. Do you have DoD customers?
35. If you have (DoD) customers, is your application currently installed and functioning in their environment?
36. If you have (DoD) customers, is the application hosted at Defense Information Systems Agency?
37. Does your product have a centralized administration dashboard?
38. Does the application support common card authentication?
39. Does the application utilize Active Directory?
40. Please describe the (software/hardware) rough order of magnitude costs for licensing, for implementation support (if any), and for migrating to your software to achieve the goal of a DFAS-wide PII remediation solution (if any).
    a. Beyond the annual license fee (if there is one), what other licensing commitments should we anticipate for the upkeep of vendor's software?
        i. Will those be one-time, periodic, annual, etc.?
    b. What is the impact of buying additional servers on the licensing structure?

Feel free to elaborate on any of the questions above with additional details.

D. Additional Question only for Small Business

This RFI part of our market research activities to make appropriate acquisition decisions and to gain knowledge of potential qualified Small Businesses, e.g., General Small Businesses, Service Disabled Veteran Owned Small Businesses, Veteran Owned Small Businesses, 8(a), HUBZone and others interested and capable of performing the work. Please note, we are only interested in communicating with vendors who have their own COTS software product. We are not interested in system integrators or business selling licenses to another business's software, so please don't respond if you are a system integrator or not the owner of the software being proposed. Such responses will be discarded. Responses to this notice shall include the type of small business, to include Service Disabled Veteran Owned small Business, Veteran-Owned small business, 8(a), HUBZone Small Business, Women Owned small business, and Small Disadvantaged business, if applicable.

Small Businesses are encouraged to provide responses to this RFI. Such responses will be used to assist DFAS in determining whether any small business vendors have created COTS software that has the out of box capability to perform the function of PII detection and remediation. Also, DFAS seeks to learn the potential levels of competition available in the industry, as well as helping to establish a basis for developing any subsequent potential subcontract plan goal percentages.

Small Business firms owning a COTS software capable of performing the tasking described in this RFI are encouraged to respond. It should be noted that any resultant contract or task order for supplies (other than procurement from a non-manufacturer of such supplies), the concern shall perform work for at least 50 percent of the cost of manufacturing the supplies, not including the cost of materials. Your supply item (software) requires at least 50 percent of the cost of contract performance incurred to be expended for employees of the concern proposing as a prime. Please see FAR Clause 52.219-14, Limitations on Subcontracting for prescription and complete version of the clause.

Responses to this RFI will help shape the government's strategy for this acquisition, as well as any subsequent formalized solicitation.

1. Does your small business have a COTS PII detection and remediation software? If so, please describe it.

2. What NAICS codes apply to the COTS PII detection and remediation software?

3. Would you elect to submit to one or more of the following sub-categories; 8a, Service-Disabled Veteran Owned Business and/or HUBZone?

4. If you would submit as an 8a and/or HUBZone, are you Small Business Administration (SBA) Certified in either or both of these sub-categories?

5. What is your exit date for your certification(s) in 8a and/or HUBZone?

E. INFORMATION REQUESTED

Information is requested to gain an understanding about vendor's products are available to satisfy the inquiry regarding questions described in paragraph C and for only small business, paragraph D. Within your response to this RFI please include recent and relevant contracts (last 3 years), including the contract number, and dollar value for procurements you have offering this COTS software product.

F. RESPONSES

Responses to this RFI shall address all items listed in the objectives above and shall not exceed 5 pages. Responses shall be e-mailed as either a PDF or MS Word attachment and must include a cover letter with the institution name, points of contact (address, phone number, and e-mail), DUNS Number and CAGE code. DFAS requests a response by February 19th, 2020. Please e-mail responses by the date shown above to the attention of Mr. Don Crawford at donald.a.crawford1.civ@mail.mil. DFAS may establish a dialog with vendors who respond if needed to gain a better understanding of their service offerings or capabilities.

E. DISCLAIMER

This is a request for information only. It is not a Request for Proposal, a Request for Quotation, an Invitation for Bids, a solicitation, or an obligation on the part of the Government to acquire any products or services. No entitlement to payment of direct or indirect cost or charges to the Government will arise as a result of a contractor submission of responses to this announcement or the Government's use of such information.

In accordance with FAR 15.201(e), responses to this notice are not offers and cannot be accepted by the Government to form a binding contract. This RFI is issued solely for information and planning purposes and does not constitute a solicitation. Neither unsolicited proposals nor any other kind of offers will be considered in response to this RFI. Responses to this notice are not offers and will not be accepted by the Government to form a binding contract. Responders are solely responsible for all expenses associated with responding to this RFI. All information received in response to this RFI that is marked Proprietary will be handled accordingly. Responses to the RFI will not be returned. At this time, questions concerning the composition and requirements for future RFPs will not be entertained.