District of Columbia Courts
Administrative Services Division
Procurement and Contracts Branch

AMENDMENT NO. 4

TO: ALL PROSPECTIVE OFFERORS

AMENDMENT
ISSUE DATE: July 19, 2021

SUBJECT: Solicitation No. DCSC-21-FSS-93 - Identity and Access Management (IAM) Solution

PROPOSAL
SUBMISSION DATE: July 29, 2021, by 1:00 p.m., Eastern Standard Time.

Responses to written question(s) received from prospective offeror(s) are included as Attachment A to this amendment.

ALL OTHER TERMS AND CONDITIONS REMAIN UNCHANGED

One (1) copy of this amendment is being sent to only those offerors who received a copy the solicitation. Offerors shall sign below and attach a signed copy of this amendment to each offer to be submitted to the Courts in response to the subject solicitation. Offers shall be delivered in accordance with the instructions provided in the original solicitation documents. This amendment, together with your offer must be received by the District of Columbia Courts no later than the date and time specified for offer submission. Revisions or price changes occasioned by this amendment must be received by the Courts no later than the date and time set for offer submission. Failure to acknowledge receipt of this amendment may be cause for rejection of any offers submitted in response to the subject solicitation. Offerors who have already submitted their responses may revise their technical and/or price proposals.

Darlene D. Reynolds

Darlene D. Reynolds
Contracting Officer

This amendment is acknowledged and is considered a part of the subject solicitation.

Signature of Authorized Representative	**Date**
Title of Authorized Representative	**Name of Firm**

ATTACHMENT A

Solicitation No. DCSC-21-FSS-93 - Identity and Access Management (IAM) Solution

RESPONSE(S) TO QUESTION(S) RECEIVED

1. **Question:** We understand that you have Microsoft Azure FedRAMP Government platform.
    a. Do you currently have Azure AD utilized in your environment?
    b. What level of Azure AD license do you currently have?
    c. If yes, do you currently have your on-premises AD synchronizing to Azure AD?
    d. If yes, what are the current Azure AD capability are you utilizing in your environment? E.g., SSO, Identity Governance, etc.

RESPONSE:

Microsoft O365 Tenant

a. Yes
b. Azure AD P1
c. Yes
d. SSO, Identity Gov, Conditional Access, App Registration, MFA

2. **Question:** In term of your IAM solution, are you looking for a single application proposal or are you open to best of the breed (multiple IAM products) proposal?

RESPONSE: The DC Courts is wanting a single product solution however if the solution requires addons/options offered by the same product manufacturer to make a complete solution that is acceptable. The Courts do not want a solution that requires multiple different product manufacturers to make it a complete solution.

3. **Question:** Could you provide additional details on the following applications in term of application server, software vendor name and version and user data store info (E.g., database, directory, etc.) for us to understand how to integrate SSO and provisioning capability with them?
    a. Tyler Odyssey Case Management System
    b. Oracle Business Intelligence
    c. Web Interpreter & Translation System
    d. Budget and Finance MIP system
    e. Access Control System
    f. Avaya Interactive Voice System
    g. Bank/Debit Card system
    h. AgileJury
    i. TeensATPromiseforSuccess (TAPS)

j. WebVoucherSystem
k. Tenable SC&IO – Vulnerability and Compliance scanner also known as Nessus. The IO version is a web scanning Vulnerability and Compliance scanner. Uses AD for login and Password Management.
l. KnowBe4 – Security Awareness Training uses AD for login and password management.

RESPONSE:

a. Tyler Odyssey Case Management System – Tyler Technologies / AWS Cloud Solution
b. Oracle Business Intelligence – Oracle Inc / Oracle Weblogic 12c / Oracle 12c database
c. Web Interpreter & Translation System – Home-grown Oracle APEX 20.x / Oracle 19c database
d. Budget and Finance MIP system - Abila
e. Access Control System
f. Avaya Interactive Voice System - Avaya
g. Bank/Debit Card system
h. AgileJury – ClearView Jury by Avenu Insights & Analytics / COTS
i. TeensATPromiseforSuccess (TAPS)- Global Justice Solutions Inc / Azure Cloud Solution
j. WebVoucherSystem – Home-grown Java / J2EE, Oracle Weblogic 12c / Oracle 12c database
k. Tenable.sc & Tenable.io – Vulnerability and Compliance scanner also known as Nessus. The Tenable.io version is a Vulnerability and Compliance scanner for our web applications/sites. Uses locally stored accounts/ login and Password Management.
l. KnowBe4 – Security Awareness Training uses AD for login and password management. Cloud based.

On behalf of AET System, Inc., I'm pleased to submit the questions below.

4. **Question:** Within DCC's Technical Environment (ref C.2 -A), which applications are already using ADFS for SSO?

RESPONSE: SEE #1 Very limited

5. **Question:** How are those applications integrated in terms of Federated SSO? Are they using WS-Federation, SAML or both?

RESPONSE: Consider this a new implementation with little to no Federated services.

6. Question: Does the scope include migrating from ADFS (on-premises) to Azure AD?

RESPONSE: The extent of this will be determined after contract award; vendor will evaluate environment, create recommended installation, schedule, and determine full implementation strategy of the environment.

7. Question: In C.3.4, the RFP states that the "Vendor shall install and configure the Virtual IAM solution in the cloud." Can you provide more detail on what exactly is meant by Virtual IAM: a virtual appliance? Something else/different?

RESPONSE: DC Courts wants a cloud-based solution. How the vendor accomplishes this is at the vendor's discretion based on the following. Best Practices, Design and Implementation provides DC Courts full usage of capabilities of the Solution proposed and it does not negatively impact the security posture of the Courts. The solution does not increase staffing requirements, meets NIST controls and FISMA requirements and vendor can fully train staff on operation of solution.

8. Question: What is the expected go-live timeframe/date?

RESPONSE: DC Courts wants award to take place by September 30, 2021, and expects go-live with-in 6 months from contract award. The follow is an example timeline:

1) Kickoff Meeting
2) Vendor meets with DC Courts to do a complete analysis of the DC Courts Environment (Applications, Hardware, Processes, Staffing structure.
3) Vendor Proposes recommendations for implementation with schedule and requirements to meet schedule.
4) Implementation and testing.
5) Vendor to provide complete implementation and configuration documentation, SOPs, and diagrams.
6) Train Staff on products.
7) DC Courts to determine acceptance.
8) Vendor to provide allotted number of professional services to address any unexpected support requirements.
9) Closeout

Regarding the technical aspects of the RFP:

9. Question: a) Which one of the listed applications (row 13) in the DCC's Technical Environment table would need to be SSO-enabled?

RESPONSE:
DC Courts wants to make all applications SSO, but analysis by Vendor and staff will be required to determine capabilities. If an application/system cannot be SSO, we expect the vendor to provide a write up of the application stating why it cannot be SSO with justification, and a response that would be acceptable to an auditor. If it can be SSO, and it just needs something to make it possible, we expect the vendor to detail this and present to DC Courts for decision.

10. Question: b) Specifically which products do the below listed systems refer to?

- Web Interpreter & Translation System
- Budget and Finance MIP system
- Access Control System
- Bank/Debit Card system

RESPONSE: SEE #3

11. Question: b.1) Are those all web-based?

RESPONSE: See #3 & 8

12. Question: b.2) Are all of those target systems expected to be on-boarded onto the SSO solution?

RESPONSE: See #8

13. Question: c) Approximately how many J2EE applications are hosted in Oracle WebLogic? Are they home-grown, COTS applications or a mix of both? Do they need to be SSO-enabled?

RESPONSE: See #3

14. Question: d) Approximately how many Oracle APEX applications are there? Are they home-grown, COTS applications or a mix of both? Do they need to be SSO-enabled?

RESPONSE: See #3

15. Question: e) Are there any web services being serviced from the Oracle SOA suite? Approximately how many, and what sort of authentication mechanism is being used? Do they need to be integrated with the IAM solution?

RESPONSE: See # 3 & 8

16. Question: f) Is the source code available for home grown systems?

RESPONSE: See #3

17. **Question:** g) On top of which stack is your DevOps/DevSecOps environment based?

RESPONSE: See #3

18. **Question:** h) Is this environment expected to be integrated with the IAM solution?

RESPONSE: YES

19. **Question:** (Provisioning 2.2) Does DC Courts want to onboard equipment data into IGA solution and if so, where is that data stored?

    RESPONSE: All at DC Data center but multiple sources.

20. **Question:** (Provisioning 2.10) Does DC Courts have an MDM system? What are they using if so?

    RESPONSE: ManageEngine is our MDM and currently it is only used for IPads

21. **Question:** (Third Party 4.2) Can you define/elaborate on what is meant by "data spare model"?

    RESPONSE: This was a typo it should have said (Third Party Contractors/Vendors 4.2 Setup data sparse model to monitor external users) Description: The IAM system to facilitate functionality to monitor 3rd party contractors/vendors/external users using data sparse model(s) to define patterns to mitigate identity and access related threats (brute force, excessive privileges, etc.)

22. **Question:** (Access Recertification 6.5) We can configure to allow mass blanket approvals (or not allow), but is that what is desired here?

    RESPONSE: We are not looking to Disable this we want to be notified if it happens.

23. **Question:** (Password Management 7.2) We can configure to expire after 90 days; however, we cannot reset the password after expiration (out of the box). Is resetting the password the requirement here?

RESPONSE: This is a capability the Courts want for elevated accounts such as an admin as well for normal users if that is decided by the Courts.

24. **Question:(**Role Management 8.6) Are you looking for automation to kick off version rollback, or would a manual process suffice?

RESPONSE: We want and automated capability in the event a role back is required.

25. **Question:**(Audit and Tracking 11.11) Are you looking to IMPORT data into the IGA solution or push data from the IGA solution into these other systems? If you are looking to import can you elaborate as to why? We have historically seen data pushes, so importing would be unusual.

RESPONSE: This would be a data push such as push to a SIEM

26. **Question:**(Cloud Governance 13.2) Are you looking for the IGA solution to be able to classify data or would a separate solution be acceptable?

RESPONSE: If the proposed solution does not have the capabilities but can be handles in another manner to meet the contract requirements and is included in the quoted price making this a complete solution it is acceptable.

27. **Question:**(Authentication 14.3) What is the current SSO/Federation solution?

RESPONSE: We have four domains and trust relationship with two of them.

28. **Question:** What are the different application types involved (on prem vs. cloud, legacy, etc.)?

RESPONSE: On Prem, Cloud and Legacy

29. **Question:** Does DC Courts have a disk management tool?

RESPONSE: No

30. **Question:** Regarding F.4 - Are US territories acceptable remote locations?

RESPONSE: This procurement is **restricted to firms that hold a current U.S. Government General Service (GSA) Schedule** and are qualified to provide the required service.

31. **Question:** What work has been accomplished by the Courts in the areas of Separation of Duties (SoD) and identifying Roles that should have access to systems in a Role Based Access Control (RBAC) environment?

    1. What specific expectations are there for the Vendor in these areas?
    2. Will the Vendor consult with and advise Court IT staff in definition and development of the required matrices or take more of a lead role in this process?

    RESPONSE: While some work has been done in this area it is best to take the approach that nothing has been done and part of this project will be defining these needs.

32. **Question:** Are duties and access levels currently controlled by which Active Directory the staff member authenticates with, physical separation (e.g. building location) or something else?

    RESPONSE: Yes by Groups, Policies in two of the Domains. Building access such as building and location cards are not joined at this point nor is it part of this project

33. **Question:** Does DCC desire to have IAM nodes in each of its physical infrastructure locations or would the Azure cloud environment be preferred?

    RESPONSE: DC Courts is wanting a Cloud based solution that provides the courts with full capabilities of product and meets at minimum all requirements in the RFP. How the vendor meets those requires is not defined by the courts but the vendor. Also, the Courts is looking for a single solution. Access must be capable of remote access and operation will provided the best possible security and meet NIST and FISMA controls.

34. **Question:** Regarding section 11.0 (Audit and Tracking) of Appendix A, many of the requirements (e.g., 11.3, 11.4 and 11.11, 11.14, etc.) are more in line with the function of a Security Information & Event Monitoring (SIEM) solution. Given that DCC also has a current request posted (DCSC-21-FSS-87) for a SIEM solution, does the Vendor need to propose this functionality in their response, or describe how integration with an industry standard SIEM solution would accomplish these requirements? If integration with the DCSC-21-FSS-87 SIEM solution is an option, would the Vendor role in this response be to work with DCC IT staff to ensure that logs are securely transmitted to the SIEM solution and understood by DCC IT staff for analysis or something else?

RESPONSE: Vendors response should include how you would propose meeting the requirement to satisfy the RFP. Yes, log management is part of the requirements.

35. Questions: Does DCC already have business policies in place regarding business processes or system usage that would form the basis for the SoD rules requested in 12.1 of Appendix A? Would business process managers be available to assist in the development and approval of these rules?

RESPONSE: Rules should be part of the proposed capabilities and DC Courts will ensure you have access to staff needed to make decisions and approvals

36. Question: Can you clarify what section 12.2 of Appendix A means?

RESPONSE: DC Courts is wanting a Solution that allows for some separation of Duties out of the box but that also can be customized to meet custom requirements.

37. Questions: In Amendment 2, Attachment A, Question 3, you indicate that Google Apps are not used, but you reference classifying Google Apps data in 13.2 of Appendix A - can you clarify which is the case? If Google Apps are not being used, Azure allows the dynamic classification of data through its Data Loss Prevention capabilities - would the Vendor be expected to consult with DCC IT staff in implementing Azure Cloud's native capabilities or is something else desired here?

RESPONSE: Google Apps are not used by DC Courts, DC Courts uses AWS for one cloud based application. Yes, the Vendor would be expected to consult with DCC IT Staff to define these capabilities and proposed solution.

38. Likewise, in 13.6 of Appendix A, sensitive document tagg Could you please clarify if the redlines from vendors are expected along with the proposal submission, i.e., on 7/29 or are they expected before the proposal submission date. If before, could you please let us know the date for submitting redlines to TC's.

Response:

The due date is the same date for submitting questions, which is July 19, 2021, by 10:00 a.m.