UNIVERSITY OF SOUTH CAROLINA

AMENDMENT NO. 5 TO SOLICITATION

TO: ALL VENDORS

FROM: Caleisha Hayes, Procurement Manager

SUBJECT: SOLICITATION NUMBER: USC-RFP-3427-CH

DESCRIPTION: IT AUDIT SERVICES

DATE: March 21, 2019

This Amendment No. 5 modifies the Request for Proposals only in the manner and to the extent as stated herein.

Vendor Questions & Answers

THE DEADLINE FOR RECEIPT OF PROPOSALS HAS BEEN EXTENDED TO APRIL 1, 2019 AT 3:00 PM.

The Award Posting Date has been extended.

OFFERORS SHALL ACKNOWLEDGE RECEIPT OF AMENDMENT NO. 5 IN THE SPACE PROVIDED BELOW AND RETURN IT WITH THEIR RESPONSE TO THE SOLICITATION. FAILURE TO DO SO MAY SUBJECT THE RESPONSE TO THIS REQUEST FOR PROPOSALS TO REJECTION.

_____ _____

Authorized Signature Name of Offeror

_____

Date

USC-RFP-3427-CH

THE FOLLOWING QUESTIONS WERE RECEIVED FROM VENDOR A:

1. Will the University provide a two week extension on the "Submit Offer By" date to allow service providers to develop a well-prepared response aligned to your requirements?

   ANSWER: ***Please see page 1 of this Amendment #5.***

2. Has the University previously used a third party provider for internal audit services?

   ANSWER: ***Yes, back in the 2014-15 period, Pondurance performed a HIPAA Security Assessment of Student Health Services, as well as to survey other departments to assist in planning for future assessments.***

3. Over the past two years, what has been the average number of man hours and duration of each IT audit engagement?

   ANSWER: ***Hours can vary widely dependent on the scope and the nature of the engagement, to give it an average may not do it justice. For example, over the last couple of years, more than 700 hours has been spent on PeopleSoft Pre Implementation Reviews (ongoing project), while about 380 hours was spent on the Cybersecurity – State Security Standards engagement.***

4. Will performing internal audit services on behalf of the University preclude service providers from conducting remediation activities?

   ANSWER: ***This is outside the scope of this RFP. However, should the University require those services, the Contractor would not be precluded from participating in the appropriate procurement process to secure remediation services. However, the IT audit team, including the manager or partner, on the U of SC engagement would be precluded from providing remediation services.***

5. Should the service provider submit the cost proposal along with the technical proposal or should we package separately?

   ANSWER: ***Please see Section II. Instructions to Offerors "Contents of Offer"; "Electronic Copies – Required Media and Format" of the RFP.***

THE FOLLOWING QUESTIONS WERE RECEIVED FROM VENDOR B:

6. How many applications, databases, servers, workstations and operating systems would be considered in-scope for the IT Universe Analysis?

   ANSWER: ***Your question is somewhat the primary goal of this engagement. The USC Columbia IT Audit Team was established in 2015, and is responsible for providing assurance to all system campuses, including their respective inventories of applications, databases, servers, workstations and operating systems. All applications, etc., would be considered in-scope initially until we have a holistic perspective of the inventory and the impact of each application listed. The system campuses are: Columbia, Aiken, Beaufort, Upstate, Lancaster, Salkehatchie, Sumter and Union. Please see Section III. Scope of Work/Specifications of the RFP.***

7. Are the applications in-scope for the IT Universe Analysis and Risk Assessment limited to server/business applications or include desktop applications?

   ANSWER: ***Please refer to Question #6.***

8. How many departments would be considered in-scope for the IT Universe Analysis?

   ANSWER: ***Approximately 60.***

9. How many applications are customized, such as modifying the source code and program in-house?

   ANSWER: ***Please refer to Question #6.***

10. Is the user provisioning process centralized for all the in-scope applications, databases and operating systems?

    ANSWER: ***No. Oracle Identity Manager is in the process of being implemented and will assist with moving this effort along.***

11. What is the historical number of hours per year each IT Audit has required?

    ANSWER: ***Please refer to Question #3.***

12. Does the University have tools to assist in developing the inventory of applications for the IT Universe Analysis? (Application Discovery, Asset Inventory, CMDB)

    ANSWER: ***The University has Content Manager.***

13. Is the audit of outsourced IT services specifically for the IBM support of the 13 core application areas?

    ANSWER: ***Yes.***

14. If the audit of outsourced IT services is for more than the IBM contract, can you please provide the names and services of the other vendors?

    ANSWER: N/A

15. [Are] the services performed by the outsourced IT provider infrastructure support, application support, or both?

    ANSWER: Application support.

16. What is the estimated annual spend for the outsourced IT provider's services?

    ANSWER: ***Approximately $7 million.***

17. How many Departments within the University's Columbia campus are subject to the HIPAA/HiTech Compliance Audit?

    ANSWER: ***We confirmed 5 in 2015.***

18. How many Departments outside of the University's Columbia campus are subject to the HIPAA/HiTech Compliance Audit?

    ANSWER: ***We confirmed 1 in 2015.***

19. Are any of the Departments joint ventures?

    ANSWER: ***No.***

20. Do the Departments follow the same HIPAA Policies and Procedures or do they have their own unique HIPAA Policies and Procedures?

    ANSWER: ***We wrote a recommendation to employ a Privacy Officer to ensure compliance with HIPAA Policies and Procedures, consistently across the University. The position was filled in 2018.***

21. Does the University want a separate report for each Department or one report for all Departments?

    ANSWER: ***Separate report for each Department.***

22. What are the University's PCI requirements? Self-Assessment Questionnaire (SAQ)? Report on Compliance (ROC)? Other?

    ANSWER: ***Divisions, departments, and campuses desiring to accept payment, by any method, for financial transactions on the University's behalf must have approval from the University Bursar, who is responsible for administering the University's PCI program. SAQs are reviewed annually by a contracted QSA. Results of the annual reviews are provided.***

23. Does the University have a preferred NIST standard for their Information Security Assessment?

    ANSWER: ***The University's Information Security office leverages the NIST framework (as a whole) to comply with the State of South Carolina Information Security and Privacy Standards.***

THE FOLLOWING QUESTIONS WERE RECEIVED FROM VENDOR C:

24. Is there an IT framework that the University has adopted to provide strategic guidance for the IT environment (ISO 27001, NIST, ITIL)?

    ANSWER: ***Please refer to Question #23.***

25. Can you provide insight in the 13 core applications that are supported by IBM?

    ANSWER: ***Banner Education System (Student Information System), PeopleSoft Finance, PeopleSoft HR, Cognos Data Warehouse, Web Portal sc.edu, Web/Student Portal, Operational Data Store/DW, Application Security, Oracle Enterprise Manager, Web Content Management, Enterprise Applications, Enterprise Financials, and Student Portal Mobile.***

26. Can you provide a list of the top enterprise applications utilized by the University if different than the 13 core applications supported by IBM?

    ANSWER: ***Banner, PeopleSoft, Carolina Card, Degree Works, Content Manager, Blackboard, Cognos, BDMS, to name a few.***

27. Are the 13 applications supported by IBM collocated or hosted in an IBM data center?

    ANSWER: ***Collocated.***

28. Other than HIPAA, PCI, FERPA can you provide insight into any other regulatory audits the University would require i.e. FISMA, GLBA, GDPR, NIST 800-171 or other state required audits?

    ANSWER: ***GLBA. Those are the primary regulations that apply enterprise-wide. There are also more targeted regulations related to export controls, environmental controls, etc.***

29. For the proposed HIPAA audit, should we include all three domains (Security, Privacy and Breach Notification) or should it just focus on a particular subset of these domains?

    ANSWER: ***Please include all three domains.***

30. Has Internal Audit established an annual budget of hours that they intend to dedicate to IT auditing services?

    ANSWER: ***Yes. For June 1, 2018 through May 31, 2019, there were approximately 2,900 hours allocated for IT audits. The hours for the upcoming fiscal year (2019-2020), which would include both internal and outsourced engagements, will be similar.***

31. Does Internal Audit currently employ IT auditors? If so, how many?

    ANSWER: ***Yes. 1 Assistant IT Audit Director, and 2 IT Audit Managers.***

32. What is number of staff that work for the division of information technology?

    ANSWER: ***In the 200 range.***

33. Can you provide the IT staffing levels for each of the campuses?

    ANSWER: ***On average, it's about 5 for each IT group.***

THE FOLLOWING QUESTIONS WERE RECEIVED FROM VENDOR D:

34. Regarding RFP Section VIII. Bidding Schedule/Price-Business Proposal (on page 38 of the RFP):
    a) Is it USC's expectation that engagements 1 - 5 will be done in sequential order?
    b) Or do you expect overlap between these engagements? If you anticipate overlap, please elaborate on your expectations.
    c) Or do you want the consultant to propose the most appropriate sequence?

    ANSWER: ***No. Engagement #'s 1 and 2 would be in sequential order. Engagement #s 3, 4 and 5 are standalone. The University will determine whether all, or which combination, of the engagements will be done. The major drivers behind which engagements we choose are: Cost, when the audit appears on the audit plan, and whether our internal team is in need of assistance in a particular area.***

35. Who is the executive sponsor of this initiative within the University of South Carolina?

    ANSWER: ***Chief Audit Executive.***

36. What are the University's key drivers for initiating this project?

    ANSWER: ***Considering the complex layout of eight campuses and their respective applications spanning across the state of South Carolina, as well as certain degree programs requiring specialized IT expertise, the primary driver is documenting the current environment in the form of an IT Universe to better position us for identifying high-risk concerns and providing value.***

37. Is there an expectation to visit all eight campuses?

    ANSWER: ***Yes, this is preferred. However, audio/video calls are acceptable where necessary.***

38. Does USC have a budget estimate or not-to-exceed threshold for this project that you can share? If yes, please provide detail.

    ANSWER: ***No, Offerors should present their best price in the Business Proposal.***

39. Does USC plan to use the new ITIL v4 framework for this engagement, which will be released in February 2019?

    ANSWER: ***The University does not have a specific framework in mind.***

40. RFP Section III. Specifications, Part C. Workpapers, #2 (on page 16 of the RFP): With regards to workpapers being publicly available, will the University determine what workpapers are to be marked as confidential, or is that the responsibility of the selected auditor?

    ANSWER: ***The University will determine this in regards to workpapers. This should not be confused with the Offeror's marking of information it determines to be Confidential within its proposal submitted in response to the Solicitation.***

41. Is Team Central able to be accessed remotely? Will the selected firm's personnel involved with projects be provided sufficient access?

    ANSWER: ***Yes to both.***

42. Is any information security responsibility handled outside of the DoIT?

    ANSWER: ***Yes, however DoIT provides guidance on complying with the state's minimum security requirements.***

43. Is IT a centralized function at each campus?

    ANSWER: ***The Columbia campus has a centralized IT function, however there are several colleges in Columbia that are decentralized. The IT function at the smaller campuses are more centralized than Columbia.***

44. Has the University engaged a previous firm to conduct IT audits as part of an internal audit role? If yes:
    a) Who is/was the vendor(s)?
    b) For how many years has USC worked with this vendor(s)?
    c) When is/was the work conducted?
    d) Please describe the nature of the project(s).
    e) What were the dollar values for this project(s)?
    f) Will the results of prior work be made available to the selected consultant?

    ANSWER: ***No.***

45. Does the University's internal audit team maintain any IT expertise?

    ANSWER: ***The Chief Audit Executive, Assistant Director of IT Audit, and both IT Audit Managers are all Certified Information System Auditors.***

46. Has a previous risk assessment been completed? Was a particular framework used?

    ANSWER: ***A university-wide risk assessment is conducted every three years as a method for developing our three-year audit schedule. These three-year assessments are high level and not technical.***

47. To what extent does the University and specific departments at the University have to be compliant with HIPAA? Have any previous engagements been completed? If yes:
    a) Who is/was the vendor(s)?
    b) For how many years has USC worked with this vendor(s)?
    c) When is/was the work conducted?
    d) Please describe the nature of the project(s).
    e) What were the dollar values for this project(s)?
    a) Will the results of prior work be made available to the selected consultant?

    ANSWER: ***The University has been designated as a Hybrid Entity as it includes both covered and noncovered functions. Yes, see below.***
    a) Pondurance
    b) Less than 1 year

c) 2014

d) Reviewing compliance with regulations where applicable and assisting in identifying units across campus that may be required to comply.

e) Determining the value of the results of the project would be hard to determine. Detailed information can be provided to the Contractor if necessary.

f) Yes, upon request by the Contractor.

48. Will an overall audit plan be established each year that defines expected audits, hours, and scope?

    ANSWER: ***Our audit leadership team reviews and determines expected audits, hours, and scope for its internal audit engagements annually. The same practice would apply in the event the outsourced contract is carried forward annually.***

49. Who will be responsible for tracking remediation efforts after the audits are completed?

    ANSWER: ***Internal Audit***

50. The Scope of Work on page 14 of the RFP outlines four project components:
    1. IT Universe Illustration
    2. Risk Assessment of IT Universe
    3. Specialized Compliance/Operational Audits
    4. Information Security Audits

    However, Section VIII (Bidding Schedule/Price-Business Proposal) on page 38 lists the project components as:

    Engagement #1 – IT Universe Analysis
    Engagement #2 – Risk Assessment
    Engagement #3 – Outsourced IT Services Performance Audit
    Engagement #4 – HIPAA/HiTech Compliance Audit
    Engagement #5 – Information Security Assessments

    Please clarify which list is more accurate and best reflects how we should refer to these project components in our proposal.

    ANSWER: ***Please use Engagement #'s 1 through 5 for your proposal.***

51. Should we be selected as the preferred vendor for this project, what is the University's process to address any issues raised by our contracts compliance during the contract negotiation process?

    ANSWER: ***Yes***

THIS CONCLUDES THE VENDOR QUESTIONS AND RESPONSES.

THE <u>AWARD POSTING DATE</u> HAS BEEN EXTENDED TO APRIL 15, 2019.