Q&A Addendum #2
RFP 715840

Question: RFP, Section 1. We recommend the University consider revising the RFP to allow for the work to be performed in accordance with American Institute of Certified Public Accountants' (AICPA) *Statement on Standards for Consulting Services* instead of as an Agreed Upon Procedures (AUP) engagement. Performing the engagement under the AICPA *Standards for Consulting Services* vs. AUP standards would provide the University increased flexibility and efficiency regarding the project approach, execution, and reporting. Further, under the AICPA consulting standards the selected provider could still assess the University's cybersecurity risk management program and provide similar deliverables to what is requested in the RFP.

Answer: We agree that the engagement should not have been described as an Agreed Upon Procedures (AUP) engagement. The engagement should be conducted in accordance with attestation standards established by the AICPA. We have renamed the RFP. Please see Addendum #2.

Question: RFP, Sections 1 and 2. If the University decides to continue the project in accordance with the AICPA AUP standards and the AICPA *Guide on Reporting on an Entity's Cybersecurity Risk Management Program and Controls*, please clarify the requirement. For instance, per the AICPA's *Guide on Reporting on an Entity's Cybersecurity Risk Management Program and Controls*, under the Purpose and Applicability section, the AICPA designed this attestation service to be performed under AT-C 105, *Concepts Common to All Attestation Engagements* and AT-C 205, *Examination Engagements*. The attestation report deliverable designed by the AIPCA for this service conflicts with the AUP standard requested by the University. If an attestation examination is required by the University the selected provider would need to propose the engagement using AT-C 105 and AT-C 205. Further, AUP standards do not provide for the preparation of descriptions, or conclusions on design, as described as a requested deliverable in the RFP.

Answer: The engagement should be conducted in accordance with attestation standards established by the AICPA. References to an AUP engagement have been removed.

Question: The RFP indicated that this will be performed under the Agreed Upon Procedures standards and then it references the use of the AICPA Guide on Reporting on an Entities Cybersecurity Risk Management Program and Controls. Is it safe to say that the request is for a SOC for Cybersecurity examination as of a point in time, or is it intended to be a true AUP where the University will specify the controls they want tested?

Answer: The engagement should be conducted in accordance with attestation standards established by the AICPA and should be completed using the AICPA's *Guide on Reporting on an Entity's Cybersecurity Risk Management Program and Controls*. The request is for a Cybersecurity Risk Management Examination as of a point in time.

Question: In the Scope of Work paragraph there is this sentence, ". This design–only engagement will include preparing a written description of the University of Arkansas System's current cybersecurity management program". Is the University expecting to have the chosen firm write the description? If so, is the University planning to engage the chosen firm to perform

a Consulting (Readiness) engagement to prepare this? Under SOC standards the University is required to write the description unless contracting with a firm to perform consulting work in helping to prepare this.

Answer: This engagement is not for a SOC report. The engagement is requesting a report prepared in accordance with the AICPA's *Guide on Reporting on an Entity's Cybersecurity Risk Management Program and Controls*.

Question: The RFP indicates there are 21 entities that all maintain a decentralized IT function. Is it expected that there will be a report for each location, or is the intent to combine these into one report?

Answer: There is expected to be a report for each location.

Question: It was noted that the expected completion date would be no later than June 30, 2021. It was also noted that Cohort 1 implementation is expected in July 2020 and Cohort 2 in July 2021. This question relates somewhat to #3 above. If the expected completion of implementation is not expected until 2021 is the intended scope going to be over the systems and processes in place after Cohort 1 is completed or on each individual location given they have decentralized IT functions currently? We understand there may be significant overlap in governance and controls between each location, but wanted to see if there was any further clarification on the reporting scope and timing of assessment.

Answer: The intended scope is not dependent on the implementation of the ERP platform.

Question: Is it expected that onsite visits will be required for each location?

Answer: Onsite visits will be determined by the selected firm.

Question: What is the anticipated start date for the chosen vendor to begin the project?

Answer: We expect the start date to be as soon as possible after the Contract Award date.

Question: Can the University please confirm the dates of the contract term?

Answer: The term of any resulting Services Contract will begin upon date of Contract Award. If mutually agreed upon in writing by the Contractor and UA, the initial term shall be the shorter of the successful completion of the engagement, or no later than the end of the biennium, June 30, 2021.

Question: What does the University of Arkansas have budget for this project?

Answer: Budget information is not disclosed during the RFP procedure.

Question: Who is the current incumbent?

Answer: This is a new engagement.

Q&A Addendum #2
RFP 715840

Question: What security frameworks does the university currently have implemented for controls and governance (COBIT, ITIL, NIST, RMF, etc)?

Answer: Security frameworks vary by campus.

Question: What is the approximate number of systems that are in scope for the audit?

Answer: The number of systems vary by campus.

Question: Is Workday the intended target of the engagement or are there other systems/controls to be assessed as well?

Answer: Workday is not the intended target. This engagement is for a Cybersecurity Risk Management Examination.

Question: Are there any third-party vendors that manage some of the controls in place?

Answer: The use of third-party vendors varies by campus.

Question: Are the use of cloud services in scope?

Answer: This engagement is for a Cybersecurity Risk Management Examination.

Question: Is wireless a part of the assessment?

Answer: This engagement is for a Cybersecurity Risk Management Examination.

Question: How many applications are in scope?

Answer: This engagement is for a Cybersecurity Risk Management Examination.

Question: Have there been prior assessments done and will those results be made available to the winning contractor?

Answer: Prior assessments have not been done.

Question: Can you clarify the statement: "This design–only engagement will include preparing a written description of the University of Arkansas System's current cybersecurity management program (consisting of policies, procedures and established internal controls) and evaluating the current design of the University of Arkansas System's cybersecurity management program related to best practices and IT industry standards

governing cybersecurity control objectives."? Does "design-only" mean that you are looking for a process to do the work while another entity does the actual work?

Answer: No. The engagement is requesting a report prepared in accordance with the AICPA's *Guide on Reporting on an Entity's Cybersecurity Risk Management Program and Controls*.

Question: How specify the number of locations to be covered under the scope? If there are multiple buildings in the same site, then please list these as individual physical locations. (H.O & other locations)

Answer: Please see Attachment A.

Question: Whether the company/institution is ISO27001 certified or any other certificates available or compliant to any international standards such as ITIL, BS 15000,PCI-DSS, ISO 27001, ISO 9001:2008, etc.?

Answer: Security frameworks vary by campus.

Question: What is the total strength of staff at each location?

Answer: This information can be provided to the selected firm as part of the engagement.

Question: How many business units or departments are there at each location? Kindly provide the organizational chart, if available.

Answer: This information can be provided to the selected firm as part of the engagement.

Question: Please list-down/share the security policies currently being complied to.

Answer: This information can be provided to the selected firm as part of the engagement.

Question: Is the organization covered under any regulatory guidelines such as Sarbanes-Oxley or EU Data Privacy etc?

Answer: The organization is covered by numerous regulatory guidelines.

Question: Please share the attachment-A or the source to obtain the same.

Answer: Attachment A is available at Hogbid.uark.edu.

Q&A Addendum #2
RFP 715840

Question: Is the final report (the AUP or the NIST Cybersecurity Framework Evaluation) intended to be shared with a third party, or is the final report for management's consideration?

Answer: The final report is for management's consideration.

Question: Does UA System intend to undergo a System and Organization Controls (SOC) for Cybersecurity examination in the future? If so:

a. Is the scope of work in the RFP intended to be a readiness engagement for a future SOC for Cybersecurity examination in the future?

b. Would the NIST Cybersecurity Framework be the basis for the description/control criteria for the SOC for Cybersecurity examination?

Answer: There is not an intent to undergo a SOC for Cybersecurity at this time.

Question: Does the UA System intend to provide an assertion if an AUP engagement is selected?

Answer: The engagement should be conducted in accordance with attestation standards established by the AICPA. References to an AUP engagement have been removed.

Question: In regards to evaluating the design of the Cybersecurity Management Program, is the UA System looking for:

a. findings as to whether or not the UA System meets the NIST Cybersecurity Framework; or

b. findings as to whether or not the UA System meets the NIST Cybersecurity Framework **and recommendations** for how to implement or improve controls to implement and adopt the NIST Cybersecurity Framework?

Answer: The engagement is requesting a report prepared in accordance with the AICPA's *Guide on Reporting on an Entity's Cybersecurity Risk Management Program and Controls*.

Question: Are there any IT services, policies, or functions that are shared among the 21 universities, colleges, and units in the UA System?

Answer: There are some shared IT services, policies, or functions among the 21 locations.

Question: Has a target date been identified for when the final deliverables for the scope of work should be completed?

Answer: The term of any resulting Services Contract will begin upon date of Contract Award. If mutually agreed upon in writing by the Contractor and UA, the initial term shall be the shorter of the successful completion of the engagement, or no later than the end of the biennium, June 30, 2021.

Q&A Addendum #2
RFP 715840

Question: Has the UA System adopted the NIST Cybersecurity Framework as their information security standard system-wide? If no, what standard has the UA System adopted, if any?

Answer: IT standards may vary by campus.

Question: Will the UA System provide a project resource or liaison for the successful bidder to assist in coordinating this effort at the System-level?

Answer: We expect the successful bidder to work with each location to obtain the information needed to complete the engagement. Contacts at each location will be provided.

Question: Sections 3 (Costs/Pricing), 10.16 (Period of Firm Proposal), and Appendix II (Official Price Sheet) state that pricing must be valid for 180 days following the proposal due date. Section 8 (Evaluation and Selection Process) states that proposals must be valid for 90 days. Is it correct that the validity of the proposal and pricing have different timeframes?

Answer: No. The timeframe should be 180 days in both places. This has been corrected in Addendum #2.

Question: Do we need to complete and return a Voluntary Product Accessibility Template ("VPAT") as part of our proposal?

Answer: The VPAT is not applicable to this RFP.

Question: Do you desire the selected consultant give and/or facilitate any presentations to UA System project leadership and/or stakeholders during the course of the project?

a. If yes, at what milestones and to what audiences?

Answer: Presentations are not anticipated at this time.

Question: Per Section 7.2 of the RFP, we understand that we are to organize our proposal to address information in the same order as the RFP. There are some topic areas that appear in multiple sections of the RFP. For example:

a. References are mentioned in Sections 4, 14, and Appendix I.

b. The scope of work is mentioned in Sections 2 and 14.

Section 14 of the RFP could be construed as a partial proposal outline. Is that correct—or—where the same information is requested in more than one location, should we respond where it is mentioned first?

Answer: The responses should be according to Section 14.

Question: Regarding the indemnification language in Sections 10.5 and 11 of the RFP: We are an accounting and consulting firm. AICPA guidelines prohibit accounting firms from

indemnifying attest clients for damages, losses, or costs that relate, directly or indirectly to an attest's client's acts. Given this prohibition, would the University consider removing the indemnification requirements contained on pages 7 (Section 10.5) and 14 (Section 11) of the RFP?

Answer: We do not interpret this language to mean that the firm selected would indemnify the University against any losses caused by the University.

Question: How many distinct policies will need review?

Answer: The number of policies varies by campus.

Question: How many pages of documentation will be provided for review?

Answer: The documentation to be provided will vary by campus.