Addendum #2
Agreed Upon Procedures for Cybersecurity Risk Management Engagement
RFP R715840

This document provides adjustments and clarification pertaining to the above captioned RFP and will be updated as necessary.

REMINDER: It is the Respondent's responsibility to thoroughly read and examine the entire RFP document and any addenda to this RFP.

Posted August 13, 2019

The RFP title has been rewritten as follows:

Cybersecurity Risk Management Engagement

Section 1 has been rewritten as follows:

1. DESCRIPTION AND OVERVIEW OF RFP

The Chief Audit Executive of the University of Arkansas System is requesting proposals from qualified firms to perform a design-only cybersecurity risk management engagement to evaluate the University of Arkansas System's cybersecurity policies, procedures and established controls. The engagement should be conducted either 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* or an evaluation of controls using the National Institute of Standards and Technology's (NIST) Cybersecurity Framework.

Section 8 and 8B has been rewritten as follows:

8. EVALUATION AND SELECTION PROCESS

It is the intent of the UA to award a Contract to the Respondent(s) deemed to be the most qualified and responsible firm(s), who submits the best overall Proposal based on an evaluation of all Proposal responses. Selection shall be based on UA assessment of the Respondent's ability to provide adequate service, as determined by the evaluation committee elected to evaluate proposals. UA reserves the right to reject any or all Proposals or any part thereof, to waive informalities, and to accept the Proposal or Proposals deemed most favorable to UA. Where Contract negotiations with a Respondent do not proceed to an executed Contract within a time deemed reasonable by UA (for whatever reasons), UA may reconsider the Proposals of other Respondents and, if appropriate, enter into Contract negotiations with one or more of the other Respondents. Proposals shall remain valid and current for the period of one hundred eighty (180) days after the due date and time for submission of Proposals. Each Proposal will receive a complete evaluation and will be assigned a score of up to 100 points possible based on the following items:

Addendum #2
Agreed Upon Procedures for Cybersecurity Risk Management Engagement
RFP R715840

B. Contractor's Expertise and Qualification (60 Points)
Respondent with highest rating shall receive sixty (60) points. Points shall be assigned based on factors within this category, to include but are not limited to:

- Experience and description of either an attestation engagement of comparable size or evaluation of controls using the NIST Cybersecurity Framework
- References
- Training and certification of assigned support.

Section 9 has been rewritten as follows:

9. CONTRACT TERM AND TERMINATION

The term ("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. Should the University decide to request additional services beyond the scope of this RFP, the contract may be renewed for up to seven (7) years from the original start date (upon mutual agreement between the Contractor and UA and completion of an Addendum to the Services Contract).

Section 14 has been rewritten as follows:

14. SPECIFICATIONS / GOALS AND DELIVERABLES

Each Proposal should contain the following information at a minimum:

- Number of employees in office and experience providing cybersecurity services;
- Listing of at least three client references with specific names and phone numbers; and
- Names, levels and resumes of the specific employees who will provide services under this contract with the University of Arkansas.
- Refer to Sections 1 & 2 of RFP (Description and Scope of Work):
    - The bidder must bid on either
        - The engagement 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*
        - Or an evaluation of controls using the NIST Cybersecurity Framework.