**This document provides adjustments and clarification pertaining to the above captioned RFP and will be followed by additional addenda if necessary.**

**REMINDER:** It is the Respondent's responsibility to thoroughly read and examine the entire RFP document and all Addendum documents as posted to the HogBid website <https://hogbid.uark.edu/>.

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 will be either an Agreed Upon Procedures (AUP) engagement performed under the American Institute of Public Accountants’ (AICPA) Statements on Standards for Attestation Engagements, section AT-C 215, *Agreed Upon Procedures Engagements* or an evaluation of controls using the National Institute of Standards and Technology’s (NIST) Cybersecurity Framework.

Section 2 has been rewritten as follows:

**2.** **SCOPE OF WORK**

UA is issuing this RFP to solicit proposals for a term contract with a qualified firm, pursuant to the specifications, terms, and conditions stated in this RFP. The University of Arkansas System is requesting a report be prepared and issued utilizing either the AICPA’s *Guide on Reporting on an Entity’s Cybersecurity Risk Management Program and Controls or the NIST Cybersecurity Framework.* 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.

 The University of Arkansas System includes seven universities, seven community colleges, and seven additional units that all maintain a decentralized IT function. (See Appendix III).

 The University of Arkansas System is moving to a shared ERP platform and has selected the Workday software solution to implement. Workday will be implemented in two major phases, organized into cohorts. Cohort 1 is scheduled for deployment in July 2020 and cohort 2 is scheduled for deployment in July 2021.

Section 6 has been updated as follows:

**6. PROJECTED TIMETABLE OF ACTIVITIES**

 The following schedule will apply to this RFP, but may change in accordance with the UA's needs:

 July 29, 2019 RFP released to prospective respondents

August 9, 2019 4:00 PM CST Last date/time UA will accept questions

August 15, 2019 Last date UA will issue an addendum

August 27, 2019 Proposal submission deadline 2:30 PM CST

 September 30, 2019 Notice of Intent to Award

 Upon Contract Approval: Service to Commence

Section 8B has been rewritten as follows:

**8. EVALUATION AND SELECTION PROCESS**

1. **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 Agreed Upon Procedures (AUP) engagements of comparable size or evaluation of controls using the NIST Cybersecurity Framework
* References
* Training and certification of assigned support.

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 Agreed Upon Procedures (AUP) engagement to be performed under the American Institute of Public Accountants’ (AICPA) Statements on Standards for Attestation Engagements, section AT-C 215, *Agreed Upon Procedures Engagements*. The AUP is necessary to enable firms to perform the cybersecurity risk management examination as set forth in 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.