UNIVERSITY OF ARKANSAS SYSTEM

Addendum 7
Identity and Access Management Services – Phase 2
RFP 644456

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

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

AMENDMENTS TO RFP LANGUAGE. The following sections of the RFP have been amended. Replace these sections with this amended language and use this new language as your firm drafts its response for Phase 2. The new or modified parts of the section are highlighted for convenience.

12.2 Evaluation Criteria for Phase 2 (Implementation Services)

A. Project Approach and Methodology (30 Points)

Respondent with the highest rating may receive up to thirty (30) points. Points shall be assigned based on factors within this category, to include but are not limited to:

- Ability to implement the appropriate functionality and interfaces with onsite Active Directory services
- Ability to meet System timeline and requirements
- Completeness of approach proposed
- Fit of methodology to System needs
- Demonstrated quality of methodology from similar engagements
- Training approach for users, operators, and administrators
- Implementation plan to meet HIPAA, FISMA, and FEDRAMP systems
- Implementation plan for PW, SSO, and 2 factor authentication using on site systems

B. Firm Qualifications and Experience (20 Points)

Respondent with highest rating may receive up to twenty (20) points. Points shall be assigned based on factors within this category, to include but are not limited to:

- Quality of firm references
- Stability of company business and financials
- Successful implementations/services at similar organizations
- Compliance with System experience requirements and standards
- Previous experience with HIPAA, FISMA, and FEDRAMP systems
- Previous experience with PW, SSO, and 2 factor authentication using on site systems

C. Proposed Project Team Experience (20 Points)

Respondent with the highest rating may receive up to twenty (20) points. Points shall be assigned based on factors within this category, to include but are not limited to:

- Quality of project team experience and references
- Previous experience in similar role
- Previous experience with solution to be implemented
- Team members are certified and/or trained in HIPAA, FEDRAMP, and FISMA Compliance
- Previous experience and/or training in Cloud Solutions other than IAM systems
- Previous experience and/or training in Web Site Protection

D. Cost (30 Points)

Points shall be assigned for the cost of the specific components and services, which comprise the overall system, including annual maintenance cost and training, as follows:

- Cost points will be assigned on the Total Cost of Ownership reflected on the Summary Presentation schedule of the Cost Proposal, for comparison and evaluation purposes.
- The bid with the lowest estimated cost of the overall system will receive the maximum points possible for this section.
- Remaining bids will receive points in accordance with the following formula:

  (a/b)(c) = d

  a = lowest cost bid in dollars

  b = second (third, fourth, etc.) lowest cost bid

  c = maximum points for Cost category (30)

  d = number of points allocated to bid

Failure of any Respondents to provide in their proposals any information requested in this RFP may result in disqualification of the proposal and shall be the responsibility of the Respondent.

14.4 IMPLEMENTATION SERVICES SCOPE (RFP PHASE 2)

This implementation services scope section provides a high-level description of the services to be included in the proposal. General project activities that will be included in each stage of the project include:

Plan

- Project Management
- Project Team Training
- Other Planning and Preparation
- Team Training and Methodology

Architect

- Analysis
- Solution Design

Configure and Prototype

- Software Configuration

- Integration and Interfaces
- Data Conversion
- Reports, Queries, and Forms

Test

- Testing

Deploy

- Administrator Training and Knowledge Transfer
- Transition Support
- Documentation
- Implementation/Deployment (roll-out) Support
- Post-implementation Maintenance and Support

The implementation scope encompasses the following outcomes for all institutions in the System:

1. All System units are connected to IAM, using it instead of any prior processes for account creation or identity management. IAM is the source of authority for identity.
    a. Connected to new ERP platform
    b. Connected to all unit-level directories
2. Identity life cycles are defined and operating.
    a. Provisioning & de-provisioning are automated.
    b. Identity and access governance processes are consistent and being used throughout the System
3. Audit and compliance reviews are automated, and produce relevant documentation.
4. Audit and access control tools produce effective event logging to assist SIEM (Security Information and Event Management) tools
5. ID card systems rely on IAM for information. IAM exploits ID cards to control building access and possibly computer access, based on the needs and abilities of each unit.
6. Each person has the ability to manage their relationships with the System and their local campus or unit though self-service account/attribute management.
7. Multi-factor authentication is available to all users at all units through existing on-site multi-factor system and is enabled by policy for individuals in high-risk positions.
8. Federated single sign-on (SSO) is in use at each unit, providing authentication and identity attributes to aid access control. The following minimum subset of services is available from each unit via the existing on-site SSO system:
    a. ERP (Enterprise Resource Planning) system
    b. LMS (Learning Management System)

c. Helpdesk / ITSM (Information Technology Service Management) tools
d. Campus portals
e. Email & Collaboration tools
f. File sharing
g. Residence housing
h. Student Success
i. Emergency notification
j. InCommon Federation, Internet2 and EDUCAUSE services

9. Each person holds a single identity that is valid throughout all institutions in the System, while still preserving the unique "identity" or spirit of each campus or unit.
10. Roles and access control are actively managed and automated. IAM is the source of authority for role definition.
    a. General roles are defined and governed at the System global level
    b. Each unit has delegated authority to create and govern its own rule structure
11. Documentation is supplied to System and units as appropriate.
12. Training is completed for System, users, operators, and unit personnel. Long-term training refresher arrangements are made.
13. Disaster recovery plans are in place and have been tested
14. Use existing on-site PW system.
15. Ensure System meets compliance with HIPAA, FISMA, and FEDRAMP.
16. Implement the appropriate functionality and interfaces with onsite Active Directory services

These services are addressed in more detail in RFP Appendix 6, *Model Statement of Work*, and will be finalized in the agreements between the System and the Respondent.

14.5 IMPLEMENTATION SERVICES STAGES (RFP PHASE 2)

The System expects to roll out the new IAM solution in stages, with the first stage including only certain institutions with certain functionality. The first stage (Stage 1) is further defined below.

Due to the complexity and variability of implementation across the System's member institutions, the System has specified a first stage for implementation for which it will require a fixed fee bid. As part of the response to this proposal, the Respondent shall provide a Stage 1 Statement of Work. The Respondents should use the *Model Statement of Work* (RFP Appendix 6) as a starting point for the Phase 1 Statement of Work submitted with their proposals. If additional analysis of the current environment for the Stage 1 participants is required, those services shall be included in the fixed fee bid for Stage 1.

Also, the initial services scope during Stage 1 includes a deliverable from the awarded services vendor to analyze all parts of the implementation not in the first stage (functionality and institutions) and develop a Statement of Work and timeline to complete the deployment across the System. (See RFP Section 14.5.4 below.) It is expected that upon completion of the analysis deliverable during Stage 1, the System and Contractor will negotiate a fixed fee for the subsequent stage(s) of implementation services.

Also, for Phase 2 the ability to implement the appropriate functionality and interfaces with onsite Active Directory services

At the completion of the first stage of deployment, the System expects that the Statement of Work for subsequent stages will have been completed and the fixed fee for subsequent stages agreed so that the services vendor may continue the IAM deployment uninterrupted.

Although the deployment will be staged by institution, the System expects that all institutions will participate in the initial design sessions. It is important that the design that is initially deployed is suitable for later deployment throughout the System without requiring modifications to the configuration of the initial institutions.

14.5.3 Stage 1 Functionality Scope

The System suggests the following scope for the first stage of the deployment. The first stage scope has been broken into two segments, although the Respondent may choose to deploy this functionality in one segment instead.

Stage 1, Segment 1. At the end of Segment 1, the new IAM platform will be managing all identities for the campus and will be integrated with the new ERP; and the old ERP platforms may be retained for legacy integration, but will not be actively managing identity in any way. End users will experience this change through improved password reset tools and password policies, and through initial single sign-on service offerings.

1. Identity Life Cycle and Governance
    a. Integration with existing sources of identity information
    b. Integration with existing directories and other consumers of identity information (account provisioning)
    c. Integration with new ERP platform as soon as it is available
    d. Workflows and automation for creating identities, delegating attribute authority, and provisioning accounts
    e. Workflows and automation for deprovisioning accounts and archiving identities
2. Role Based Access Control
    a. Role discovery and mapping
    b. Governance and procedures for managing role registry
    c. Workflows and automation to assign and remove roles from an individual based on business rules
    d. Workflows and automation for mapping roles to downstream access control structures

3. Self-Service password reset
    a. Use existing on-site PW System
4. Federated Single Sign On
    a. Implement SAML Identity Provider
    b. Join InCommon Federation
    c. Identify and prioritize SAML-capable services
    d. Transition a representative set of services to SAML SSO

Stage 1, Segment 2. At the end of Segment 2, end users will have access to stronger authentication through two-factor authentication tools, and easier access to special access environments through a request-based workflow that makes it easy for those managing access to approve and re-verify access.

1. Multi-Factor Authentication
2. Account Isolation and Credential Revocation
    a. Workflows and automation to scramble passwords, and other credentials when compromised
    b. Workflows and automation to freeze account access based on various criteria
3. Requestable Roles
    a. Workflows and automation to enable users to request access to roles not granted by birthright or business rules
4. Access control review and reattestation
    a. Workflows and automation to support periodic review and reattestation of access rights for a user and access control implementation per platform

If additional analysis of the current environment for the Stage 1 participants is required, those services shall be included in the fixed fee bid for Stage 1.

Additional functionality offered by the IAM solution will be implemented in later stages of the project.

17.7 Tab 5: Implementation Services. The Respondent will provide narrative responses regarding the proposed implementation services, organized in accordance with the outline below.

Project Management Methodology and Approach

1. The Respondent shall describe its approach to managing the project. As part of its project management approach, the Respondent shall describe the project management tools, standards, controls, and procedures that will be utilized to create a proven, reliable process, as well as proposed standards for status reporting, risk management, issue management, and communications.
   Respondents are invited to provide recommendations for project governance in this section of their response.

Timeline and Implementation Approach

2. The Respondent should describe its proposed implementation approach for Stage 1 of the implementation project. Respondent should provide a high-level work plan

demonstrating the relationship between the work to be performed, the deliverables to be provided as described, and the timeline recommended in your approach. This section shall encompass all services and deliverables identified in RFP Section 14.4, *Implementation Services Scope (RFP Phase 2)*, and RFP Section 14.5, *Implementation Services Stages (RFP Phase 2)*.

Describe in your narrative how your recommended approach will reduce risk to the System and facilitate System-wide deployment and user acceptance. In this section, Respondent should discuss its approach to complete the analysis deliverable discussed in RFP Section 14.5.4 that will support the creation of a Statement of Work for subsequent phases of the project.

The description provided should include the following information:

- Key principles and distinguishing characteristics;
- Phases and major activities;
- Recommended testing phases;
- Implementation timeframes; and
- Proposed deliverables.

Specific Services

3. Describe any pre-implementation activities the System could take to prepare for the implementation project.
4. Describe any tools, utilities or special access that the implementation will require for the implementation project, whether service is being done on-site or off-site.
5. Regarding the Respondent staff assigned to the project:
   a) Discuss if the members of the team are certified and/or trained in HIPAA, FEDRAMP, and FISMA Compliance
   b) Discuss if there are personnel on the team that have experience and/or training in Cloud Solutions other than IAM systems
   c) Discuss if there are personnel on the team that have experience and/or training in Web Site Protection
6. Discuss Scope and Methodology of User, Operator, and Administrator training. List the recommended training by role for the System's project resources, and the recommended timing for this training. If there are options for delivery, discuss those options here. The System expects the Respondent's bid to include the training costs for the System project team (not including any travel expense). Include any additional costs as a line item on the Cost Proposal.
7. Is there documentation for review before implementation begins? If so, describe what the documentation is available.
8. Describe the process for customization of reports, workflows, or similar items during implementation.
9. Describe security features that are configured during implementation.
10. Are any role discovery tools in operation during implementation? If so, which ones?
11. Describe any procedures typically put in place to protect legacy systems and data during implementation.

12. What training is recommended for key System administrative and support staff who are not part of the project team? Include recommendations/information for training material and delivery approach. Include any additional costs as a line item on the Cost Proposal.
13. Discuss how role-based authorization is implemented in the proposed solution.
14. Describe how session management is implemented in the proposed solution.
15. Describe your firm's ability to implement the appropriate functionality and interfaces with onsite Active Directory services.
16. Describe any training material that will be available to the System post-implementation. Include a description of the training subject and delivery method. Include any additional costs as a line item on the Cost Proposal.

All else regarding this RFP solicitation remains as is. Further questions concerning all matters of this RFP should be sent via email to:

Whitney Smith, Procurement Coordinator
Office of Business Services
wesmith@uark.edu