UofA
UNIVERSITY OF ARKANSAS SYSTEM

Addendum 3
Identity and Access Management Software and Services
RFP 644456

This document provides updated information and clarification pertaining to the above captioned RFP and the Pre-Proposal conference held June 15, 2017.

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

POSTED 6/22/17: Q&A Information

1. Whether companies from Outside USA can apply for this? (like, from India or Canada)
   RESPONSE: Non-US companies can submit RFP responses. The minimal expectation is that all communications occur in written and spoken English.

2. Whether we need to come over there for meetings?
   RESPONSE: The respondent should indicate which activities will occur on-site and which activities will occur remotely.

3. Can we perform the tasks (related to RFP) outside USA? (like, from India or Canada)
   RESPONSE: The respondent should indicate which activities will occur on-site and which activities will occur remotely.

4. Can we submit the proposals via email?
   RESPONSE: No.

5. We have been requested to participate in the RFP and while [firm] works with certified SMEs in many security solutions and have overseen IT projects on this scale, we are staffing and project partnership experts, not an integration partner for one specific solution. If the Subject Matter Experts that we put in place to run the project are demonstrably certified by the solution vendor and have implemented solutions on this scale, would [firm] be able to be considered on that basis, or would [firm] have to be an integration partner for the solution in question?
   RESPONSE: We would like to modify the response we have at the conference. Because this is a deliverables-based service contract, we expect the services firm to shoulder responsibility for outcomes, not just supply effort. Therefore, we expect the firm to be well-qualified to work with our selected product. If the software manufacturer has an accreditation or partnering program, we expect the selected services firm to have this relationship with the software firm.

6. The file labeled RFP643699_UASYS_IAM_Appendix2_CampusMetrics.pdf details the user totals per campus. At the bottom of the chart there is a row for Category Total. The

totals across any of the rows do not match the numbers in the Campus Total Column. Can you please provide clarification around that?
RESPONSE: Some column counts are included in the counts for other columns: The “Students” column counts all students, including “incoming students.” The “total alumni” column counts all tracked alumni, including “new alumni.” The “campus total” column sums employees, students, applicants, and “total alumni.”

7. There is mention in the RFP of Federated Single Sign-On. Would you happen to know how many Federations will need to be deployed to satisfy the University of Arkansas use cases?
   RESPONSE: There will be at least two Federations, however, consider this number unbounded. We hope to see recommendations based on your expertise.

8. There is mention for integration with a Security Information and Event Manager. Which SIEM does the university currently use or will this be a future purchase?
   RESPONSE: Fayetteville uses Splunk, the other campuses may be using different tools. Some campuses may not have a SIEM tool in place.

9. Approximately how many downstream target systems are there?
   RESPONSE: At a minimum, expect a directory (Active Directory or LDAP) and a Learning Management System (LMS) (Blackboard or similar) per campus. We expect authentication to go through standard systems (AD/Kerberos, SAML, RADIUS), so they will not be counted. Some additional downstream provisioning is expected, but these numbers are unknown.

10. What is the primary System(s) of Record?
    RESPONSE: The IAM platform will be the system of record for identity once it is established. We expect the new ERP platform to be authoritative for the attributes it manages.

11. Multi-Factor Authentication (MFA), aside from One Time Passcodes are there requirements for integration with 3rd party MFA solutions?
    RESPONSE: We desire a complete MFA solution that integrates with desktop login, federated single sign-on (SSO), and other authentication mechanisms. We prefer systems that implement open standards.

12. Is Reverse Password Synchronization required?
    RESPONSE: While not required, we desire the ability to synchronize passwords between campus directories and the IDM.

13. Is a vendor precluded from participating in Phase 2 (implementation) if they respond to Phase 1 (software/SaaS) and are the winning vendor?
    RESPONSE: No. Any vendor that participated in the pre-proposal call may respond to either phase, or both phases. Vendors may also submit a combined bid addressing both phases.

14. We are assuming BASIS is the locally developed mainframe application. If that is the case, what is the platform? RACF? Other? Please explain the integration via "scripts" to combine the SIS and BASIS data to form a single identity in a bit more detail. Which language is used? Do you expect your vendor to replace the scripts used to export the information from the mainframe and SIS?
    RESPONSE: (This answer applies to the Fayetteville campus.) The BASIS application is developed in Natural and ADABAS, providing both 3270 (green screen) and web-based interfaces. RACF authenticates 3270 sessions, and LDAP authenticates web sessions. Nightly batch processes on the mainframe and in the PeopleTools environment synchronize information between the two systems, and produce a flat file is used to provision accounts in LDAP and Active Directory. We expect the chosen solution to be able to supplement these capabilities as the current Mainframe and PeopleSoft systems are transitions to the new ERP platform.

15. It appears you have a fairly extensive Authentication infrastructure. Which specific components will be replaced by your vendor of choice? Please further describe your desired future statue for your authentication infrastructure and user experience.
    RESPONSE: Not all campuses have the same authentication infrastructure. We desire a system capable of providing all authentication functions. If the chosen solution lacks desired functionality, we will explore integrating third party tools with the chosen implementer.

16. Do you want to maintain the batch processing for SAP or look to introduce more direct, seamless integration and eliminate the FTP step?
    RESPONSE: The goal with any such integration is to remove latency from the process, moving away from batch processing toward more real-time flows.

17. Will users that are both faculty and staff have two domain accounts? How would you like to handle multiple affiliations for both authentication and domain access?
    RESPONSE: We envision a single account per user. Most, if not all, campuses already use a single domain. We envision that affiliations will be expressed via roles or other attributes, and that these attributes will be used with a rules engine to determine the state of each individual's affiliation with each campus.

18. Are you looking to combine all 5 campus into a single IAM solution or do you foresee separate instances for each campus?
    RESPONSE: We hope to see recommendations based on your expertise. We envision a unified IAM solution for the entire system. The goal is to enable an individual to begin their affiliation with one campus and transfer from there to multiple campuses thereafter. An individual may have many roles at several campuses simultaneously. In all cases, we want to view that individual as a single entity from the perspective of IAM. Respondents may choose to propose a single-tenant approach, a multi-tenant approach, or any other approach that addresses the System's goals.

19. Is vendor registration mandatory for this bid? If yes, then by what date, can I register Infosys with your procurement department?

RESPONSE: Complete the VII form (as provided in the RFP) and submit the completed form with your bid. That's the form we need to register your vendor in our system.

20. In the section 14.2, Software scope of RFP Phase 1 is provided. However as we understand, in RFP Phase 1 we only need to suggest the solution along with the subscription/licensing/hosting cost. The implementation cost of this scope is to be provided in the RFP Phase 2. Please confirm.
    RESPONSE: This is correct.

21. What is the number and type of sources of identity that need to be integrated to the IDM system?
    RESPONSE: The primary identity source will ultimately be the new ERP system. However, each campus has existing IDM systems that will need to have their information preserved. Respondents should plan to migrate that information, and for their proposed IDM system to replace any identity/account generation tools currently in place as each campus transitions to the new ERP platform. Refer to the Appendices 1 and 5 for examples of systems in use. Expect other campuses in the same class (2-year vs. 4-year) to have similar platforms in use.

22. What is the number and type of target systems for identity provisioning to be integrated to the IDM system?
    RESPONSE: Please refer to our answer to question 9.

23. What is the new ERP system that needs to be integrated?
    RESPONSE: The RFP for the new ERP system has not announced its intent to award. The finalists are Oracle Cloud and Workday.

24. What is the approximate number of identity provisioning workflows needed to be setup?
    RESPONSE: We expect to need at least 3 workflow types: an automatic full flow that provisions most (if not all) attributes, e.g. into a directory; an automatic partial flow for provisioning account information into a downstream application, and a manual/ad-hoc flow for provisioning special-use or local accounts, e.g. for conferences, workshops, summer camps, etc.

25. What is approximate number of different type of roles that need to be setup?
    RESPONSE: We envision many hundreds of roles will be needed per campus. We envision a layered role design, where certain roles (e.g. "student") are more general and may apply to all campuses, while other roles are specific to a campus and may not make sense or be visible beyond its scope.

26. What is the scope of Multi-Factor Authentication?
    RESPONSE: We envision Multi-Factor Authentication (MFA) to be available at all campuses, to all users, including students, and required for some individuals whose risk score is higher. The proposed MFA solution may replace the extant system at UAMS. We prefer a solution that provides a variety of MFA methods (e.g. SMS, smart phone app, token, fob, smart card), but we choose not to make any of these required. We envision an MFA solution capable of performing "step-up" authentication, that is, an authentication

system that allows single factor for low-risk users or activities, but returns to request the second factor when it becomes needed.

27. What is the approximate number of approval workflows for roles and access provisioning that need to be setup?
    RESPONSE: We expect to need at least two workflow types for role and access provisioning: An automated flow that assigns roles or access based on an individual's attributes and a set of rules; and a manual flow that allows individuals to request certain roles or access, but have that access approved, either by automated process, or by human review and approval.

28. How many different pre-prod environments need to be setup- Dev, SIT, UAT?
    RESPONSE: We hope to see recommendations based on your expertise. We believe this number to be solution-specific; respondents should propose the structure they feel best meets our other needs. However, we expect to have at a minimum a separate instance to test and train with that does not operate on live data. A method of testing or simulating the effects of large changes on our live data set is also desired.

29. Any preference to specific Cloud platform for hosting the IAM solution?
    RESPONSE: No preference.

30. What is the current authentication system/mechanism and user directory being used?
    RESPONSE: This varies by campus. See Appendices 1 and 5. Common current platforms include LDAP, Active Directory, and Google Apps for Education. In some locations, authentication may be performed locally, rather than against a directory-borne credential.

31. What are different types of authentication mechanism that are required?
    RESPONSE: We expect all campuses to be interoperable, and to use industry standard protocols such as Kerberos, SAML, and RADIUS. Some public key or certificate-based authentication may be used in certain areas. We desire to deprecate LDAP as an authentication mechanism where possible, because of its lack of true AAA functionality. We desire to implement Multi-Factor Authentication at all campuses, and for all authentication mechanisms (AD/Kerberos, SAML, RADIUS).

32. Is there a requirement for coarse/fine grain access management or only Single Sign On is required?
    RESPONSE: We expect federated SSO to support the assertion of entitlements, roles, group memberships, and other salient attributes, as each application needs these, either for authorization purposes, or for just-in-time provisioning.

33. What are different types of Multi-Factor Authentication mechanisms that need to be supported?
    RESPONSE: We desire flexibility in the MFA mechanism, to improve the end-user experience. Without requiring any specific mechanism, we are interested in seeing both a "lowest common denominator" solution, such as SMS or phone call, as well as a more user-friendly method such as a smart phone application, a physical token, or smart card.

Smart cards that can double as a campus ID card may be considered as well. Respondents may suggest any mechanisms they feel will meet the System's needs.

34. Is Risk based and Adaptive Authentication required?
    RESPONSE: While not required, risk scoring, adaptive authentication, and step-up authentication are desired features. We desire to identify varying risk in individuals, tasks, and data, and adjust security requirements accordingly. We may choose to vary password lifetime for low- or high-risk individuals, permit single-factor authentication for low-risk activity, but step up authentication with a second factor if privileged actions are to be performed.

35. Is there a requirement of Privileged Access Management?
    RESPONSE: Privileged Access Management (PAM) may be proposed for both root and other administrative account control, as well as for the management of shared accounts.

36. [Firm] will have several respondents potentially to this RFP, we're working with several partners on responses currently. Is it ok for me to join the call today and represent multiple potential responses?
    RESPONSE: Yes.

37. I just missed the pre-proposal conference due to a flight delay. Are we still able to respond to RFP 644456 for Identity and Access Management Software and Services?
    RESPONSE: Unfortunately, since [firm] was not represented on the pre-proposal call this morning we will not be accepting a bid submission directly from [firm]. However, if [firm] will be partnering with another company that was represented on the call, then we can accept a joint bid as submitted by that partner.

38. Whitney, a question that came up on our internal post review call today was around services. At this point UARK still has a few considerable unknowns. Building services around these unknowns leaves a lot of room for interpretation. For example, the [product] has over 5,000 pre-integrated applications like Workday. If UARK chose Workday as their ERP solution this would reduce the services needed to install [product]. We do not want to miss-represent our services or build unnecessary cost into the services proposal. Question: Will UARK be able to address these unknowns prior to the bid date and leave room to adjust to these updates? If not, how would UARK suggest a respondent to go about the proposal give these unknowns?
    RESPONSE: In the specific case of the ERP, we suggest that vendors may want to address their solution's approach to both ERP finalists, Oracle and Workday. For other unknowns, we are unable to offer guidance.

39. In RFP643699_UASYS_IAM_Appendix4_Requirements.xls, User interface and experience, line 92: "The solution provides a complete IoT/mobile experience." Are we talking about devices provisioning or about MDM features/end users experience? How important is this feature to you?
    RESPONSE: This requirement is not meant to address any MDM need. We desire a solution that is built with mobile performance in mind. If the user interface is browser-based, the system should work with any modern browser, and should work on mobile

platforms (phone, tablet). If a smart phone app is available, please indicate that. References to IoT are intended to represent the collection of technologies outside of normal desktop, client/server, and mobile interactions. This may include building access control, kiosks, printing, campus safety, audience response ("clickers"), and other similar technologies. In this context, IoT support is focused on provisioning and access control.

40. We would also be very interested in bidding on the Services work (Phase 2), depending on which platform you decide to move forward with. If you can also let us know when that decision has been made that will allow us to craft a response for the bid, additionally knowing the selection for the ERP system would help with how we can address our responses. While we have done both Workday and PeopleSoft implementations it would just allow us to be more specific in the document.
    RESPONSE: We will announce a winner for Phase 1 before the Phase 2 deadline. If Phase 1 is delayed, we will adjust the deadlines for Phase 2 accordingly.

41. The file "RFP Appendix 1: Diagrams of Current Environments" is corrupted. Please share it again.
    RESPONSE: Thank you for telling us. We will address any file corruption issues.

42. If the answers to these questions are not readily available, please share approximate numbers or list assumptions to work with:
    a) What is the approximate number and type of sources of identity that need to be integrated?
    b) What is the number and type of target systems for identity provisioning to be integrated?
    c) What is the number of applications that will be integrated?
    d) What would be approximate number of different type of roles?
    e) What is the approximate number of approval workflows for roles and access provisioning that need to be setup?
    f) How many workflows for attestation of rights need to be setup?
    g) How many federation partnerships need to be set up?
    h) How many applications would need SSO?
    i) How many applications need to integrated for Multi Factor Authentication? What is the Multi-Factor Authentication method required?
    j) In case of On-premise solutions, how many Datacenters University has (for hybrid, HA, DR Planning, Deployment Topology).
    k) Any specific Non Functional Requirements (Performance Metrics).

    RESPONSE: For each part...
    A) Refer to question 21.
    B) Refer to question 9.
    C) Refer to question 9.
    D) Refer to question 25.
    E) Refer to question 27.
    F) Refer to question 27.
    G) Refer to question 7.

H) We believe this number to be large. Fayetteville today has over 100 service providers (relying parties) served by its Shibboleth SSO instance, with several others served by Azure AD. We expect other 4-year campuses to have similar scale, with 2-year campuses using fewer applications.
I) Multi-factor authentication should be implemented such that it can protect any application, including desktop login, remote shell access, and federated SSO. Refer to previous questions about the number of applications deployed. Ideally, MFA will be applied at and through the authentication interfaces (Kerberos, LDAP, SAML, RADIUS), and not through an application itself. Refer to questions 10, 25, 32, and 33 for further exposition.
J) For an on-premises implementation, we may elect to use datacenters on multiple campuses, making 5 or more geographically diverse datacenters available. If implemented at a single campus site, expect to use no more than 2 datacenters for on-premises implementation.
K) Respondents should describe any capacity limits within their solutions. For example, are there caps on the number of users, roles, groups, served applications, active federations, or any other item used? Respondents should describe the throughput limits within their solutions. For example, how quickly do changes to an entity's information converge and propagate out to "downstream" systems? How much time passes after the creation of new polices, rules, or workflows before they propagate and go into effect?

43. Please list your priority for IAM deployment - on premise vs cloud?
RESPONSE: We believe that a cloud (SAAS) solution or hosted implementation of an on-premises solution will be preferable to directly implementing the on-premises solution in our datacenters. Remember that innovative solutions are welcome. Do note that all responses to the RFP must propose a cloud (SAAS) or hosted solution, as we believe this maintains uniformity in proposal structure.

44. By when can we expect these clarifications to be made available to us?
RESPONSE: We plan to post responses by Wednesday, July 21.

45. Given the complexity and detail required for proposal responses, with current due dates in and around Independence Day, would the System please extend the due date for both phases by at least two weeks so that vendors may adequately account for answered questions into final solutions and subsequently provide compliant and qualified responses?
RESPONSE: We have decided to extend the deadline. We will communicate the new deadline through our normal channels. See Addendum 2.

46. Are both Phase 1 and Phase 2 proposals due on the same day or are they due a week a part? There was conflicting information between Mandatory Con-Call and the RFP. Would the System please clarify?
RESPONSE: Phase 1 and Phase 2 have different deadlines as outlined in the RFP, and the modified timeline in Addendum 2. The Phase 1 deadline applies to those proposing a phase 1 only proposal, or the software portion of a combined proposal.

47. Part of the ‘vision’ for the IAM is: “simplify the process of applying to colleges and universities” – it is unclear in the remainder of the document how the IAM solution will meet this part of the vision. Please elaborate on how this part of the vision is met based on the detailed requirements provided.
    RESPONSE: We envision a future where prospective students may apply to multiple campuses through a unified application process, as is available in other states. We view unified identity as an integral piece of the lifelong learning relationship that individuals will have with their campus(es).

48. How does the “System” vision this IAM solution helping with “Simplify the process of applying to colleges and universities”?
    RESPONSE: Refer to question 47.

49. How does the “System” vision this IAM solution helping with “Simplify the process of taking courses at multiple campuses”?
    RESPONSE: Refer to question 47.

50. What is the “Systems” decision of no on-premise solutions based on, are there specific items that have led to this decision?
    RESPONSE: There were many considerations regarding the System’s decision to specify either a cloud or hosted platform for delivering the solution. For proposal purposes, the System is not entertaining an on-premises solution.

51. The RFP indicates that the IdM becomes the source of authority for identity information. The source of authority is typically the origination of user information, such as an HRM or SIS and the IdM is the coordinator. By stating that the IdM is the source, it indicates that it will not receive any user information from another system (like the HRM or SIS) and that updates to information (such as a name change) must always originate from the IdM as the authoritative master of information. Please confirm that this is UARKs intention or provide clarifying wording to better indicate the relationship between the IdM and the source systems.
    RESPONSE: As we have discussed our accounts are created and used today, it has become clear that there are many exceptions to the expected flow illustrated by this question. Not everyone who needs a user account necessarily exists in the ERP, and not everyone in the ERP necessarily needs a user account. Our intent is to illustrate that these many edge cases must be addressed by the IDM platform, as we believe it is the only platform equipped to do so. Attributes that the ERP hold authority for may be delegated to the ERP, if the IDM supports that feature (e.g. tell the IDM that for users that exist within the ERP, delegate attributes such as address and date of birth to the ERP). Most importantly, we wish to avoid a scenario where the ERP is consulted as "authoritative" for some users, but the IDM or another system is consulted for other "non-ERP" users. We desire a single point of authority for all applications. Ideally, even the ERP would rely upon the IDM for authentication and access control, and identity information whenever possible, though this circular reference is a unique point, and is not a requirement.

52. Please indicate whether the future ERP is a source or a target of the IdM.
    RESPONSE: Refer to question 51.

53. The RFP only discusses provisioning and deprovisioning – if there are other scenarios (such as changes of name, status, role, etc.) please list them.
    RESPONSE: All of these scenarios are part of this RFP and are generally considered part of "Identity Lifecycle Management."

54. Please indicate the use cases for multi-factor authentication.
    RESPONSE: Refer to questions 11, 26, 33, 34, and 42(i) for further exposition.

55. The RFP indicates one of the requirements: "Identity and access governance processes are consistent and being used throughout the System". While a tool can help to automate portions of the processes, governance requires a measurable amount of periodic people-time from various organizations. As this is listed under the "Implementation Services" category, does this mean that UARK intends for the service provider to ensure that personnel from the various campuses are performing their governance duties?
    RESPONSE: No. The intent is that the service provider will assist our staff in defining and establishing the processes necessary for good governance, and will provide training for the core staff in executing and maintaining those processes over time.

56. The RFP indicates one of the requirements: "Audit and compliance reviews are automated, and produce relevant documentation." Does UARK intend 'reviews' here or 'reports'? As reviews require user participation, that necessitates at least one manual step, preventing complete automation.
    RESPONSE: This is correct. The correct wording is "reports." We wish for automated reports as part of the audit and compliance process. We do expect that the service provider will assist our staff in building review processes that provide input to those automated reports.

57. The RFP indicates one of the requirements: "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." The wording for this item seems to indicate that the IdM would control building access. Please confirm that the intent here is that the IdM would integrate with a building access management system and potentially assign rights based on defined roles. Please further confirm that the intention of controlling computer access is for ID cards to be used as a multi-factor authentication mechanism.
    RESPONSE: Yes. The expectation is that IDM will integrate with building access management systems. The vision for computer access through ID cards is multi-factor authentication, such as a smart card reader, USB or RFID token.

58. The RFP indicates one of the requirements: "Each person has the ability to manage their relationships with the System and their local campus or unit through self-service account/attribute management". Please elaborate on what sort of attribute and relationship management UARK envisions users wanting/needing to perform.

RESPONSE: We desire to reduce friction for end users, and repetitive actions by staff in updating user records. We desire an individual to be able to update his or her address, phone number, email addresses, and other personal information. Since the IDM platform will manage users known to the ERP as well as users external to the ERP, we believe it to be best suited to support this functionality. Of course, we remain open to alternative solutions.

59. For the federated single sign-on requirement, please confirm that appropriate interfaces are already available for the listed services or that UARK will take on the responsibility for providing appropriate interfaces for SSO/federation technology to integrate.
RESPONSE: We believe the appropriate SAML interfaces already exist for all listed services. We do not expect a vendor to build a SAML interface for a third party that lacks one.

60. Please elaborate on what UARK considers 'preserving the unique "identity" or spirit of each campus or unit'.
RESPONSE: While there is one "University of Arkansas" system, our students do not think of themselves in that way. Students at each campus take pride in their school identity and in their "belonging" to that school. A UALR "Trojan" would be insulted to be mistaken for a Razorback. While we desire to unify identity to improve inter-campus collaboration and transfer of students as they pursue their studies, we in no way want to make a student's experience generic, or to sever the bond they have with their campus.

61. The RFP indicates that the IdM should be online and integrated with all campuses in advance of the ERP. Is UARK aware that integration of the ERP as a feed into an IdM (as opposed to a consumer of the IdM) after campuses have been tied in means reworking/replacing all of the connectors built to gather information from the source systems at the campuses and a major data reconciliation effort to synchronize existing directory data with the ERP?
RESPONSE: At Fayetteville, the current user account generation process is tightly coupled to the exiting ERP systems (mainframe and PeopleSoft). We believe that it is necessary for IDM to replace this process prior to the transition to the new ERP, to minimize service disruption. Other campuses will have similar needs as they prepare to transition to the new ERP. The goal of our request is to address that risk. If respondents feel they have a better solution to this problem, they are encouraged to propose it.

62. The RFP Indicates that the institutions in scope for Stage 1 are Fayetteville, Little Rock, eVersity, Division of Agriculture and the CC at Morrilton. However, the systems provided in Appendix 1 are Fayetteville, Medical Sciences, Monticello, the CC at Morrilton, and the School for Math, Science and the Arts. Also, Appendix 5 aligns with Appendix 1. Please confirm which institutions are included in Stage 1. If the included institutions do not align with the five listed in Appendix 1 and Appendix 5, please provide the information for those institutions that was not included in Appendix 1 and Appendix 5.

RESPONSE: The institutions provided in Appendix 1 are intended to be illustrative of their peers within the system. The list of campuses for stage 1 is correct as listed in the RFP.

63. The RFP only discusses provisioning and deprovisioning – if there are other scenarios (such as changes of name, status, role, etc.) please list them.
RESPONSE: Refer to question 53.

64. Please elaborate on what is intended by "role discovery and mapping" under the Role Based Access Control section. We have found this to mean different things to different organizations, and the specific interpretation could mean significant differences in scope.
RESPONSE: The campuses today lack consistent definition of roles. We expect the service provider to assist each campus in uncovering the known and unknown roles that define the various types of access needed by individuals at that campus, and to normalize those roles where possible to enable more globally illustrative roles across the system. We also expect that this process will discover the access and entitlements that make one role different from another, and that the service provider will define these roles and entitlements within the IDM as part of implementation. Refer to question 24 for further exposition.

65. Please elaborate on the specific use cases for multi-factor authentication.
RESPONSE: Refer to question 54.

66. For account isolation and credential revocation, is the ask here for the IdM to detect violations/risk and then take actions, or simply to provide workflows to take action after compromise is detected by an appropriate system/organization?
RESPONSE: We are asking for the workflows and automation to take action. If the IDM can detect violations or do risk scoring as well, that is welcome; those features should also feed into any alerting, logging, and reporting, feature set.

67. Does the System require all resources to be on-site full time? Is remote work acceptable when appropriate and available?
RESPONSE: Remote work is acceptable when direct interaction with our teams is not necessary. The respondent should indicate which activities will occur on-site and which activities will occur remotely.

68. Should the fixed fee bid include travel expenses, or does the system want to reimburse expenses as incurred?
RESPONSE: The bid should include travel expenses. UASys does not intend to directly manage, approve, or reimburse travel expenses.

69. The text indicates that 'once approved', accounts are provisioned into Active Directory. Is that a manual process of creating AD accounts? Is POISE capable of producing text file output, or can its database be queried from an external system?
RESPONSE: POISE is capable of producing text output. The current account creation process uses scripts to create the AD accounts. (response via UACCM)

70. App. 1, ASMSA: No Active Directory is currently present, is the intent to implement Active Directory at this location?

    If the answer is yes: Will all current applications utilize Active Directory going forward?

    If the answer is no: Please describe how you envision an IdM working here. If the current source of authority is also the directory, how does UARK envision an IdM providing value in this space?

    RESPONSE: ASMSA is willing to implement an Active Directory, if that is the best design. If the best design is for the IDM to integrate with the existing Google Apps for Education (GAE) infrastructure, then IDM would take integrate with GAE and use it as the directory for that campus.

71. App 4 – Identity Lifecycle Management, #21 - Please elaborate on the use case for self-selection.

    RESPONSE: We are aware that some campuses outside of our System allow users to select their own username (account name) during user enrollment. Those schools find that this flexibility reduces user complaints about odd or difficult to remember account names, and reduces complaints if the policy is that the account name cannot change. The System campuses have not yet agreed on a username strategy, but we would like the flexibility to use this option should we decide it is best for us. A common method is to present the user with a workflow that allows them to try out several account names, searching for one that is not in use, and optionally suggesting available names.

72. App 4 – Identity Lifecycle Management, #23 - Please elaborate on the use case for self-enrollment.

    RESPONSE: Some campuses outside our system allow an individual to establish a user account within IDM at some point during the academic application or employment application process. They elect to allow the user to self-enroll, providing many identity attributes either through this self-enrollment process, or from the relevant application. This process is instead of having an automated process do all the account creation automatically. The System campuses have not yet agreed on an account establishment strategy, but we would like the flexibility to use this option should we decide it is best for us.

73. App 4 – Identity Lifecycle Management, #24 - Please define 'locally-created' identities – is this local to the identity management solution, local to workstation, something else?

    RESPONSE: Locally created identities refer to individuals who need accounts, but do not exist in the ERP. A mechanism is needed to create accounts for them while preventing them from colliding with ERP users. Refer to question 50 for further exposition.

74. App 4 – Authentication, #34 - Please clarify the use cases for multi-factor authentication. Workstation login, app login, VPN login, something else?

    RESPONSE: All of the above. Refer to questions 11, 26, 33, 34, and 42(i) for further exposition.

75. App 4 – Authentication, #45 - The solution enables federation between University of Arkansas System campuses and outside of the System. - what degree of federation functionality is required?
    RESPONSE: We desire:
    A) UASys users will be able to authenticate to internal and external services known to the federation.
    B) External users that are members of other federation entities will be able to authenticate to services at UASys campuses, if those are exposed to the federation.
    C) UASys (or individual campuses) may need to maintain a local SAML metadata aggregate, or other means of enabling SSO for internal applications. The intent is that SAML SSO be used for all web applications, whether or not exposed to an external federation, so that web SSO approaches true single sign-on.
    D) In both cases, the asserted identity information may include additional attributes to aid in establishing the user's entitlements, roles, or other useful information.
    E) In both cases, asserted identity information may identify the user using methods that vary in their characteristics (persistent, revocable, opaque, targeted, etc.) Refer to the following URL for illustration of the various characteristics:
    https://wiki.shibboleth.net/confluence/display/CONCEPT/NameIdentifiers

76. App 4 – Authentication, #46 - The solution has provisions for "shared" accounts. - please explain how the accounts are shared? Does this refer to "superuser" accounts?
    RESPONSE: There are a couple of current use cases. We need a mechanism to account for "service" accounts, where the password may be known to several individuals, but the use case is for one application to authenticate to another, in absence of other tools like certificates. Another common use is for access to shared resources. For example, at Fayetteville, student clubs and similar organizations are assigned an account for the organization that is shared among the officers of the club and provides access to shared mailbox, web space and similar resources. We believe there are better methods to provide this functionality.

77. App 4 – Authentication, #46 - Please clarify the use case for ‘shared’ accounts.
    RESPONSE: Refer to question 76.

78. App 4 – Roles, #59 - Please provide your definition of a ‘dynamically defined role’.
    RESPONSE: A role is dynamic if it is assigned and removed based on identity attributes or business rules, rather than being linked other grouping hierarchies like simple group membership.

79. App 4 – User Interface and Experience, #81 - Please provide detail on your definition of a ‘complete experience’ with respect to IoT devices as well detail as your desired integration for IoT devices.
    RESPONSE: Refer to question 39 for further exposition.

80. App 4 – User Interface and Experience, #87 - Please elaborate on your meaning here.
    RESPONSE: There are several portal- launcher-like models common in higher education. They tend to trend toward one of three forms:

1. An application that presents a grid of application can use via SSO.
2. A top ribbon (like Google Apps that provides an SSO grid and other menu functionality on top of other applications)
3. A traditional intranet portal with widgets (portlets) that present information to the user from various applications.

In all cases, SSO should support the portal operation. In the portlet model, SSO should support pass-through authentication, allowing the portal to pass the SSO assertion through to the application it is exposing to the end user.

81. App 4 – Risk, Assurance and Compliance, #98 - Please provide detail on which of the parts of NIST SP 800-63 you are referring to, or if it is all parts. Also, please confirm that you are aware that this is a draft specification of guidelines likely to change before ratification.
    RESPONSE: This requirement refers to the ability to certify to a given level of assurance (LoA) that the individual using a given account is the known owner of that account and that it is his or her sole control. The requirements of InCommon SILVER mirror SP 800-63 in this regard, and SILVER is likely to be the LoA assertion model in use.

82. App 4 – Risk, Assurance and Compliance, #99 - Please clarify your meaning here. Since a security framework provides no specific implementation, it is unclear how you would 'integrate' with it.
    RESPONSE: The NIST framework defines activities and outcomes that the IDM will directly support, such as access control requirements. Still other activities and outcomes must be addressed, such as backups, audit/log records, anomaly detection, and monitoring. During implementation, we expect to document the solution's approach to addressing these functions.

83. Section 15.6 Questions 33-36. Can you please explain what is meant by "privacy status" for a user? What are your expectations in regards to a privacy status?
    RESPONSE: This refers to our requirements under FERPA to protect student information, and to allow them to opt out of public use of their information should the elect to do so.

84. Does this absolutely have to be cloud based or is there any option for on premise solution?
    RESPONSE: Refer to question 50.

85. Can you provide me with the total number of total full-time employees? The Employees total currently encompasses both full-time and part-time employees. This is relevant to us due to our licensing model.
    RESPONSE: We are providing an additional appendix that provides 2015 IPEDS data for full-time vs part-time employees. Note that these numbers do not match those conveyed in Appendix 2 because the IPEDS data is older. We suggest that you infer employee population counts by comparing the two tables. Current populations will be provided during the negotiation phase for vendors that reach it.

86. [Firm] would like to make a formal request to push back the phase 1 due date June 30th.
RESPONSE: Refer to question 45. We have decided to extend the deadline. We will communicate the new deadline through our normal channels.

87. The RFP request document states, 'Provide Privileged Account Management where needed.' Can you provide more context regarding this requirement? I.E. How many systems need to be protected or how many accounts need to be protected by a PAM solution?
RESPONSE: Refer to questions 35 and 76 for further exposition.

88. The RFP request document states, 'Provide Privileged Account Management where needed.' Are you looking for any specific requirements for PAM functionality? I.E. Session Recording is a must, etc.
RESPONSE: Refer to questions 35 and 76 for further exposition.

89. Are there any other applications beyond those listed in the Software Environment PDF that will need to be integrated with the new IAM system?
RESPONSE: We are unable to collect a comprehensive list of applications to be integrated. There are many applications that will need integration. The list changes frequently. We desire to provide most authentication through standard methods (Kerberos, SAML, RADIUS, LDAP), and to provision accounts in these applications either in a just-in-time manner, through a SCIM/SPML like standard, or through ETL (flat file) at last resort.

90. This is to confirm [firm]'s intent in responding to the RFP, in the following manner:
Phase I & II – [firm] plans to bid for Phase I and Phase II together, where we will partner with an IAM vendor.
Phase II - It's possible that University's decide to procure/purchase a IAM platform which isn't part of our first proposal. In this scenario, we request University of Arkansas to give us an opportunity to respond to Phase II as a Service vendor. We are global Technology corporation and have mature project delivery capabilities (configuration, system integration and support services) across IAM platforms.
Please do let me know if University is fine with this approach.
RESPONSE: Refer to question 13. Vendors may respond to Phase 1 and Phase 2. Vendors may respond to phase 2 even if not selected in their Phase 1 proposal.

91. Can we receive a list of company attendees?
RESPONSE: We will be posting that information to the Hogbid website. The list of participants and the Q&A from that session will be posted.