Q+A – RFP #757537

1. **Page 8 - SCOPE OF WORK** - The Scope of work states that MSU is soliciting proposals for vendors/implementer services to assist in the selection and implementation, are you seeking responses from organizations that can sell you their specific technology + implement it? Or are you seeking a vendor to make a product recommendation based on their industry knowledge and then help with implementation following the purchase of the tool(s)?

   Answer: MSU is seeking responses from organizations that can sell us technical solutions and implementation services for those solutions. We are NOT looking for services associated with the selection or recommendation of products or tools.

2. **For the Scope of Work - Can some or all this work be performed remotely? If yes, what percentage? If not, what is the place of performance?**

   Answer: This engagement does not require any on-site presence, if it does not interfere with timelines, goals, or quality of the solution. However, MSU is open to working in person should the need arise, or be beneficial to the engagement.

3. **For the Scope of Work - What are your current systems of record for students, faculty, and staff?**

   Answer: Current systems of record are as follows:

   a. **Student Information Sources**
      i. Slate – CRM for student recruitment.
      ii. Peoplesoft Campus Solutions – SIS system and source of authority for student records.
      iv. EDW Enterprise Data Warehouse – Data warehouse for institutional data and staging area for identity data.
      v. Salesforce Ascend – Alumni/Advancement CRM and data source.

   b. **Employee Information Sources**
      i. PageUp – Employee recruiting CRM platform.
      ii. SAP – HRMS system and source of authority for employee records.
      iii. EDW Enterprise Data Warehouse – Data warehouse for institutional data and staging area for identity data.

   c. This may also require temporary integrations with legacy systems, depending on deployment order and timing.

4. **For the Scope of Work - What do you use for your Student Information System? If you are using Banner, what other Banner modules do you use?**
Answer: MSU currently uses Campus Solutions On-Prem (CS) using PeopleTools as well as Update Manager. We also using Student Financial Planner (Cloud Version).

5. **For the Scope of Work - Will this solution directly or indirectly service auxiliary systems, e.g., Parking Office, Photo ID, Student Health Services, Intramural Sports Office, and so on?**
   
   Answer: This solution will manage identities, accounts, identifiers, access, and any associated peripheral services or entities, so it is important the product be capable of supporting these functions. However, the initial implementation should be scoped to replace existing core IAM services. MSU envisions using a Enterprise Messaging System to assist in facilitating the updates for most auxiliary systems. Future engagements may be needed/necessary to integrate with other non-MSU entities.

6. **For the Scope of Work - Will this solution service outside vendors or service providers such as financial institutions, state reporting services, research consortiums, or other non-MSU entities?**
   
   Answer: This solution will manage identities, accounts, identifiers, access, and any associated peripheral services or entities, so it is important the product be capable of supporting these functions. However, the initial implementation should be scoped to replace existing core IAM services. Future engagements may be needed/necessary to integrate with other non-MSU entities.

7. **For the Scope of Work - Will this solution be used by your alumni office or foundation?**
   
   Answer: Yes. Please include integration with university advancement in your scope of work. See Question 3 for details.

8. **For the Scope of Work - What is the level of executive sponsorship and oversight for this project?**
   
   Answer: This project is a small part of a 3-year IAM Roadmap and Program supported at the highest levels of executive sponsorship.

9. **For the Scope of Work - Is Michigan State open to discussing a cloud hosted SaaS solution that includes SailPoint, Radiant Logic for data aggregation, the Ping Suite of products, and CyberArk as a PAM solution?**
   
   Answer: MSU is open to any technical solution that meets the requirements as defined in the RFP.

10. **In Section 2.27.1, MSU highlights that the "Platforms can integrate with and manage access in ID badge and physical access platforms out of the box". What’s the downstream system that the platform must connect into to manage ID Badge and Physical Access Platforms? Do these utilities support open protocols such as SCIM or possess APIs which the proposed solution would be able to use to facilitate identity management into the Physical Access services?**
    
    Answer: Today’s ID Card System is UltraBadge and Transact is used for meal planning and payment processing. For integration options, Transact has API’s, but UltraBadge can only use SQL. We are working on migrating from Mercury to Genetec for physical access.

11. **In Section 2.27.2, MSU calls out that the "Platform can support and scale to all required data formats (e.g., to support ID images, barcodes, etc.)". What are all of the different data formats that the platform must support regarding Physical Access Management?**
    
    Answer: This requirement was meant to express a need for the ability to include JPEG image files as part of the identity record in the core identity system.
12. In Section 2.45.1, MSU writes that the “Platform is able to verify each identity as a single person utilizing and identifier that never changes”. What kind of ID Proofing services is MSU expecting the proposed solution to provide from an Identity Management perspective? Would MSU want Identity Proofing to take into effect when identity records are created, updated in the service, or when external, guest, or affiliate users sign-up or register an account with MSU?
Answer: This requirement is meant to express the need for the solution to provide functionality to assert a single identity for each physical person, regardless of their affiliation with the university. We will not presuppose any specific solution for how the ID Proofing Service should be accomplished, just that the product is capable of doing so. The specifics around when the identity proofing should occur will depend upon product capabilities and options that will be flushed out during the requirements gathering and design phase of the implementation services.

13. In Section 2.45.2 MSU notes that the “Platform can differentiate between low, medium, and high levels of assurance for an identity, based on criteria or verification processes”. Does MSU possess specific criteria indicating low, medium, or high levels of assurance for an identity, or would the proposed platform need to have those assurance levels baked into the platform?
Answer: Michigan State University levels of assurance standards are currently based on the REFEDS Assurance Framework (RAF). The product needs to be capable of supporting levels of assurance as defined by RAF1.0.

14. General Question: Are respondents allowed to partner with other solutions to provide a joint response to this RFP?
Answer: Yes.

15. Do you have a preference of a SaaS IGA solution or on-premises?
Answer: See question 9.

16. Are you considering or open to using IdentityIQ as your IGA solution?
Answer: See question 9.

17. It says MSU will provide a PM for ¼ FTE for each initiative, do you expect your implementation partner to also provide a PM?
Answer: Yes.

18. How flexible is your milestone/schedule?
Answer: MSU is willing to entertain an alternate schedule provided the appropriate reasoning and justification.

19. How did you determine the proposed schedule of milestones?
Answer: The milestones align with the timing in our IAM roadmap.

20. Are you looking for a time & materials contract or fixed price?
Answer: MSU is willing to consider both fixed prices as well as time & materials estimates, provided that they are scoped appropriate to the effort requested in the Implementation Services Statement of Work section 5, and some limitation on overages is provided.

21. Do you currently have source control for your current IAM products (vendor and homegrown)?
Answer: Yes, we are using Bitbucket for our SCM.

22. How do you currently use IdentityIQ today and how many users do you have?
Answer: Our current IdentityIQ implementation serves as an identity data broker for our ERP systems, Active Directory, Okta, and our data warehouse. There are hourly, daily, and weekly batch jobs that keep all of these systems in sync. There are currently 772,494 identities in our IdentityIQ production environment.

23. How do you currently manage users in multiple sources today from a matching perspective and creating one identity?
Answer: Current matching is done primarily with social security number. We do not have any fuzzy logic matching implemented.

24. Do you currently use a source control management software? If so what are you using?
Answer: See question 21.

25. Do you currently have a CICD pipeline platform in place across the organization? If so what is it?
Answer: Yes, we are using Bamboo for our CI/CD pipeline.

26. Are you using any cloud services and if so which cloud vendor do you prefer (GCP, AWS, Azure)?
Answer: We are not currently using any cloud services for our IAM platforms. We are a Microsoft shop, but would hear why cloud offerings outside Azure are the right solution.

27. How many workflows do you have for access requests in TeamDynamix?
Answer: We currently use three workflows. One for all access requests using iPaaS forms, one for creating and managing service accounts(application users) and one for merging and changing MSU NetID accounts.

28. How complex are your approval processes today?
Answer: Currently, all access approvals require at least one level of approval by the department designated approvers. These individuals verify that the end users work for the department and need the requested access for valid business reasons.

Some, but not all systems also need approval by the system owners. They verify that the access being requested is correct and valid for the business needs stated by the requestor/department.

IAM also inserts ourselves into the approval process for our generic request forms as these are open text documents. We verify the request makes sense, is valid and has the right amount of information to process, then route the approval tasks to the appropriate systems approvers if necessary.

29. How well documented or knowledgeable are your staff of your current IAM solution(s)?
Answer: Some of our current homegrown IAM components were designed and implemented by people that are no longer employed at MSU and documentation is spotty at best. Our more modern components are fully documented, and our team is fully versed in their knowledge.

30. Can you submit multiple responses for different vendors?
Answer: Yes.
31. **Are you anticipating building a custom registry for that abstraction layer between ERP and IAM or is this something you expect the product to support? Would you consider using IdentityIQ for a Registry/Hub where it can do complex matching and workflows for ID resolution?**
   Answer: We expect the product or the implementation services to include the development, build, configuration, and/or implementation of the Identity Registry/Hub. We have no preference for the specific solution that accomplishes this.

32. **How many Active Directories do you manage?**
   Answer: We manage a 3-tier Active Directory environment.

33. **How complex is your AD OU structure?**
   Answer: We currently have two user OUs in Active Directory. One OU is for Guest accounts, and one for all other account types.

34. **How many birthright roles do you have today?**
   Answer: Today, we use 5 birthright roles: Students, Faculty, Staff, Affiliate, and Guest. It is expected to be much more granular than this in future state.

35. **Does MSU plan on providing developers for the build phase?**
   Answer: MSU will have developers available to support systems integration and development.

36. **Does MSU have developers versed in Java and/or beanshell?**
   Answer: MSU has developers versed in Java, and developers versed in Beanshell. We do not have any developers with in-depth experience in both.

37. **What language(s) are your homegrown solutions written in?**
   Answer: Our homegrown solutions are written in Bash, Python, Perl, C, Java, and ASP.NET, with the majority being written in Java.

38. **Are you currently using Entra/AD Connect to provision O365, mailboxes, licenses?**
   Answer: We are currently using AD Connect and custom PowerShell scripts to provision Office 365 mailboxes and licensing.

39. **Is Password Management in scope or do you currently have a solution for that?**
   Answer: Yes, password management is in scope for this RFP. Please see sections 2.9.1 and 5.5.3.6 for requirements.
40. **Can you elaborate on your requirements around delegated administration? What types of use-cases do you need to support?**
Answer: It is hard to tell which requirement this is in reference to, so we will assume you meant requirement 2.25. The use case for 2.25 is to allow business units and/or colleges to manage access rights and/or groups themselves by allowing them to grant access or add/remove people from groups utilizing criteria or include/exclude capabilities.

41. **Do you anticipate travel for the implementation partner to be needed?**
Answer: See the answer to Question 2.

42. **Can you clarify the following: Invoice payment terms for the agreement resulting from this RFP shall be 2.75% 10, NET 30 from date of receipt of invoice?**
Answer: If invoice is paid within 10 days, MSU shall be entitled to a 2.75% prompt payment discount on the invoice otherwise net amount of the invoice will be payable.

43. **Can you clarify: The University prefers a single consultant approach but will consider an alternative approach of using a team of consultants. If you propose a team of consultants approach, please provide an explanation on why it would be in the University’s best interest to take this approach?**
Answer: The single consultant approach refers to our preference to have dedicated resources as part of the implementation services throughout the life of the engagement, as opposed to consultants working on many other projects/clients that change throughout. If you prefer to bid on this with a consultant team approach, please explain the benefit of this approach and MSU will review the submissions to determine if it is in our best interest to take this approach.

44. **Can you provide a total number of in-scope target applications i.e. 5.3.16 SQL, MySQL, and Oracle Databases. How many databases and is this managing user accounts or data provisioning?**
Answer: We have 3 Oracle databases with 1-5 schemas each, 3 SQL servers with 1-3 databases each, 1 MySQL database with 2 schemas, and 1 Firebird database. These are replicated across four deployment tiers: DEV, TEST, QUAL, and PROD. These are used both for managing user accounts and for data provisioning.

45. **What type of historical data do you plan on importing?**
Answer: We are planning on importing identity data (name, address, phone number, national identifiers, etc.) and MSU identifiers to ensure that we don't duplicate any identities.

46. **What current apps/services do you plan to deprecate as part of this project?**
Answer: We are planning to deprecate our homegrown legacy stack, which includes: MySQL database, Firebird database, batch scripts, and a handful of custom web portals used for administration and identity lookups.

47. **Do you plan on maintaining and keeping IdentityIQ as product for IAM?**
Answer: We do not have answer at this time as this is dependent on this RFP.

48. **How many staff/contractors support your current IAM functions today?**
Answer: We have 12 FTEs and 2 contractors supporting our identity functions, and 8 FTEs and 2 contractors supporting our access functions.
49. **Do you have a current governance process in place for your IAM program?**
   Answer: We are in the process of developing an IAM governance process.

50. **Who are the decision makers for awarding the RFP?**
   Answer: A cross functional team at MSU including IT and campus partners.

51. **Regarding 5.6.4. “Configure certification and Separation of Duties (SoD) policies.” I assume some HIPAA, FERPA... What other audit standards need to be addressed at this step? Are portions of the University audited regarding compliance with ITAR restrictions, NIST 800-53/ISO standards? How many key systems, which are they, and how many annual audits does the University undergo?**
   Answer: 5.6.4 is intended for access certification, i.e. prompting service owners that individuals and groups still require access to their service. This process should not require IAM staff to support, and separates the certification duty from IAM onto the service owners. Separate from section 5.6.4, our program framework is built around NIST CSF and we do have regulatory control audits/assessments/compliance requirements for HIPAA, PCI DSS, NERC-CIP, FERPA, GLBA, CMMC/CUI/NIST 800-171, ITAR, CJIS, and some others.

52. **Similarly in 5.5.3.5.6. Configure Separation of Duties Policies for access requests”. Can you please elaborate on specific SoD requirements? What key systems / applications does it apply to? What are the audit/reporting requirements?**
   Answer: See question 51.

53. **Why are there still manual processes if the University has a current IGA tool? Are there specific use cases that the current solution cannot address? Does it require too much coding for a small identity team to keep processes current? Has it failed to integrate with some University systems?**
   Answer: The existing IGA did not receive the necessary support to be fully implemented.

54. **In 2.6.1. Platform provides a data store or directory to host identities, that provides distinction between principals and accounts. Can you please define principals and accounts in this context to avoid ambiguity?**
   Answer: In this context, the principal refers to a person’s identity record, which is a distinct concept from an account. A principal, or identity, refers to the electronic record that contains all of the information associated with an identity. An account is a credential that identifies a person to a service. There can be multiple accounts associated with a principal/identity, but there can only be one principal/identity per physical person.

55. **Page 8 - Does the University have a rough estimate on the number of anticipated roles/affiliations intended to be managed within the program?**
   Answer: There are currently about 150 roles/affiliations that will be managed within the program.

56. **RFP Page 8 - Does the University have a rough estimate on the number of anticipated roles/affiliations intended to be managed within the program?**
   Answer: See question 55.
57. **RFP Page 8 - Is IdentityIQ currently used and to what extent? Older version, need upgrading?**
   Answer: Yes, we are currently using IdentityIQ 8.2p4. This will need to be upgraded prior to July 2024 to remain in the SailPoint support window. See question 22 for how we are using IdentityIQ.

58. **RFP Page 8 - Why is it that some identity tools have been deployed but not fully leveraged? Is user experience not intuitive, poor feature set, lack of integration capabilities, no vendor support, hard to implement / maintain, or not scalable?**
   Answer: See question 53.

59. **RFP Page 8 - What are the greatest barriers to greater maturity in your identity security program?**
   Answer: Multiple authoritative sources, complex business requirements, complex identity journeys where an individual can be a student, faculty, and staff member at a single time. Identity governance and integration are complex requirements.

60. **RFP Page 29 - Is VPAT_534364_7 the correct version of the VPAT document that needs to be submitted?**
   Answer: You can download the form here: https://www.itic.org/policy/accessibility/vpat/ . The following version can be used: VPAT 2.4Rev WCAG

61. **What is your current IAM solution, and can you share your key pain points/challenges with your existing solution?**
   Answer: We are currently using SailPoint IdentityIQ and a homegrown legacy stack for our IAM solution. Key pain points and challenges are available upon request. See question 62 for how to submit a documentation request.

62. **Are you able to share any documentation on your current state (e.g., design/integration diagrams)?**
   Answer: These documents are available upon request. Please send an email to rmaas@msu.edu to request these documents.

63. **Is the expectation that your current IAM solution will be decommissioned, or will there be a period when there is co-existence?**
   Answer: Both of these statements are true. We will have a period of co-existence during implementation, but the goal will be to decommission our current IAM solution at the end of the engagement.

64. **With regards to the number of users provided in Section 1.0 – Background: Over 12,000 permanent and part-time faculty, and staff; 49,695 students; 16,000 annual student employments; and 3,000 annual graduate teaching and research assistant appointments.**
   Are these numbers unique identities or is there overlap in your different roles (i.e., student employments are included in the active student numbers)? We are interested
in identifying the number of unique identities and the number of contractors being held in Non-Employee Risk Management.

Answer: There is overlap in between the roles, particularly for active students and student employees. Please see question 65 for unique counts.

65. With regards to the number of guest accounts, identities, and usernames provided in Section 1.0 – Background:

- Over 100,000 guest accounts, 750,000 identities, and over 1.5 million usernames taken from our namespace.

Of the numbers provided, how many will you be including in your new governance solution? Are you provisioning to any of these accounts or are they being held in your access management solution? Of those numbers, can you define the number of unique, alumni, inactive, guest, or other types?

Answer: Alumni – ~280,000; Inactive – ~800,000; Guest – ~105,000; Active Student – ~70,000; Active Employees – ~30,000, Active Student Employees – ~12,000

66. Page 25 / 5.2 – In Scope Sources of Authority - Provide additional information regarding the types of identities for which each SOA contains data and if multiple SOAs can contain information on the same identity.

Answer: See questions 3 and 64.

67. Page 25 / 5.3 & 5.4 – In Scope Target Systems and In Scope Sources/Targets for Legacy Historic Import - Provide additional details related to the priority and criticality of applications that will be integrated into the solution.

Answer: We are looking to work with the awarded vendor to help determine our priority and criticality of integrations. The Legacy/Historic systems will be among the first, but the exact order is to be determined. The prioritization of this effort falls under section 5.5.1.

68. Page 26 / 5.5 – Identity Data Management and Identity Governance & Administration Implementation Services - Are there any identified project prerequisites or dependences for this the SailPoint Identity Security Implementation effort is reliant on?

Answer: We do not have a SailPoint Identity Security Implementation effort.

69. Page 26 / 5.5.1 – Dependency Discovery - Deconstruct the entanglement of IAM dependencies and develop a surgical replacement plan for homegrown IAM services - Provide additional details / priority around the existing process/homegrown applications that are in scope to be retried/replaced as part of this implementation.

Answer: See questions 3 and 67.

70. Page 27 / 5.7 – Third-Party / Non-Employee Management Implementation Services - Provide the desired timeframe for implementation of Non-Employee Management. Does this need to be complete prior to, as part of, or after the implementation of SailPoint Identity Security Cloud?

Answer: We do not have any current plans to implement the SailPoint Identity Security Cloud.
71. **Page 28 / 5.7.1.3** – Capable of moving between a third-party/non-employee and a source-driven identity if applicable - Provide an example use case for an identity that may move between a third-party and a source-driven identity.

Answer: An example use case for this would be a high school student creating a guest account to use with our LMS and then becoming an admitted student with a source-driven identity in our SIS.

72. **Pages 24-25 / 5.1.7** – Unit testing and User Acceptance Testing - Please clarify the expectations on User Acceptance Testing. For example, under the Proposed Solution section of the RFP, there is this statement: Michigan State University workgroup members will validate solution(s) build, confirming the solution(s) meet the institution’s business requirements and needs.

Answer: Unit testing will be performed by the vendor and UAT use cases will be supplied by the vendor. UAT will be performed by MSU with the support of the vendor.

73. **Under section 5.1, one of the implementation services engagements that the vendor is expected to consult on and deliver is: 5.1.7 Unit testing and User Acceptance Testing. Who is ultimately responsible for User Acceptance Testing, the Michigan State University workgroup members, or the vendor?**

Answer: See question 72.

74. **Page 25 / 5.2,5.3,5.4** – In Scope Sources of Authority, In Scope Target Systems, and In Scope Sources/Targets for Legacy/Historic Import - Are the sources & targets detailed in the RFP the only sources & targets for the vendor to consider for implementation services planning, or are there potentially additional sources & targets that could be added to scope prior to the project kickoff and planning phase in Q2 of 2024?

Answer: The in scope systems are the only systems that need to be considered for implementation as part of this RFP. Additional systems may be taken on operationally during the implementation phase of this engagement, but will not fall under the purview of the awarded contract.

75. **Background - Page 8** · Over 12,000 permanent and part-time faculty, and staff; 49,695 students; 16,000 annual student employments; and 3,000 annual graduate teaching and research assistant appointments. Are the numbers provided unique identities or is there overlap in your different roles (i.e., student employments are included in the active student numbers)? We are interested in identifying the number of unique identities and the number of contractors being held in Non-Employee Risk Management.

Answer: See question 65.

76. **Background - Page 8** · Over 100,000 guest accounts, 750,000 identities, and over 1.5 million usernames taken from our namespace. Of the numbers provided, how many will you be including in your new governance solution? Are you provisioning to any of these accounts or are they being held in your access management solution? Of those numbers, can you define the number of unique, alumni, inactive, guest, or other types?
77. **Scope of Work – Background - Page 8 of 31: What is the quantity of seats required for this new, holistic IAM platform solution?**
   Answer: We will need more information on what the term “seat” refers to. We are currently anticipating storing roughly 1 million identities and ensuring that the 1.5 million names in our namespace are not reused. Many of those accounts will be in an inactive state, awaiting the potential event that the individual needs to reactivate their MSU account(s).

78. **Page 3 - There is a table of the evaluation criteria. Are the requirements weighted equally or does one area hold a higher weight/priority?**
   Answer: The weight and priority are determined solely by MSU however, MSU is not sharing the weighting at this time.

79. **Page 8 - Of the numbers provided, how many will you be including in your new governance solution? Are you provisioning to any of these accounts or are they being held in your access management solution? Of those numbers, can you define the number of unique, alumni, inactive, guest, or other types?**
   Answer: See questions 65 and 77.

80. **Page 8 - Are the numbers provided unique identities or is there overlap in your different roles (i.e., student employees are included in the active student numbers)? We are interested in identifying the number of unique identities and the number of contractors being held in Non-Employee Risk Management.**
   Answer: See question 65.

81. **Page 8 - Of the 750,000 historical identities, how many of these identities still have accounts in the environment? How many of these identities are being maintained to preserve usernames/email addresses?**
   Answer: See question 65.

82. **Page 9 - In section 2.1.3, it mentions the need to support near real-time synchronization. Which of the in-scope target systems or authoritative sources is this required for? Do you currently have this capability?**
   Answer: This is required for all in-scope target systems and authoritative systems. We do not currently have this capability, but are working on deploying an Enterprise Messaging Service to assist with this.

83. **Page 9 - Please provide use cases where near real-time synchronization is important.**
   Answer: Real-time synchronization is important for Name/Gender/Pronoun updates and student and/or employee attrition.
84. **Page 10 - What data elements are available in the sources of authority for data matching?**
   Answer: The following data elements are available in the sources of authority for data matching: name(s), address(es), phone number(s), national identification number(s).

85. **Page 11 - In item 2.9.2, please describe use cases for account management/administration delegation.**
   Answer: See question 40.

86. **Page 11 - In item 2.12.2, does MSU have a SIEM tool of choice?**
   Answer: MSU currently uses Humio.

87. **Page 12 - In item 2.12.3, please provide example use case(s).**
   Answer: Referring to: “Platform provides the capability to report on effective access by utilizing stateful information solicited from factual data.” This requirement is intended to ensure the solution will provide audit data that is factual and reflects the actual state of connected systems, rather than an assumed state, based on synchronization actions.

88. **Page 14 - In item 2.18.2, please provide use case(s) for peak performance and the anticipated burst capacity needed.**
   Answer: Peak use is at the start of the fall semester onboarding roughly 15,000 students, and at the end of the fall and spring semesters when student employee positions are terminated.

89. **Page 14 - In item 2.20.2, please elaborate on the use case for “Create/delete sets of roles/attributes based on criteria”.**
   Answer: This requirement is intended to ensure the solution can create/delete authorization constructs such as groups or attributes based on logic and criteria. An example of this might be to create a group for each course section for the current semester with each student and faculty member in the group being managed dynamically. Then, 3 semesters later deleting the groups.

90. **Page 14 - In item 2.21.3, please provide use case for group nesting.**
   Answer: A use case for group nesting would be a group for a department, and a sub-department below the department. For example, our IAM Platforms department exists within Enterprise Services department. There are some permissions that IAM Platforms receives due to being in Enterprise Services and nesting IAM Platforms under Enterprise services would grant those permissions. Group nesting should be both easily visible in the IGA and exportable to Active Directory.

91. **Page 15 - In item 2.22, please describe views that might exist in the service catalog.**
   Answer: Potential views that might exist in the service catalog are: 1) a guest view that allows guests to request access to services that are not part of the birthright guest access. These may or may not require approval by the service owner(s). 2) employees/student employees requesting service accounts for their applications. 3) departments requesting affiliate identities for incoming contractors.
This is not intended to be an all-encompassing answer, and all or none of these may be implemented in the eventual service catalog.

92. **In item 2.26.3, please provide use case(s) where MSU would provision/deprovision access through flat file integration.**
   Answer: MSU’s legacy stack relies heavily on flat file integrations to load data into those systems, and would need to be supported as we work to implement the IGA.

93. **Page 16 - In item 2.27, please provide the current vendor platforms in use at MS for ID badge and physical access management.**
   Answer: See question 10.

94. **Page 16 - In item 2.27.2, please elaborate on requirements for “to support ID images, barcodes, etc.”.**
   Answer: See question 11.

95. **Page 19 - In item 2.36.3, please elaborate on use cases for “Self-service request and invite services”.**
   Answer: The solution should include the ability for a person to self-register an identity record that can be used to provision a guest or affiliate account. The solution should also provide the ability for a sponsor to create an identity record that can be used to provision a guest or affiliate account.

96. **Page 19 - In item 2.26.3, is MSU open to invite requests being sent to external email accounts?**
   Answer: Assuming this is 2.36.3, please see question 95.

97. **Page 19 - In item 2.38.1, please describe the use case for multiple identifiers amongst multiple target and source systems?**
   Answer: At MSU we have identifiers for IAM, as well as identifiers for students and employees from the ERPs that need to be kept in sync and tied to a single identity.

98. **Page 20 - In item 2.40.4, please define requirements for management of historical identities after expiration.**
   Answer: The platform will retain sufficient identity information such that the existing identifiers can be reprovisioned for an individual that returns to MSU in any capacity.

99. **Page 20 - In item 2.41.1, please describe how MSU envisions identities will be created for non-person accounts.**
   Answer: Non-person accounts will be created by requests to the team(s) that support the service the accounts will be used with. The teams supporting the services should be able to request their own service accounts, potentially with manager approval. These requests would ideally be handled by the views in the service catalog (see section 2.22).
100. **Page 20 - In item 2.45.2, please elaborate on the type of criteria/verification processes required for identity proofing.**
   Answer: See question 13.

101. **Page 24 - Will there be an MSU project manager assigned to collaborate with the implementor project manager or will the implementor provide all project management services?**
   Answer: See Question 17.

102. **Page 24 - Will MSU staff be engaged in the implementation process, particularly production configuration, or is the expectation that the implementor team will perform all tasks until the system is live?**
   Answer: MSU staff are expected to be engaged during the implementation process so that they can learn the tool, understand the implementation process, and take part in decision-making for how the tool is implemented.

103. **Page 24 - Are overseas resources permitted?**
   Answer: No

104. **Page 25 - In item 5.1.6, what is MSU’s expectation on the number and type of non-production environments?**
   Answer: MSU expects to have a minimum of 3 non-production environments.

105. **Page 25 - In item 5.1.7, will MSU staff participate in testing processes or is the expectation that the implementor will provide all testing resources?**
   Answer: See question 72.

106. **Page 31 - For items in 5.3, do non-production environments exist for each platform for testing. For Active Directory/Azure AD, is there an integrated test environment with synchronization available for testing?**
   Answer: All in scope target systems in 5.3 have at least one non-production environment, with most having two or three. There are two non-production environments of Active Directory/Azure AD available for testing, though these are not explicitly used by the IAM Platforms team and will not be greenfield.

107. **Page 26 - Section 5.5.1 reads as if this would be a separate projects(s). When would you anticipate starting this workstream and do you need us to provide the cost for these project(s)?**
   Answer: This workstream has already been started by internal MSU resources, but this initiative needs the guidance and expertise of the implementation partner to help us understand the least disruptive way to implement the new product(s). We do not see this as a separate effort, but an engagement to help us determine a phased approach for the implementation effort.
108. Page 26 - Section 5.5.2, reads as if there would be an additional effort to create new abstraction layer between ERP and IAM. Do you envision that the integration of the SoAs would go through this source or would this hub/registry be used for other integrations? When would you anticipate starting this workstream and do you need us to provide the cost for this project?
Answer: See question 31.

109. Page 26 - In section 5.5.3.5, does MSU have documentation for entitlements that need to be assigned to each group? Does MSU have documentation on entitlements that must be configured for SoD?
Answer: MSU does have documentation on entitlements that are required for each group and what will need to be configured for SoD. These will be not disclosed at this time and may not reflect future state requirements.

110. Page 26 - In section 5.5.3.5.1, you would like to be able to automatically create and manage group membership. Which in scope target systems will the solution need to create groups for?
Answer: The in-scope target systems that need the automatic directory groups are Active Directory and TeamDynamix.

111. Page 27 - In section 5.5.3.8, there’s a requirement to configure identity hub interface for self-service management of personal and DEI information. Will this be part of the expected project milestones? Would all user populations be eligible to self-service manage their information or just specific populations?
Answer: All user populations will be eligible to self-service management for their information. This includes inactive accounts after fulfilling sufficient identity assurance.

112. Page 27 - In section 5.6.1, it mentions the need to migrate request workflows from Team Dynamix. Are there available documents detailing the existing request workflows to ensure they are compatible with the proposed solution? Would all requests come through the solution instead of Team Dynamix or just requests for the in-scope systems?
Answer: Yes. We have documentation for each workflow in TeamDynamix today. However, this will not be disclosed until after the contract resulting from this RFP has been awarded. Requests for in-scope systems would come through the new solution.

113. Page 27 - In section 5.6.4, you have a desire to configure Separation of Duties (SoD) policies. For which in scope systems will SoD policies need to be setup? Will this be part of the expected project milestones?
Answer: Requirements for SoD policies will be determined during the engagement in section 5.1.2 and 5.1.3 in the implementation services statement of work. These requirements will be expected to be implemented as part of the solution.
114. Page 27 - In section 5.6.6, you have a desire to configure certification/attestation for regulatory compliance. How many certifications will you be looking for assistance configuring and what month or quarter would you expect those to launch?
Answer: The number of certifications is dependent on the total number of roles and permissions integrated into the final solution. These are expected to launch alongside the project go-live.

115. Page 27 - In section 5.6.7, you state that configuration policies so that access is tied to security training? Are you envisioning that this is a preventative control, i.e., meaning that access will not be provisioned without training or is a detective control to ensure that users who have particular access maintain their training status?
Answer: This is meant to cover both the initial training and continued training/refreshers. The solution should have the capability to disable access for anyone out of compliance.

116. Page 28 - In sections 5.7.2.2, 5.7.3.2, 5.7.4.2, it lists configure baseline roles and birthright entitlements. How many baseline roles will need to be configured? Are these roles and their entitlements already defined?
Answer: See question 34.

117. Page 28 - In section 6, there are project milestones. Are the project milestones firm or can they be adjusted? For example, if the solution build will take more than 3 months are you open to that?
Answer: The project milestones are an estimate and can be adjusted based on the solution recommendation.

118. Page 28 - In section 6, with the milestones provided, is MSU envisioning that all objectives will be implemented at once (i.e. big bang)? If so, are there reasons why MSU is not considering a phased approach?
Answer: MSU is envisioning a phased approach to ensure a smooth transition to the new IGA.

119. Page 28 - In section 6, if the schedule requires adjustment, are there particular windows where go-live events can occur within the university calendar?
Answer: This is more easily defined as when they cannot go, which is within one week either side of a semester’s start and end.

120. Page 29 - In section 8.a.vi, MSU states that there is a preference for a combination of on-site and off-site work. Does MSU have particular project activities that it would like to have completed on-site or does this statement reflect a more general spirit of focus and collaboration?
Answer: See question 2
121. Multiple Identity sources are listed on page 25, can you align them to the user types –
staff, part time, students, etc.

5.2. In Scope Sources of Authority (SoA) [see section 1 for details]:
5.2.1. SAP HCM (with identifier writeback)
5.2.2. Oracle Peoplesoft Campus Solutions (with identifier writeback)
5.2.3. Slate (with identifier writeback)
5.2.4. PageUp (with identifier writeback)
5.2.5. Enterprise Data Warehouse
5.2.6. MuleSoft

Answer: 5.2.1 SAP-HCM: Employees; 5.2.2 Oracle Peoplesoft Campus Solutions: Students; 5.2.3
Slate: Admitted students before matriculation; 5.2.4 PageUp: Employees prior to entering SAP-HCM;
5.2.5 Enterprise Data Warehouse: All populations; 5.2.6 MuleSoft: All populations.

122. Is cloud based solution allowed or has to be local on-premise solution?
Answer: See question 9.

123. Is there an existing ID or badge management system?
Answer: See question 10.

124. Is there a minimum set of 3rd party risk factors you want a solution to use to score a user?
Answer: There is no minimum set of 3rd party risk factors to use for scoring.

125. To what extent is identity security - meaning identity security posture management
(static) and identity threat detection and response (kinetic / active threats) - in-scope for
this RFP?
Answer: “Threat” detection is not in scope for this RFP and will be a part of a later initiative.

126. Is it worthwhile for a vendor to respond to a portion of one or more of the 3 sections with
solutions that address the identity security and risk management portion of an identity
program?
Answer: We will not accept partial responses to any sections in a complete RFP. You may partner
with other vendors to submit a single bid that addresses all requirements for all sections of the RFP,
or you may submit a bid that addresses all of the requirements for just 1 or 2 sections.

127. Does this RFP also cover wireless and wired network identification such as 802.1x or can a
response also provide this capability?
Answer: We are not seeking products or services for network authentication. We already have a
solution.

128. Is the intent to eliminate as many identity sources as possible and consolidate to as few
sources as possible?
Answer: The intent is to move to an identity first model and create a single SoA for identity data.

129. **Is a single user experience desired regardless of identity source?**
    Answer: Yes. MSU desires a single, unified user experience for the entire identity lifecycle.

130. **Page 8 - What is the most important or critical element of success for the deployment of the following three solutions?**
    of the following at the University:
    • Identity Data Management and Identity Governance & Administration Platform.
    • Access Management Platform.
    • Third-party / Non-Employee Management Platform.
    Answer: All three of these are extremely important to MSU and part of our roadmap.

131. **Page 8 - Are the numbers provided unique identities or is there overlap in your different roles (i.e., student employments are included in the active student numbers)? We are interested in identifying the number of unique identities and the number of contractors being held in Non-Employee Risk Management.**
    Answer: See question 65.

132. **Page 8 - Of the numbers provided, how many will you be including in your new governance solution? Are you provisioning to any of these accounts or are they being held in your access management solution? Of those numbers, can you define the number of unique, alumni, inactive, guest, or other types?**
    Answer: For unique user counts, please see question 65. For numbers included, please see question 77.

133. **Page 8 - Could you define what MSU means when they say Access Management Platform? Does this include workforce and / or customer identity & access management (CIAM)? Is MSU looking for an identity provider? Single Sign On (SSO) and / or Multi Factor Authentication (MFA)?**
    Answer: We are not looking for an identity provider or SSO/MFA solution. We are looking for a customer experience and access rights management platform, with the feature-set described in the requirements in 2.20 - 2.35.

134. **Page 8 - Can you elaborate on how you are using SailPoint IIQ and Okta today?**
    Answer: See question 22 for SailPoint IIQ use. We are using Okta as our SSO/MFA solution.

135. **Page 8 - Was there a migration assessment performed for SailPoint IIQ? If so, are you able to share those results?**
    Answer: We did not perform a migration assessment for SailPoint IIQ.
136.  **Page 10 – 2.5.1 - Could you clarify an example of 'transformations'?**  
Answer: The term transformations in this context refers to the concept of transforming data as it is written. E.g., changing a data attribute from Epoch time to MM/DD/YYYY.

137.  **Page 10 - 2.5.2 - Please define Data Normalization.**  
Answer: Data normalization can be defined as a process designed to facilitate a more cohesive form of data entry, essentially 'cleaning' the data.

138.  **Page 11 – 2.9.4 - What ITSM tools do you need to integrate with and what is the needed interaction or functionality needed?**  
Answer: See questions 3 and 61.

139.  **Page 11 – 2.10.2 - Could you provide an example of a Sponsored Identity?**  
Answer: A researcher, who is doing work for a specific research or faculty member (sponsor).

140.  **Page 12 – 2.13.2 - Could you clarify what you mean by the ability to modify source code and what sort of modifications you would want to make?**  
Answer: The need to modify source code is only targeted at open source solutions, and can be disregarded for commercial vendors.

141.  **Page 14 – 2.21.3 - Could you clarify what you mean by group nesting?**  
Answer: See question 90.

142.  **Page 16 – 2.27 - What physical access (badging) platforms do you use?**  
Answer: See question 10.

143.  **Page 18 – 2.28.3 - Could you clarify what you mean by stateful information solicited from factual data?**  
Answer: See question 87.

144.  **Page 25 – 5.3 - Could you go more in depth with the roles that the following target systems are currently serving within your organization: SailPoint IIQ, Okta, Shibboleth?**  
Answer: See question 22 for SailPoint IIQ. We are using Okta for our SSO/MFA solution, and Shibboleth for attribute release for applications that are not fully onboarded to Okta.

145.  **Page 25 – 5.4 - For your In Scope Source/Targets for Legacy/Historic imports (e.g. Sailpoint, Sentinel, etc.) are you looking for the selected Identity solution to import data from those systems or export data to them? For imports, what format is the data in for access by the selected Identity solution? For exports, is the selected Identity solution providing data outputs or does it need to interact directly with those systems?**
The selected identity solution should be able to import from and export to those systems. For imports, the data is in a database. For exports, there will be a combination of data outputs and direct system interactions.

146. **Page 27 – 5.6.1 - For migration of workflows currently in Team Dynamix, what format is the data in?**
   Answer: TDX workflows are in JSON format

147. **Can you Confirm SAP HCM is SAP SuccessFactors?**
   Answer: MSU uses SAP HCM but not SuccessFactors

148. **For Slate, do you have direct API connection into Slate today with your IAM solution to export/import data?**
   Answer: We do not currently have a direct API connection into Slate. We will be looking to onboard the Slate integration during the implementation phase of this engagement.

149. **For the in scope target systems, are you directly connecting to these for the management of users or are some of them managed by entitlements from AD/LDAP/ETC or Just In Time Provisioning via SSO?**
   Answer: We are currently directly connecting to these for the management of users. Okta is performing JIT provisioning during sign on, but only for itself. In our current configuration, Okta does not JIT provision users to other applications.

150. **Do you have a list of legacy utilities mentioned in "Configure IGA platform to replace identity administrative tools currently provided by legacy utilities."**
   Answer: See section 5.4.

151. **What database backends your Enterprise Data Warehouse?**
   Answer: Oracle 18c - 18.14

152. **For MuleSoft, does your current system pass information into it or collect events that need to occur and then process them?**
   Answer: Our current implementation requires information to be passed to it. We are working to implement an Enterprise Messaging System that will allow it to collect events.

153. **Based on the timeline and requirements, it looks like there would be a "big bang" go live of all features / process. Is that correct?**
   Answer: See question 118.
154. From a timeline perspective, will there be a steering committee involved throughout the project? If so, are there specific number of times this committee would meet, if involved, to ensure there are no delays on decisions that need to be made?  
Answer: There will be a steering committee that will meet on a scheduled cadence to ensure timely decision-making.

155. Is MSU open to leveraging a national purchasing cooperative contract?  
Answer: See question 103.

156. Has MSU engaged with any 3rd organizations to assess IAM needs and assist in the development of this RFP? If so, who?  
Answer: Yes, MSU is currently engaged with Moran Technologies to assess IAM needs and assist in the development of this RFP.

157. How many target systems are in scope for integrating with the IDAM / IGA tool? Will systems listed in section 5.2 and 5.3 be the final?  
Answer: See question 74.

158. If any of the requirements could not be accomplished with out of the box functionality and require additional scripts / integrations, would MSU like these specific requirements be called out, and the proposal to share how the vendor would accomplish it?  
Answer: Yes, MSU would like to have these called out with a proposed solution to accomplish the functional requirements.

159. If Identity Security Cloud has been finalized as the IDAM / IGA product of choice, has MSU completed SailPoint's Migration assessment? If yes, can vendor be provided with the assessment?  
Answer: Identity Security Cloud has not been finalized as the IDAM / IGA product of choice. This RFP is to determine MSU’s IDAM / IGA product of choice.

160. Who will performing the decommission of the existing tool / software(s)? Will it be the vendor or the MSU team?  
Answer: This will taken on collaboratively with MSU and the vendor.

161. Scope 2.1.3: How real time should the synchronization be? Can the synchronization be scheduled for regular interval?  
Answer: Real-time synchronization should be as immediate as possible and event driven. Scheduled synchronizations are by definition not real-time.

162. Scope 2.9.4: What are the different ITSM tools currently being used at MSU?  
Answer: See question 61.
163. **Scope 2.10.2: How many types of sponsored identities are there currently in MSU? Are the sponsored identities part of Non-Employees?**
   Answer: We have approximately 5,000 sponsored identities. These are included as the Affiliate portion of the non-employee designation.

164. **Scope 2.20.2: How many birthright and requestable roles are there currently in the existing IDAM system? Are all of them expected to be migrated to the new system?**
   Answer: We have approximately 550 roles in our existing IDAM. All of them are expected to be migrated to the new system, with the potential to add more.

165. **Scope 2.27: What system is being used for management for ID badges and physical access?**
   Answer: See question 10.

166. **Section 5.5.3.9.1.6: Legal Hold - Please elaborate. Does the IDAM system need to have the legal hold functionality or would it suffice if the IDAM system can set legal hold in some target systems like MS Entra?**
   Answer: This capability refers to identity administration. Legal hold capability should include the ability for administrators to preserve an identity so that it will remain in its current state beyond normal deprovisioning lifecycle, while also locking the user out.

167. **Section 5.7: Will Affiliate, Guest and Research be the only types of Non-Employee identities?**
   Answer: The specifics around the number of and types of non-employee entities depend upon product capabilities and options that will be flushed out during the requirements gathering and design phase of the implementation services.

168. **Page 8 mentions “over 1.5 million usernames are taken from our namespace”. Does this mean these usernames were used in past and cannot be reused? Is there a repository that contains these 1.5 million usernames already used?**
   Answer: Yes, these usernames have been used previously and cannot be reused. There is a repository that contains these usernames.

169. **List and explain the functionality of legacy/home grown IAM components like Creator, D20, ACORNS etc.**
   Answer: See question 3. Additional documentation is available by request, see question 62 for how to request.

170. **1.0 - Background Page 8: Proposal Language: Over 12,000 permanent and part-time faculty, and staff; 49,695 students; 16,000 annual student employments; and 3,000 annual graduate teaching and research assistant appointments.**
Are the numbers provided unique identities or is there overlap in your different roles (i.e., student employments are included in the active student numbers)? We are interested in identifying the number of unique identities and the number of contractors being held in Non-Employee Risk Management.
Answer: See question 65.

171. 1.0 Background Page 8:
Proposal Language: Over 100,000 guest accounts, 750,000 identities, and over 1.5 million usernames taken from our namespace.
Question: Of the numbers provided, how many will you be including in your new governance solution? Are you provisioning to any of these accounts or are they being held in your access management solution? Of those numbers, can you define the number of unique, alumni, inactive, guest, or other types?
Answer: All will be included in the new IGA, with the majority being solely held in the IGA. Please see question 65 for unique counts.

172. About exploring hybrid options - Is MSU open to exploring non-USA/Canada based hybrid options to provide the requested services and solutions? Our clients typically want to leverage this option to get access to our global pool of cybersecurity intelligence analysts in a cost-efficient manner. Please confirm.
Answer: See question 103.

173. About Budget - Can MSU provide any information on the budget required to support these services? (E.g., budget details)
Answer: In order to ensure an unbiased procurement process, MSU is not sharing budget information at this time.

174. About Current Vendor/Supplier - Is MSU currently using any service providers that are assisting the College in performing the requested services? If so, who are these providers?
Answer: No. We are not currently working with any service providers for the services requested. We used a vendor to assist with writing our IAM Roadmap/RFP requirements and that vendor is still consulting with MSU during this RFP selection.

175. About Single/multiple award contract - Does MSU plan to select a single vendor or multiple vendors to provide these services?
Answer: MSU will select the vendor or vendors who can deliver the best solution in each service; however, each service will only be awarded to one vendor. One vendor can be awarded multiple service contracts.

176. About multiple categories response options - Is MSU seeking respondents that can offer all categories of services, or can the respondent elect to provide certain services?
Answer: See question 126.