MICHIGAN STATE UNIVERSITY

REQUEST FOR PROPOSAL
RFP #925540

SailPoint Implementation Partner

RFP Timeline	
RFP Issue Date:	April 14, 2026
Deadline for Respondent Questions to MSU:	April 21, 2026
RFP Response Due Date:	**May 19,2026, 3:00 pm Eastern**
Estimated Contract Award	End of June 2026

RFP Contact	
Name:	Amber Marr
Unit:	MSU Procurement
Email:	amber.marr@msu.edu
Phone:	517-884-6166

DESCRIPTION: Michigan State University (the "**University**" or "**MSU**") is soliciting proposals through this Request for Proposal ("**RFP**") for the purpose of selecting a SailPoint IdentityIQ Implementation Partner. The requested services are more thoroughly described under the Scope of Work Section of this RFP. Firms intending to respond to this RFP are referred to herein as a "**Respondent**" or "**Supplier**."

MICHIGAN STATE UNIVERSITY

PROPOSAL INSTRUCTIONS

1. **PROPOSAL PREPARATION.** The University recommends reading all RFP materials prior to preparing a proposal, particularly these Proposal Instructions. Respondents must follow these Proposal Instructions and provide a complete response to the items indicated in the table below. References and links to websites or external sources may not be used in lieu of providing the information requested in the RFP within the proposal. Include the Respondent's company name in the header of all documents submitted with your proposal.

Document	Description	Response Instructions
Cover Page	Provides RFP title and number, important dates, and contact information for MSU	Informational
Proposal Instructions	Provides RFP instructions to Respondents	Informational
Respondent Information Sheet	Company and Contact Information, and Experience	Respondent must complete and submit by proposal deadline
Scope of Work	Describes the intended scope of work for the RFP	Respondent must complete and submit by proposal deadline
Pricing	Pricing for goods and services sought by the University through this RFP	Respondent must complete and submit by proposal deadline
Master Service Agreement	Provides legal terms for a contract awarded through this RFP	Deemed accepted by Respondent unless information required in **Section 9, Master Service Agreement** is submitted by proposal deadline

2. **EXPECTED RFP TIMELINE**.

Activity	Date
Issue RFP	April 14, 2026
Deadline for Respondent Questions to MSU	April 21, 2026
RFP Response Due	**May 19,2026, 3:00 pm Eastern**
Estimated Contract Award	End of June 2026

3. **CONTACT INFORMATION FOR THE UNIVERSITY.** The sole point of contact for the University concerning this RFP is listed on the Cover Page. Contacting any other University personnel, agent, consultant, or representative about this RFP may result in Respondent disqualification.

4. **QUESTIONS.** Respondent questions about this RFP must be submitted electronically by email to the contact listed on the cover page of this RFP. In the interest of transparency, only written questions are accepted. Answers to all questions will be sent to Respondents via email. Submit questions by referencing the following: (i) Question Number, (ii) Document Name, (iii) Page Number, and (iv) Respondent Question. Please refer to **Section 2** above for the deadline to submit questions.

5. **MODIFICATIONS.** The University may modify this RFP at any time. Modifications will be sent via email. This is the only method by which the RFP may be modified.

6. **DELIVERY OF PROPOSAL.** The Respondent must submit its proposal, all attachments, and any modifications or withdrawals electronically via email to the contact listed on the cover page of this RFP. **The price proposal should be saved separately from all other proposal documents and should be sent as a separate attachment from the other proposal documents.** The Respondent should submit all documents in a modifiable (native) format (examples include but are not limited to: Microsoft Word or Excel and Google Docs or Sheets). In addition to submitting documents in a modifiable format, the Respondent may also submit copies of documents in PDF. Respondent's failure to submit a proposal as required may result in disqualification. The proposal and attachments must be fully uploaded and submitted prior to the proposal deadline. **Do not wait until the last minute to submit a proposal**. The University **may not** allow a proposal to be submitted after the proposal deadline identified in the Cover Page, even if a portion of the proposal was already submitted.

7. **MANDATORY MINIMUM REQUIREMENTS.** The RFP may contain minimum qualifications, which will be identified as "**Mandatory Minimum Requirements**" in the Scope of Work Section of this RFP. If the RFP does contain mandatory minimum requirements, any proposal not meeting these minimum requirements **will be deemed non-qualified and will not be considered**. All proposals meeting these mandatory minimum requirements will proceed for review and evaluation consistent with **Section 8**, **Evaluation Process**.

8. **EVALUATION PROCESS.** The University will convene a team of individuals from various Departments within MSU to evaluate each proposal based on each Respondent's ability to provide the required services, taking into consideration the overall cost to the University. The University may require an oral presentation of the Respondent's proposal; conduct interviews, research, reference checks, and background checks; and request additional price concessions at any point during the evaluation process.

   Proposals will be evaluated based on the Respondent's ability to demonstrate proven capability, not just stated compliance.

   MSU may require:

   - Live demonstrations
   - Detailed solution walkthroughs
   - Reference architecture
   - Client references for comparable environments

   The following criteria will be used to evaluate each proposal:

Criteria	Weight
Implementation Approach & Technical Quality	**20%**
Identity Data Management & Integrity Strategy	**15%**
Migration Strategy, Risk Management & Coexistence	**15%**
Governance Model & Compliance Enablement	**10%**
Knowledge Transfer & Sustainability	**10%**
Total cost to MSU	**15%**
Supplier Risk	**10%**
Acceptance of and adherence to legal terms	**5%**
Total Score	**100%**

Implementation Approach & Technical Quality (20%)

Sub-Criteria	Description
Architecture & Solution Design	Clarity, completeness, and scalability of the proposed IAM architecture, including alignment with SailPoint best practices
Integration Approach	Approach for integrating with multiple SoAs and target systems, including handling of middleware (e.g., MuleSoft) and avoiding hidden logic
Provisioning & Deprovisioning Design	Design for automated provisioning, deprovisioning, and lifecycle management across all target systems
Testing & Validation Strategy	Approach for validating that provisioning and integrations function correctly in target systems (not just test execution)
Technical Depth & Feasibility	Demonstrated understanding of complex IAM environments and ability to deliver at MSU scale

Identity Data Management & Integrity Strategy (15%)

Sub-Criteria	Description
Identity Correlation Strategy	Approach for correlating identities across multiple systems of authority (e.g., SAP, PeopleSoft, Slate, PageUp)
Handling of Incomplete or Evolving Identities	Strategy for managing pre-hire identities and transitions (e.g., SSN to EmplID)
Duplicate Prevention & Resolution	Methods for detecting, preventing, and resolving duplicate identities
Identifier Strategy	Approach for unique identifier creation, mapping, lifecycle management, and writeback
Data Integrity & Reconciliation	Ability to detect and remediate discrepancies between IAM and downstream systems (e.g., “provisioned but not present” scenarios)

Migration Strategy, Risk Management & Coexistence (15%)

Sub-Criteria	Description
Legacy System Analysis	Ability to identify and understand identity-related logic in legacy systems (e.g., ACORNS, D20, Creator)
Data Migration & Cleansing Approach	Strategy for cleansing, transforming, and migrating identity and access data (not lift-and-shift)
Identity Consolidation	Approach for reconciling and consolidating identities across legacy systems
Coexistence Strategy	Plan for operating legacy and new systems in parallel without conflicts or duplicate provisioning
Decommissioning Strategy	Clarity and feasibility of plan to retire legacy IAM systems and eliminate redundant logic
Risk Identification & Mitigation	Identification of key risks and effectiveness of mitigation strategies

Governance Model & Compliance Enablement (10%)

Sub-Criteria	Description
Role & Access Model Design	Approach to defining and managing roles, birthright access, and entitlement structures
Certification & Attestation	Strategy for access reviews, certifications, and ongoing governance
Separation of Duties (SoD)	Design and enforcement of SoD policies
Regulatory Compliance Alignment	Ability to support FERPA, HIPAA, GDPR, and other regulatory requirements
Policy Enforcement	Effectiveness of tying governance policies to actual provisioning and access control

Knowledge Transfer & Sustainability (10%)

Sub-Criteria	Description
Knowledge Transfer Approach	Quality and completeness of training and knowledge transfer to MSU staff
Documentation Quality	Delivery of accurate, complete, and usable documentation (e.g., as-built, runbooks)
Operational Readiness	Preparedness of the solution for ongoing operations and support
Maintainability & Support Model	Ease of maintaining the solution and avoiding over-customization
Transition to Operations	Effectiveness of transition from implementation to steady-state support

Vendors must provide specific examples, artifacts, or demonstrations to support their responses. Responses that are high-level or lack supporting detail may receive reduced scores.

9. **MASTER SERVICE AGREEMENT**. The University strongly encourages strict adherence to the terms and conditions set forth in the Master Service Agreement. The University reserves the right to deem a proposal non-responsive for failure to accept the Master Service Agreement. Nevertheless, the Respondent may submit proposed changes to the Master Service Agreement in track changes (i.e., visible edits) with an explanation of the Respondent's need for each proposed change. Failure to include track changes with an explanation of the Respondent's need for the proposed change constitutes the Respondent's acceptance of the Master Service Agreement. General statements, such as "the Respondent reserves the right to negotiate the terms and conditions," may be considered non-responsive.

10. **CLARIFICATION REQUEST.** The University reserves the right to issue a Clarification Request to a Respondent to clarify its proposal if the University determines the proposal is not clear. Failure to respond to a Clarification Request timely may be cause for disqualification.

11. **RESERVATIONS.** The University reserves the right to:
    a. Disqualify a Respondent for failure to follow these instructions.
    b. Discontinue the RFP process at any time for any or no reason. The issuance of an RFP, your preparation and submission of a proposal, and the University's subsequent receipt and

evaluation of your proposal does not commit the University to award a contract to you or anyone, even if all the requirements in the RFP are met.

c. Consider late proposals if: (i) no other proposals are received; (ii) no complete proposals are received; (iii) the University received complete proposals, but the proposals did not meet mandatory minimum requirements or technical criteria; or (iv) the award process fails to result in an award.
d. Consider an otherwise disqualified proposal, if no other proposals are received.
e. Disqualify a proposal based on: (i) information provided by the Respondent in response to this RFP; or (ii) if it is determined that a Respondent purposely or willfully submitted false or misleading information in response to the RFP.
f. Consider prior performance with the University in making its award decision.
g. Consider total-cost-of-ownership factors (e.g., transition and training costs) when evaluating proposal pricing and in the final award.
h. Refuse to award a contract to any Respondent that has outstanding debt with the University or has a legal dispute with the University.
i. Require all Respondents to participate in a Best and Final Offer round of the RFP.
j. Enter into negotiations with one or more Respondents on price, terms, technical requirements, or other deliverables.
k. Award multiple, optional-use contracts, or award by type of service or good.
l. Evaluate the proposal outside the scope identified in **Section 8, Evaluation Process**, if the University receives only one proposal.
m. Obtain and consider information from other sources concerning a Respondent, such as the Respondent's capability and performance under other contracts, the qualifications of any subcontractor identified in the Proposal, the Respondent's financial stability, past or pending litigation, and other publicly available information.
n. Utilize third parties to assist in the evaluation process, provided such parties are subject to confidentiality requirements.

12. **AWARD RECOMMENDATION.** The contract will be awarded to the responsive and responsible Respondent who offers the best value to the University, as determined by the University. Best value will be determined by the Respondent meeting any mandatory minimum requirements and offering the best combination of the factors in **Section 8**, **Evaluation Process**, and price, as demonstrated by the proposal. The University will email a **Notice of Award** to all Respondents. A Notice of Award does not constitute a contract, as the parties must reach final agreement on a signed contract before any services can be provided. The awarded Respondent is prohibited from partnering with losing bidders unless the RFP specifically allows for such arrangement, and any violation of this prohibition may result in disqualification of the awarded Respondent.

13. **GENERAL CONDITIONS.** The University will not be liable for any costs, expenses, or damages incurred by a Respondent participating in this solicitation. The Respondent agrees that its proposal will be considered an offer to do business with the University in accordance with its proposal, including the Master Service Agreement, and that its proposal will be irrevocable and binding for a period of 180 calendar days from date of submission. If a contract is awarded to the Respondent, the University may, at its option, incorporate any part of the Respondent's proposal into the contract. This RFP is not an offer to enter into a contract. This RFP may not provide a complete statement of the University's needs, or contain all matters upon which agreement must be reached. Proposals submitted via email are the University's property.

14. **FREEDOM OF INFORMATION ACT.** Respondent acknowledges that any responses, materials, correspondence or documents provided to the University may be subject to the State of Michigan Freedom of Information Act ("FOIA"), Michigan Compiled Law 15.231 *et seq*., and may be released to third parties in compliance with FOIA or any other law. Questions about the Respondent's own

performance can be directed to the RFP Contact indicated on page 1 of this document. Questions about the overall evaluation and any other post-award inquiries must be submitted via a formal FOIA request to the Michigan State University FOIA office.

MICHIGAN STATE UNIVERSITY

RESPONDENT INFORMATION SHEET

Please complete the following Information Sheet in the space provided:

Information Sought	Response
Contact Information	
Respondent's sole contact person during the RFP process. Include name, title, address, email, and phone number.	
Person authorized to receive and sign a resulting contract. Include name, title, address, email, and phone number.	
Respondent Background Information	
Legal business name and address. Include business entity designation, e.g., sole proprietor, Inc., LLC, or LLP.	
What state was the company formed in?	
Main phone number	
Website address	
DUNS# AND/OR CCR# (if applicable):	
Number of years in business and number of employees	
Legal business name and address of parent company, if any	
Has your company (or any affiliates) been a party to litigation against Michigan State University? If the answer is yes, then state the date of initial filing, case name and court number, and jurisdiction.	
Experience	
Describe relevant experiences from the last 5 years supporting your ability to successfully manage a contract of similar size and scope for the services described in this RFP.	
Experience 1	
Company name Contact name Contact role at time of project Contact phone Contact email	
1. Project name and description of the scope of the project 2. What role did your company play? 3. How is this project experience relevant to the subject of this RFP?	
Start and end date (mm/yy – mm/yy)	
Status (completed, live, other – specify phase)	
Experience 2	
Company name Contact name Contact role at time of project Contact phone	

Contact email	
1. Project name and description of the scope of the project 2. What role did your company play? 3. How is this project experience relevant to the subject of this RFP?	
Start and end date (mm/yy – mm/yy)	
Status (completed, live, other – specify phase)	
Experience 3	
Company name Contact name Contact role at time of project Contact phone Contact email	
1. Project name and description of the scope of the project 2. What role did your company play? 3. How is this project experience relevant to the subject of this RFP?	
Start and end date (mm/yy – mm/yy)	
Status (completed, live, other – specify phase)	

MICHIGAN STATE UNIVERSITY

SCOPE OF WORK

Please address each of the sections below in a written response, which can be completed on a separate sheet (using the same section headings).

1. Background.

MSU is soliciting proposals for vendor/implementer services to assist in the implementation of a **SailPoint IdentityIQ & Access Management Platform** at the University.

Facets of the University that bear on this project:

- More than 200 programs of study offered by 17 degree-granting colleges.
- Nearly 200 administrative units (providing infrastructural support to the institution's mission).
- Professional medical programs in osteopathic, allopathic, veterinary medicine, and nursing.
- Out-patient clinical practice centers for osteopathic, allopathic, and nursing. Teaching hospital for small and large animal veterinary medicine.
- Sponsored research of about $725 million in 2019.
- As the nation's pioneer land-grant university, MSU continues in that tradition through state-wide agricultural extension agencies, and experimental research stations funded separately by the state of Michigan.
- Significant auxiliary budgets and self-supporting units including, but not limited to, athletics, and housing and food services.
- 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.
- Over 100,000 guest accounts, 750,000 identities, and over 1.5 million usernames taken from our namespace.

Though Michigan State University (MSU) Information Technology Services (IT Services) delivers consistent and dependable account provisioning services for a wide range of IT applications and services, the current MSU Identity and Access Management (IAM) environment was implemented one piece at a time to solve specific problems and has grown in an ad hoc, rather than strategic, manner over decades. There has been significant growth in the complexity of identities and privileges since the solution was first implemented, the home-grown components are becoming more difficult to maintain and adapt, and the commercial and open-source components are loosely integrated at best. Both the University's growth as well as changing technological demands require that the MSU IAM environment become more strategic and holistic, better standardized, data driven, more automated, and flexible.

The current identity and access management services are comprised of a collection of legacy homegrown and recent industry leading products deployed across the campus landscape that include:

- Home-grown components and custom databases such as: Creator, D20, Sentinel/D6501, ACORNS, etc.
- Commercial and Open-source solutions such as: MuleSoft, IBM DataStage, SailPoint IIQ, Okta, Shibboleth, Active Directory, Open LDAP, MIT Kerberos, Google Workspace, Microsoft 365, etc.

MSU is looking for a partner who can assist in **implementing SailPoint** and replace the homegrown components with the functionality and features of SailPoint.

2. Definition of Success

1. The implementation will be considered functionally successful when:

- SailPoint IdentityIQ is implemented as the authoritative identity governance and administration platform, replacing identified homegrown IAM components and integrations in scope.

- In-scope Sources of Authority (SoAs), target systems, and legacy/historic systems are integrated in accordance with approved designs, with data flowing reliably, securely, and in near real-time where required.
- Identity lifecycle events (joiner, mover, leaver), baseline roles, birthright entitlements, and automated access workflows as designed across employee, student, affiliate, guest, and research populations.
- Identity matching, resolution, and unique identifier assignment are accurate, repeatable, and auditable at MSU scale.
- Audit logging, reporting, certifications, and separation-of-duties controls are implemented and demonstrably support MSU's regulatory and compliance obligations (e.g., FERPA, HIPAA etc.).

2. Data Quality and Identity Integrity

The implementation will be considered successful when:

- Identity data is ingested, normalized, matched, and governed in a manner that materially improves data quality, consistency, and traceability compared to the current environment.
- Data hygiene, transformation rules, and match resolution processes are clearly defined, documented, and operationalized.
- Authoritative source conflicts are handled through defined governance processes rather than ad-hoc or manual intervention.
- Diversity, Equity, and Inclusion (DEI) attributes (including names, pronouns, diacritics, and honorifics) are supported end-to-end without loss or corruption.

3. Cutover, Coexistence, and Risk Management

The implementation will be considered successful when:

- A phased migration strategy is executed that minimizes disruption to critical university services.
- Legacy IAM components are retired in a controlled, sequenced manner aligned with documented dependency analysis.
- Clear coexistence strategies are defined and executed where parallel operation is required during transition.
- Rollback and contingency plans are defined, tested, and documented for major cutover events.
- MSU leadership has confidence in the stability and resilience of the IAM environment at each major milestone.

4. Governance and Operating Model Readiness

The implementation will be considered successful when:

- MSU has a clearly defined post-go-live operating model for IAM, including administrative responsibilities, engineering ownership, data stewardship roles, and governance bodies.
- Decision authority for identity data, access policy, exceptions, and escalations is clearly documented and understood.
- Business units, system owners, and data stewards are appropriately integrated into request, approval, and certification workflows.
- Governance processes are designed to scale with institutional growth rather than requiring future re-architecture.

5. Knowledge Transfer and Institutional Sustainability

The implementation will be considered successful when:

- MSU staff are fully trained and capable of administering, supporting, and evolving the SailPoint platform without long-term dependency on the implementation partner.
- Documentation is complete, current, and usable, including:
    - As-built architecture and integration documentation
    - Operational runbooks and support procedures
    - Configuration and customization rationale

- MSU is positioned to independently onboard new systems, identity populations, and policy changes using the established framework.

6. Program Governance and Delivery Success

The implementation will be considered successful when:

- Roles, responsibilities, and escalation paths between MSU and the implementation partner are clearly defined and adhered to.
- Project governance supports timely decision-making, risk management, and change control.
- Deliverables are reviewed and accepted based on agreed-upon success criteria rather than solely on completion of tasks.
- The implementation partner demonstrates a clear understanding of MSU's institutional context, complexity, and risk tolerance.

7. Overall Outcome

Ultimately, success for this engagement means that MSU transitions from a brittle, fragmented IAM ecosystem to a strategic, governable, and sustainable identity platform that supports the University's academic, research, clinical, and administrative missions for the next decade and beyond.
Respondents are expected to explicitly describe how their proposed approach, staffing model, deliverables, and timeline support this definition of success.

3. SailPoint Implementation Overview

A workgroup will be created of members who will be responsible for planning and executing the tasks for the project. The workgroup will be complemented by a vendor/implementation partner experienced in these kinds of activities. The MSU workgroup members will guide and review the deliverables and provide feedback on a weekly or as needed basis. Subject matter experts and stakeholders will also be expected to participate by contributing verbal or documented information to the work of the workgroup.

The project will be completed using the following methodology:

- Assign a project manager on a part-time (1/4 FTE per initiative) basis to work closely with the MSU Project Manager and the team to manage the project.
- Work closely with the implementation partner to review current state, identifying business requirements, integration requirements (source and target), data dependencies and schema mappings, required data transformations.
- implementation partner will produce solution(s) design based on gathered requirements and will solicit institutional feedback for necessary adjustments.
- implementation partner will build the solution(s) based on gathered requirements from the approved solution(s) design.
- Michigan State University workgroup members will validate solution(s) build, confirming the solution(s) meet the institution's business requirements and needs.
- Implementation Partner will assist with the deployment of the solution(s) in the institution's Test and Production environment.

4. SailPoint Implementation Requirements

4.1. Project Objectives

For each implementation engagement, the Vendor shall provide end-to-end delivery of SailPoint implementation services, including planning, design, configuration, testing, deployment, and transition to operations. Deliverables must be measurable, reviewable, and formally approved by MSU.

4.1.1. Project Management and Governance

The Vendor shall:

4.1.1.1. Provide a named project manager responsible for delivery
4.1.1.2. Develop and maintain a detailed integrated project plan (Vendor + MSU tasks, dependencies, critical path)
4.1.1.3. Establish *governance structure, including:*
4.1.1.3.1. Weekly status reporting (risks, issues, milestones)
4.1.1.3.2. RAID log ownership
4.1.1.3.3. Escalation procedures
4.1.1.4. Define clear roles and responsibilities (RACI)

4.1.2. Requirements and Discovery

The Vendor shall:

4.1.2.1. Lead structured discovery workshops across business and technical stakeholders
4.1.2.2. Produce validated requirements documentation, including:
4.1.2.3. Identity lifecycle (Joiner/Mover/Leaver)
4.1.2.4. Non-employee populations (e.g., guests, affiliates, pre-hires)
4.1.2.5. Access request, certification, and provisioning flows
4.1.2.6. Provide traceability from requirements → design → implementation → test cases

4.1.3. Use Cases and Identity Lifecycle Modeling

The Vendor shall:

4.1.3.1. Define end-to-end lifecycle use cases for each identity type, including but not limited to:
4.1.3.1.1. Employees
4.1.3.1.2. Contractors / Guests
4.1.3.1.3. Pre-hires (pre-EmplID scenarios using alternate identifiers such as SSN)
4.1.3.2. Document:
4.1.3.2.1. Source systems of truth
4.1.3.2.2. Identity correlation rules
4.1.3.2.3. Provisioning triggers and timing expectations
4.1.3.3. Validate lifecycle scenarios against real-world edge cases

4.1.4. Business Process Design

The Vendor shall:

4.1.4.1. Provide specific, actionable recommendations for process improvements
4.1.4.2. Clearly distinguish:
4.1.4.2.1. Current state vs. future state
4.1.4.3. Identify:
4.1.4.3.1. Manual steps to be eliminated
4.1.4.3.2. Control gaps and audit risks

4.1.5. Solution Design Documentation

The Vendor shall:

4.1.5.1. Produce comprehensive design artifacts, including:
4.1.5.1.1. Logical and physical architecture
4.1.5.1.2. Integration design (e.g., LDAP, HR systems, AD, etc.)
4.1.5.1.3. Data flows and reconciliation logic

4.1.5.1.4. Error handling and retry mechanisms
4.1.5.1.5. Role model and access policy design

4.1.6. Integration and Testing Strategy

The Vendor shall:

4.1.6.1. Define and implement a multi-environment strategy (e.g., DEV, TEST, PROD)
4.1.6.2. Design a testing framework that includes:
4.1.6.2.1. Independent validation of provisioning outcomes
4.1.6.2.2. Reconciliation verification across systems
4.1.6.3. Ensure all integrations support:
4.1.6.3.1. Idempotency
4.1.6.3.2. Logging and traceability
4.1.6.3.3. Failure recovery

4.1.7. Testing Execution

The Vendor shall:

4.1.7.1. Develop and execute:
4.1.7.1.1. Unit tests
4.1.7.1.2. System integration tests
4.1.7.1.3. User Acceptance Testing (UAT)
4.1.7.2. Provide documented test cases and results
4.1.7.3. Support MSU in UAT, including defect resolution

4.1.8. Deployment and Go-Live Planning

The Vendor shall:

4.1.8.1. Develop a detailed go-live plan, including:
4.1.8.1.1. Cutover steps
4.1.8.1.2. Rollback procedures
4.1.8.1.3. Validation checkpoints
4.1.8.2. Coordinate all stakeholders for deployment readiness

4.1.9. Operational Readiness and Documentation

The Vendor shall:

4.1.9.1. Deliver runbooks and operational procedures, including:
4.1.9.1.1. Provisioning failure handling
4.1.9.1.2. Reconciliation processes
4.1.9.1.3. Incident response workflows
4.1.9.2. Provide backup and recovery procedures

4.1.10. Production Deployment

The Vendor shall:

4.1.10.1. Migrate the solution to a highly available production environment
4.1.10.2. Validate:
4.1.10.2.1. Performance
4.1.10.2.2. Scalability
4.1.10.2.3. Failover capabilities

4.1.11. Go-Live and Hypercare Support

The Vendor shall:

4.1.11.1. Provide post-go-live (hypercare) support for a defined period (e.g., 30–60 days)
4.1.11.2. Resolve defects and stabilize operations
4.1.11.3. Transition ownership to MSU

4.1.12. Training and Knowledge Transfer

The Vendor shall:

4.1.12.1. Deliver role-based training, including:

4.1.12.1.1. Administrators

4.1.12.1.2. Help desk / operations

4.1.12.1.3. Business users (if applicable)

4.1.12.2. Provide recorded sessions and documentation

4.1.13. As-Built Documentation

The Vendor shall:

4.1.13.1. Deliver final as-built documentation, including:

4.1.13.1.1. Configurations

4.1.13.1.2. Customizations

4.1.13.1.3. Integration mappings

4.1.13.2. Ensure documentation reflects actual deployed state, not design intent

4.2. In Scope Sources of Authority (SoA) [see section 1 for details]:

4.2.1. **The Vendor shall design, implement, and validate integrations with the following Systems of** Authority (SoA). The Vendor is responsible for establishing a cohesive, enterprise identity data model across all sources.

4.2.1.1. For each system, the Vendor must clearly define and document:

4.2.1.2. Data ownership and authoritative attributes (at the attribute level)

4.2.1.3. Identity correlation and matching logic across systems

4.2.1.4. Data precedence and conflict resolution rules

4.2.1.5. Identifier generation, mapping, and writeback behavior

4.2.2. The Vendor shall ensure that a single, unique identity is maintained across all SoAs, including reconciliation of identities originating from multiple upstream systems.

4.2.3. The Vendor shall not treat middleware or integration platforms (e.g., MuleSoft, DataStage) as authoritative sources of identity data unless explicitly approved. All authoritative data must be traceable to a system of record.

4.2.4. General Requirements for All SoA Integrations

For each SoA listed below, the Vendor shall:

4.2.4.1. Data Ownership and Authority

4.2.4.1.1. Define and document:

4.2.4.1.1.1. Authoritative attributes by system (e.g., legal name, status, affiliation, identifiers)

4.2.4.1.1.2. System of record at the attribute level, not solely by system

4.2.4.1.2. Define and implement data precedence rules where multiple SoAs provide overlapping attributes

4.2.4.2. Identity Correlation and Duplicate Prevention

4.2.4.2.1. Design, implement, and validate identity correlation logic across all SoAs, including:

4.2.4.2.1.1. Deterministic and/or probabilistic matching rules

4.2.4.2.2. Handling of missing, inconsistent, or delayed identifiers (e.g., pre-hire scenarios)

4.2.4.2.3. Implement controls to prevent duplicate identity creation

4.2.4.2.4. Reconcile existing identities across systems to establish a single authoritative identity record

4.2.4.3. Data Ingestion and Processing

4.2.4.3.1. Support event-driven and/or batch ingestion, with clearly defined timing and latency expectations

4.2.4.3.2. Handle high-volume identity transactions (e.g., semester starts, hiring cycles) without degradation

4.2.4.3.3. Ensure ingestion processes are idempotent and repeatable

4.2.4.4. Error Handling, Reconciliation, and Observability

4.2.4.4.1. Implement robust error handling and retry mechanisms

4.2.4.4.2. Provide end-to-end logging, monitoring, and traceability for all identity data flows

4.2.4.4.3. Implement automated reconciliation processes to:

4.2.4.4.3.1. Detect discrepancies between SoAs and downstream systems

4.2.4.4.3.2. Identify missing or incorrectly provisioned accounts

4.2.4.4.3.3. Trigger remediation workflows

4.2.4.5. Data Flow Transparency (Required Deliverable)

4.2.4.5.1. Provide detailed data flow diagrams illustrating:

4.2.4.5.1.1. All inbound and outbound identity data flows

4.2.4.5.1.2. Integration points (direct vs via middleware)

4.2.4.5.1.3. Transformation logic and ownership boundaries

4.2.5. Identifier Strategy and Writeback Requirements

The Vendor shall define and implement a comprehensive enterprise identifier strategy, including:

4.2.5.1. Identifier Design and Mapping

4.2.5.1.1. Define a canonical identity identifier model, including:

4.2.5.1.1.1. Unique identifier generation strategy

4.2.5.1.1.2. Mapping of identifiers across all SoAs and downstream systems

4.2.5.1.2. Support identity lifecycle transitions, including:

4.2.5.1.2.1. Pre-hire → hire (e.g., SSN to EmplID mapping)

4.2.5.1.2.2. Cross-population identity merging (e.g., student → employee)

4.2.5.2. Identifier Writeback

4.2.5.2.1. Design and implement explicit identifier writeback processes, including:

4.2.5.2.1.1. Target systems for writeback

4.2.5.2.1.2. Timing (real-time vs batch)

4.2.5.2.1.3. Data validation prior to writeback

4.2.5.2.2. Ensure:

4.2.5.2.2.1. Idempotent operations (no duplication or corruption)

4.2.5.2.2.2. Failure handling and retry logic

4.2.5.2.2.3. Auditability of all writeback events

4.2.5.3. Data Integrity and Drift Prevention

4.2.5.3.1. Prevent identifier drift or duplication across systems

4.2.5.3.2. Continuously validate identifier consistency between SailPoint and SoAs

4.2.5.3.3. Implement controls to detect and remediate:

4.2.5.3.3.1. Orphaned identities

4.2.5.3.3.2. Conflicting identifiers
4.2.5.3.3.3. Partial identity records
4.2.5.3.4. Critical Requirement: “Writeback” must be explicitly designed, implemented, and validated. Vendor responses that only state “supported” will be considered non-responsive.

4.2.6. Source-Specific Requirements

4.2.6.1. SAP HCM (with identifier writeback)

4.2.6.1.1. Define role as primary SoA for employee lifecycle events
4.2.6.1.2. Support:
4.2.6.1.2.1. Hire, rehire, termination, job changes, and position updates
4.2.6.1.3. Ensure:
4.2.6.1.3.1. Alignment with HR data governance policies
4.2.6.1.3.2. Accurate propagation of lifecycle events to downstream systems
4.2.6.1.4. Validate synchronization between SAP and all dependent systems

4.2.6.2. Oracle PeopleSoft Campus Solutions (with identifier writeback)

4.2.6.2.1. Define role for:
4.2.6.2.1.1. Student lifecycle
4.2.6.2.1.2. Affiliate and academic relationships
4.2.6.2.2. Handle overlapping populations, including:
4.2.6.2.2.1. Student employees
4.2.6.2.2.2. Dual-affiliated identities
4.2.6.2.3. Define clear precedence rules relative to SAP HCM and other SoAs

4.2.6.3. Slate (with identifier writeback)

4.2.6.3.1. Support pre-hire / applicant identity lifecycle
4.2.6.3.2. Define:
4.2.6.3.2.1. When identity records are created in SailPoint
4.2.6.3.2.2. Correlation strategy prior to availability of primary identifiers (e.g., EmplID)
4.2.6.3.3. Implement transition logic from applicant to employee identity
4.2.6.3.4. Handle partial and evolving identity data

4.2.6.4. PageUp (with identifier writeback)

4.2.6.4.1. Support recruitment lifecycle similar to Slate
4.2.6.4.2. Define:
4.2.6.4.2.1. Relationship and precedence relative to Slate and SAP HCM
4.2.6.4.3. Prevent duplicate identity creation across recruiting platforms
4.2.6.4.4. Ensure consistent identity correlation across applicant systems

4.2.6.5. Enterprise Data Warehouse (EDW)

4.2.6.5.1. Explicitly define role as:
4.2.6.5.1.1. Non-authoritative reporting/aggregation system, unless otherwise approved
4.2.6.5.2. Clarify:
4.2.6.5.2.1. Whether EDW contributes identity attributes or strictly consumes them
4.2.6.5.3. Prevent:
4.2.6.5.3.1. Circular data dependencies

4.2.6.5.3.2. Use of derived or stale data as authoritative identity inputs

4.2.6.6. MuleSoft

4.2.6.6.1. Define role strictly as:

4.2.6.6.1.1. Integration and orchestration layer, not a system of authority

4.2.6.6.2. Document:

4.2.6.6.2.1. All integrations routed through MuleSoft vs direct connectors

4.2.6.6.2.2. Any transformation logic applied within MuleSoft

4.2.6.6.3. Ensure:

4.2.6.6.3.1. All transformations are transparent, documented, and do not obscure authoritative data ownership

4.2.6.6.3.2. No identity data ownership is implicitly shifted to middleware

4.2.6.7. Additional Mandatory Requirement: Legacy Rationalization

The Vendor shall:

4.2.6.7.1. Identify all existing IAM-related functionality currently implemented across:

4.2.6.7.1.1. Homegrown systems [e.g., Forms Tracking System (FTU)]

4.2.6.7.1.2. Middleware (e.g., MuleSoft, DataStage)

4.2.6.7.1.3. Databases and scripts

4.2.6.7.2. Define how each function will be:

4.2.6.7.2.1. Replaced by SailPoint

4.2.6.7.2.2. Retired

4.2.6.7.2.3. Or explicitly retained (with justification)

4.2.6.7.3. Provide a roadmap for decommissioning legacy identity logic and systems

4.2.6.8. Additional Mandatory Requirement: Current-State Assessment

The Vendor shall:

4.2.6.8.1. Conduct a comprehensive assessment of the current IAM ecosystem, including:

4.2.6.8.1.1. Identity data flows

4.2.6.8.1.2. Provisioning logic

4.2.6.8.1.3. Existing inconsistencies and failure patterns

4.2.6.8.2. Deliver documented findings to inform final SoA and integration design

4.3. In Scope Target Systems

4.3.1. The Vendor shall design, implement, and validate provisioning, deprovisioning, and reconciliation of integrations between SailPoint and the following target systems.

4.3.2. The Vendor is responsible for ensuring that access provisioning is accurate, consistent, auditable, and reversible across all target systems.

4.3.3. General Requirements for All Target System Integrations

For each target system listed below, the Vendor shall:

4.3.3.1. Provisioning and Deprovisioning

4.3.3.1.1.1. Implement automated provisioning and deprovisioning aligned with identity lifecycle events

4.3.3.1.2. Ensure:
4.3.3.1.2.1. Timely account creation, modification, and removal
4.3.3.1.2.2. Consistent enforcement of access policies and roles
4.3.3.1.3. Support:
4.3.3.1.3.1. Birthright access
4.3.3.1.3.2. Role-based access
4.3.3.1.3.3. Request-based access (if applicable)

4.3.3.2. Reconciliation and Data Integrity (CRITICAL)
4.3.3.2.1. Implement automated reconciliation processes to:
4.3.3.2.1.1. Verify that accounts marked as provisioned in SailPoint exist and are correctly configured in the target system
4.3.3.2.1.2. Detect missing, orphaned, or misconfigured accounts
4.3.3.2.2. Provide mechanisms to:
4.3.3.2.2.1. Remediate discrepancies automatically or via workflow
4.3.3.2.2.2. Prevent repeated provisioning failures

4.3.3.3. Error Handling and Resiliency
4.3.3.3.1. Implement:
4.3.3.3.1.1. Robust error handling and retry logic
4.3.3.3.1.2. Idempotent provisioning operations
4.3.3.3.2. Ensure failed provisioning events are:
4.3.3.3.2.1. Logged
4.3.3.3.2.2. Visible
4.3.3.3.2.3. Actionable

4.3.3.4. Observability and Auditability
4.3.3.4.1. Provide end-to-end traceability of provisioning actions, including:
4.3.3.4.1.1. Who/what triggered the action
4.3.3.4.1.2. When it occurred
4.3.3.4.1.3. Final outcome in the target system
4.3.3.4.2. Ensure all actions are auditable for compliance purposes

4.3.3.5. Performance and Scale
4.3.3.5.1. Support high-volume provisioning events, including:
4.3.3.5.1.1. Semester onboarding
4.3.3.5.1.2. Mass hires or terminations
4.3.3.5.2. Ensure no degradation in performance across target systems

4.3.3.6. Access Model Alignment
4.3.3.6.1. Define and document:
4.3.3.6.1.1. Account structures (1:1 vs shared vs service accounts)
4.3.3.6.1.2. Role/group mapping strategy
4.3.3.6.2. Align provisioning with:
4.3.3.6.2.1. SailPoint roles
4.3.3.6.2.2. Target system entitlements (e.g., AD groups, Google roles)

4.3.3.7. Integration Method Requirements
4.3.3.7.1. Clearly define:
4.3.3.7.1.1. Connector type (API, LDAP, SCIM, database, etc.)
4.3.3.7.1.2. Use of middleware (e.g., MuleSoft) vs direct integration
4.3.3.7.2. Ensure:

4.3.3.7.2.1. No hidden provisioning logic exists outside SailPoint without documentation and approval

4.3.4. Directory and Authentication Systems (High-Risk Area)

4.3.4.1. Applies to:

4.3.4.1.1. Campus Active Directory
4.3.4.1.2. Private LDAP
4.3.4.1.3. Public LDAP
4.3.4.1.4. Sentinel LDAP
4.3.4.1.5. Community ID LDAP
4.3.4.1.6. MIT Kerberos

The Vendor shall:

4.3.4.2. Define a directory strategy, including:

4.3.4.2.1. Purpose of each directory (authoritative vs consumer vs authentication)
4.3.4.2.2. Account placement rules (which identities go where and why)

4.3.4.3. Ensure:

4.3.4.3.1. Consistent identity representation across all directories
4.3.4.3.2. Synchronization between directories where required

4.3.4.4. Implement:

4.3.4.4.1. Reconciliation processes to detect drift between directories
4.3.4.4.2. Controls to prevent:

4.3.4.4.2.1. Accounts existing in one directory but not another (unless explicitly intended)
4.3.4.4.2.2. Duplicate or conflicting accounts

4.3.5. Identity Providers and Cloud Platforms

4.3.5.1. Applies to:

4.3.5.1.1. Okta
4.3.5.1.2. Azure AD / Microsoft 365
4.3.5.1.3. Google Workspace

The Vendor shall:

4.3.5.1.4. Integrate SailPoint with identity providers to:

4.3.5.1.4.1. Provision accounts
4.3.5.1.4.2. Assign and revoke access (groups, roles, licenses)

4.3.5.1.5. Define:

4.3.5.1.5.1. Relationship between SailPoint and IdP (source of truth vs downstream system)

4.3.5.1.6. Ensure:

4.3.5.1.6.1. Consistent identity and access state across all platforms

4.3.5.1.7. Implement:

4.3.5.1.7.1. License assignment and reclamation logic (where applicable)

4.3.6. Enterprise and Administrative Systems

4.3.6.1. Applies to:

4.3.6.1.1. TeamDynamix
4.3.6.1.2. PlanOn

4.3.6.1.3. Transact
4.3.6.1.4. TracyTime Systems (UltraBadge)

The Vendor shall:

4.3.6.2. Define:
4.3.6.2.1. Access models for each system
4.3.6.2.2. Integration capabilities (API, file-based, manual fallback)
4.3.6.3. Ensure:
4.3.6.3.1. Provisioning aligns with business roles and lifecycle events
4.3.6.4. Document:
4.3.6.4.1. Any limitations or required custom integrations

4.3.7. Academic and Communication Systems

4.3.7.1. Applies to:
4.3.7.1.1. Desire2Learn (D2L)
4.3.7.1.2. ListServ
4.3.7.1.3. FOLIO

The Vendor shall:

4.3.7.2. Implement provisioning aligned with:
4.3.7.2.1. Enrollment status
4.3.7.2.2. Course participation
4.3.7.2.3. Academic roles
4.3.7.3. Ensure:
4.3.7.3.1. Timely provisioning and deprovisioning aligned with academic cycles

4.3.8. Database Systems

4.3.8.1. Applies to:
4.3.8.1.1. SQL, MySQL, Oracle Databases

The Vendor shall:

4.3.8.2. Define:
4.3.8.2.1. Whether databases are:
4.3.8.2.1.1. Direct provisioning targets
4.3.8.2.1.2. Or sources for downstream applications
4.3.8.3. Implement:
4.3.8.3.1. Secure credential and access management practices
4.3.8.4. Avoid:
4.3.8.4.1. Direct identity provisioning where not appropriate (unless explicitly required)

4.3.9. Mandatory Requirement: Provisioning Validation

The Vendor shall:

4.3.9.1. Demonstrate that provisioning actions result in actual, verifiable changes in each target system
4.3.9.2. Provide:
4.3.9.2.1. Validation reports comparing SailPoint state vs target system state
4.3.9.3. Ensure:

4.3.9.3.1. No reliance on “assumed success” of provisioning events

4.3.10. Mandatory Requirement: Legacy Integration Rationalization

The Vendor shall:

4.3.10.1. Identify any existing provisioning logic implemented in:
- 4.3.10.1.1. Scripts
- 4.3.10.1.2. Middleware (e.g., MuleSoft)
- 4.3.10.1.3. Legacy systems

4.3.10.2. Define how each integration will be:
- 4.3.10.2.1. Migrated to SailPoint
- 4.3.10.2.2. Simplified
- 4.3.10.2.3. Or decommissioned

4.3.10.3. Ensure:
- 4.3.10.3.1. No duplicate provisioning paths exist post-implementation

4.4. In Scope Sources/Targets for Legacy/Historic Import

4.4.1. The Vendor shall design and execute a comprehensive legacy data migration and rationalization strategy for the following systems:
- 4.4.1.1. SailPoint IIQ
- 4.4.1.2. Sentinel/D6501
- 4.4.1.3. Creator and Creator 2
- 4.4.1.4. D20
- 4.4.1.5. ACORNS

4.4.2. The Vendor is responsible for ensuring that all relevant identity, account, and access data is accurately migrated, reconciled, and aligned with the target SailPoint solution design, without propagating legacy inconsistencies or redundant logic.

4.4.3. General Migration Requirements

The Vendor shall:

4.4.3.1. Data Discovery and Analysis
- 4.4.3.1.1. Perform a detailed analysis of each legacy system, including:
  - 4.4.3.1.1.1. Identity data structures
  - 4.4.3.1.1.2. Account and entitlement models
  - 4.4.3.1.1.3. Embedded business logic (explicit and implicit)
- 4.4.3.1.2. Identify:
  - 4.4.3.1.2.1. Data quality issues
  - 4.4.3.1.2.2. Duplicate or conflicting identities
  - 4.4.3.1.2.3. Orphaned accounts and entitlements

4.4.3.2. Data Mapping and Transformation
- 4.4.3.2.1. Define and document:
  - 4.4.3.2.1.1. Field-level data mappings from legacy systems to SailPoint
  - 4.4.3.2.1.2. Transformation rules for:
    - 4.4.3.2.1.2.1. Identity attributes
    - 4.4.3.2.1.2.2. Account attributes
    - 4.4.3.2.1.2.3. Entitlements and roles
- 4.4.3.2.2. Align all mappings with:

4.4.3.2.2.1. Defined SoA model (Section 4.2)
4.4.3.2.2.2. Target access model (roles, policies, entitlements)

4.4.3.3. Data Cleansing and Rationalization (CRITICAL)

4.4.3.3.1. Cleanse legacy data prior to migration
4.4.3.3.2. Eliminate:
4.4.3.3.2.1. Duplicate identities
4.4.3.3.2.2. Obsolete accounts
4.4.3.3.2.3. Invalid or unused entitlements
4.4.3.3.3. Normalize identity data to support:
4.4.3.3.3.1. Accurate correlation across systems
4.4.3.3.3.2. Consistent lifecycle management

4.4.3.4. Identity Correlation and Consolidation

4.4.3.4.1. Reconcile identities across all legacy systems to:
4.4.3.4.1.1. Establish a single authoritative identity per individual
4.4.3.4.2. Handle:
4.4.3.4.2.1. Conflicting identifiers
4.4.3.4.2.2. Partial identity records
4.4.3.4.2.3. Cross-system duplicates

4.4.3.5. Migration Execution

4.4.3.5.1. Define and execute a phased migration approach, including:
4.4.3.5.1.1. Data extraction
4.4.3.5.1.2. Transformation
4.4.3.5.1.3. Validation
4.4.3.5.1.4. Load into SailPoint
4.4.3.5.2. Ensure migration processes are:
4.4.3.5.2.1. Repeatable
4.4.3.5.2.2. Auditable
4.4.3.5.2.3. Reversible (rollback capability)

4.4.3.6. Validation and Reconciliation

4.4.3.6.1. Validate that migrated data:
4.4.3.6.1.1. Accurately reflects intended identity and access states
4.4.3.6.1.2. Aligns with current authoritative sources (SoAs)
4.4.3.6.2. Perform post-migration reconciliation to:
4.4.3.6.2.1. Detect discrepancies
4.4.3.6.2.2. Confirm completeness and accuracy

4.4.4. Legacy System-Specific Requirements

The Vendor shall:

4.4.4.1. SailPoint IIQ
4.4.4.1.1. Assess existing configurations, including:
4.4.4.1.1.1. Roles
4.4.4.1.1.2. Policies
4.4.4.1.1.3. Workflows
4.4.4.1.1.4. Integrations
4.4.4.2. Define:
4.4.4.2.1. What will be:

4.4.4.2.1.1. Migrated
4.4.4.2.1.2. Redesigned
4.4.4.2.1.3. Retired

4.4.4.3. Avoid direct “lift-and-shift” of legacy configurations without validation and optimization
4.4.4.4. Sentinel / D6501
4.4.4.5. Creator and Creator 2
4.4.4.6. D20
4.4.4.7. ACORNS
4.4.4.8. For each system, the Vendor shall:
4.4.4.8.1. Identify:
4.4.4.8.1.1. All identity-related data and provisioning logic
4.4.4.8.1.2. Dependencies on other systems
4.4.4.8.2. Document current functionality and business purpose
4.4.4.8.3. Define how each function will be:
4.4.4.8.3.1. Replaced by SailPoint
4.4.4.8.3.2. Integrated temporarily
4.4.4.8.3.3. Or decommissioned
4.4.4.8.4. Extract relevant identity, account, and entitlement data
4.4.4.8.5. Ensure no critical identity logic is lost or unintentionally duplicated
4.4.4.9. Mandatory Requirement: Legacy Logic Identification and Elimination

The Vendor shall:

4.4.4.9.1. Identify all implicit and explicit identity-related logic embedded in legacy systems, including:
4.4.4.9.1.1. Provisioning rules
4.4.4.9.1.2. Access assignment logic
4.4.4.9.1.3. Data transformation rules
4.4.4.9.2. Ensure that:
4.4.4.9.2.1. Required logic is re-implemented in SailPoint in a controlled and documented manner
4.4.4.9.2.2. Unnecessary or redundant logic is eliminated
4.4.4.10. Mandatory Requirement: Decommissioning Strategy

The Vendor shall:

4.4.4.10.1. Provide a detailed decommissioning plan for each legacy system, including:
4.4.4.10.1.1. Timeline
4.4.4.10.1.2. Dependencies
4.4.4.10.1.3. Risk mitigation steps
4.4.4.10.2. Ensure no continued reliance on legacy systems for identity or access decisions post-implementation
4.4.4.11. Mandatory Requirement: Data Retention and Audit Compliance

The Vendor shall:

4.4.4.11.1.1. Ensure that historical data required for:

4.4.4.11.1.2. Audit
4.4.4.11.1.3. Compliance
4.4.4.11.1.4. Reporting is preserved and accessible
4.4.4.11.2. Define:
4.4.4.11.2.1. What data is migrated vs archived
4.4.4.11.2.2. Where and how archived data will be stored and accessed

4.5. Identity Data Management and Identity Governance & Administration Implementation Services

4.5.1. The Vendor shall design, implement, and validate a scalable, data-driven Identity Governance and Administration (IGA) solution using SailPoint that replaces legacy IAM capabilities and establishes a single, authoritative, and governed identity model for MSU.

4.5.2. All deliverables must be measurable, testable, and approved by MSU.

4.5.3. Dependency Discovery and Legacy Decomposition
The Vendor shall:

4.5.3.1. Conduct a comprehensive dependency analysis of all IAM-related systems, including:
4.5.3.1.1. Homegrown applications
4.5.3.1.2. Middleware (e.g., MuleSoft, DataStage)
4.5.3.1.3. Direct and indirect provisioning logic

4.5.3.2. Work collaboratively with:
4.5.3.2.1. IDM Team
4.5.3.2.2. ADS
4.5.3.2.3. Access Management
4.5.3.2.4. Identity Office

4.5.3.3. Required Deliverables:
4.5.3.3.1. Documented dependency map of all IAM components
4.5.3.3.2. Identification of:
4.5.3.3.2.1. Hidden or undocumented identity logic
4.5.3.3.2.2. Redundant or conflicting processes
4.5.3.3.3. A sequenced replacement roadmap, including:
4.5.3.3.3.1. Order of system decommissioning
4.5.3.3.3.2. Risk mitigation strategies
4.5.3.3.3.3. Business impact analysis

4.5.3.4. Critical Requirement:
4.5.3.4.1. The Vendor shall ensure that all identity-related logic currently embedded in legacy systems is either:
4.5.3.4.1.1. Re-implemented in SailPoint in a controlled manner, or
4.5.3.4.1.2. Explicitly retired

4.5.4. Identity Hub Implementation (Core Identity Layer)

4.5.4.1. The Vendor shall design and implement an Identity Hub (identity registry and abstraction layer) that:
4.5.4.1.1. Serves as the central identity aggregation and correlation layer
4.5.4.1.2. Decouples upstream systems (SoAs) from downstream provisioning systems

4.5.4.2. Core Capabilities

The Vendor shall configure the Identity Hub to:

4.5.4.2.1. Data Ingestion and Processing

4.5.4.2.1.1. Ingest identity data from all in-scope SoAs and legacy systems

4.5.4.2.1.2. Support near real-time processing and event-driven updates

4.5.4.2.1.3. Normalize identity data across sources

4.5.4.2.2. Identity Correlation and Matching

4.5.4.2.2.1. Implement:

4.5.4.2.2.1.1. Hard, soft, and fuzzy matching rules

4.5.4.2.2.1.2. Match confidence scoring

4.5.4.2.2.2. Configure:

4.5.4.2.2.2.1. Match resolution workflows and queues

4.5.4.2.2.2.2. Automated and manual resolution actions

4.5.4.2.3. Identity Data Quality and Hygiene

4.5.4.2.3.1. Define and enforce:

4.5.4.2.3.1.1. Data cleansing rules

4.5.4.2.3.1.2. Standardization and transformation logic

4.5.4.2.4. Identity Consolidation (CRITICAL)

4.5.4.2.4.1. Ensure each individual is represented by a single authoritative identity

4.5.4.2.4.2. Handle:

4.5.4.2.4.2.1. Duplicate identities

4.5.4.2.4.2.2. Partial records

4.5.4.2.4.2.3. Cross-system inconsistencies

4.5.4.2.5. Identifier Management

4.5.4.2.5.1. Define and implement:

4.5.4.2.5.1.1. Unique identifier creation and lifecycle

4.5.4.2.5.1.2. Identifier mapping across systems

4.5.4.2.5.2. Support:

4.5.4.2.5.2.1. Pre-hire identity creation (e.g., SSN-based)

4.5.4.2.5.2.2. Transition to primary identifiers (e.g., EmplID)

4.5.4.2.6. Data Flow and Integration

4.5.4.2.6.1. Configure:

4.5.4.2.6.1.1. Near real-time data flows and triggers

4.5.4.2.6.1.2. Schema and integration points

4.5.4.2.6.1.3. Implement SoA writeback where required

4.5.4.2.7. Identity Proofing and Verification

4.5.4.2.7.1. Define and enforce identity proofing standards

4.5.4.2.7.2. Support identity verification workflows

4.5.4.2.8. Required Validation:

4.5.4.2.8.1. The Vendor shall demonstrate that:

4.5.4.2.8.1.1. Identity data is accurately correlated across all sources
4.5.4.2.8.1.2. No duplicate or orphaned identities exist post-implementation

4.5.5. Real-Time Identity Lifecycle and Baseline Access

4.5.5.1. The Vendor shall implement end-to-end identity lifecycle management, including:
4.5.5.1.1. Lifecycle Automation
4.5.5.1.1.1. Joiner / Mover / Leaver processing
4.5.5.1.1.2. Multi-affiliation identity handling (e.g., student + employee)
4.5.5.1.2. Baseline Access Model
4.5.5.1.2.1. Define and implement:
4.5.5.1.2.1.1. Baseline (birthright) roles
4.5.5.1.2.1.2. Role-to-entitlement mappings
4.5.5.1.2.2. Ensure:
4.5.5.1.2.2.1. Roles are governable, auditable, and maintainable
4.5.5.1.2.3. Prevent:
4.5.5.1.2.3.1. Role explosion
4.5.5.1.2.3.2. Direct entitlement sprawl
4.5.5.1.3. Provisioning Modernization
4.5.5.1.3.1. Replace all existing provisioning/deprovisioning processes
4.5.5.1.3.2. Ensure:
4.5.5.1.3.2.1. Real-time or near real-time provisioning where required
4.5.5.1.3.2.2. Consistent enforcement across all target systems
4.5.5.1.4. Identity Services
4.5.5.1.4.1. Implement:
4.5.5.1.4.1.1. Account claim processes
4.5.5.1.4.1.2. Password management integration
4.5.5.1.4.1.3. Identity administration capabilities
4.5.5.1.5. Compliance and Policy Enforcement
4.5.5.1.5.1. Configure:
4.5.5.1.5.1.1. Audit policies
4.5.5.1.5.1.2. Reporting and monitoring
4.5.5.1.5.2. Ensure compliance with:
4.5.5.1.5.2.1. GDPR (e.g., right to know, right to be forgotten)
4.5.5.1.5.2.2. FERPA, HIPAA, and other applicable regulations

4.5.6. Identity Administration Capabilities

4.5.6.1. The Vendor shall configure administrative capabilities including:
4.5.6.1.1. Identity lookup and search
4.5.6.1.2. Emergency termination workflows
4.5.6.1.3. Provisioning/deprovisioning overrides and grace periods

4.5.6.1.4. Attribute management
4.5.6.1.5. Account lock/unlock and enable/disable
4.5.6.1.6. Legal hold management
4.5.6.1.7. Administrative management of DEI attributes

4.5.7. Access Request, Workflow, and Fulfillment

The Vendor shall:

4.5.7.1. Implement SailPoint access request capabilities, including:
4.5.7.1.1. Workflow-driven approvals
4.5.7.1.2. Delegation models
4.5.7.1.3. Automated fulfillment
4.5.7.2. Migrate request workflows from TeamDynamix
4.5.7.3. Workflow Requirements
4.5.7.3.1. Define and implement:
4.5.7.3.1.1. Approval chains (data owners, supervisors, system owners)
4.5.7.3.1.2. Delegation of request management to business units
4.5.7.3.1.3. Provide catalog of requestable access
4.5.7.4. Fulfillment Automation
4.5.7.4.1.1. Integrate with target systems to automate fulfillment of common access requests
4.5.7.4.1.2. Ensure no manual provisioning steps remain without justification

4.5.8. Application Authorization and Entitlement Governance

The Vendor shall:

4.5.8.1. Inventory all applications with internal authorization models
4.5.8.2. Map application roles → SailPoint entitlements
4.5.8.3. Configure integration patterns (API, DB, file, etc.)
4.5.8.4. Governance Controls
4.5.8.4.1. Implement:
4.5.8.4.1.1. Certification campaigns
4.5.8.4.1.2. Separation of Duties (SoD) policies
4.5.8.4.2. Configure attestation requirements for:
4.5.8.4.2.1.1. Privileged access
4.5.8.4.2.1.2. Regulatory compliance (FERPA, HIPAA, etc.)
4.5.8.5. Policy Enforcement
4.5.8.5.1. Ensure access is:
4.5.8.5.1.1. Tied to training and compliance requirements
4.5.8.5.1.2. Support periodic review and revocation

4.5.9. Third-Party / Non-Employee Identity Management

The Vendor shall:

4.5.9.1. Lifecycle Management
4.5.9.1.1. Design and implement lifecycle management for:
4.5.9.1.1.1. Guests
4.5.9.1.1.2. Affiliates
4.5.9.1.1.3. Researchers

4.5.9.2. Identity Requirements
- 4.5.9.2.1. All non-employee identities must:
  - 4.5.9.2.1.1. Be managed within the Identity Hub
  - 4.5.9.2.1.2. Be uniquely identifiable and correlated across all systems
  - 4.5.9.2.1.3. Support transition between:
    - 4.5.9.2.1.3.1. Non-employee → employee (and vice versa)

4.5.9.3. Access and Lifecycle Controls
- 4.5.9.3.1. Configure:
  - 4.5.9.3.1.1. Baseline roles and entitlements
  - 4.5.9.3.1.2. Renewal processes and expiration policies
  - 4.5.9.3.1.3. Notifications and approvals
- 4.5.9.3.2. Ensure automated provisioning and deprovisioning

4.5.9.4. Critical Requirement: Reconciliation
- 4.5.9.4.1. The Vendor shall implement controls to ensure:
  - 4.5.9.4.1.1. Non-employee accounts (e.g., guest accounts) are:
- 4.5.9.4.2. Consistently provisioned across all target systems
  - 4.5.9.4.2.1. Regularly reconciled to detect and remediate discrepancies

4.5.9.5. Mandatory Requirement: Definition of Done
- 4.5.9.5.1. Deliverables in this section will not be considered complete until:
  - 4.5.9.5.1.1. Identity data is accurately correlated across all sources
  - 4.5.9.5.1.2. Provisioning is verified in all target systems
  - 4.5.9.5.1.3. No critical reconciliation gaps exist
  - 4.5.9.5.1.4. All lifecycle scenarios (including edge cases) are validated

5. Project Milestones

As part of the written proposal, provide a timeline. Below is a list of milestones MSU would like included in the proposal.

- Kickoff Meeting with Vendor 09-01-2026
- Requirements | Subject Matter Expert Meetings 11-30-2026
- Leadership Review 12-15-2026
- Begin TEST/QA Build of SailPoint 01-05-2027 through 06-30-2028
    - QA to PROD Go-Live Phases
        - IDM (see detailed apps in the earlier requirements)
        - Access Management
- Project Complete 06-30-2028

6. Travel

6.1. All travel shall be reimbursed at actual cost and shall be subject to MSU's Travel Reimbursement Policy set forth at https://travel.msu.edu/reimbursement/reimbursement-charts

6.2. All travel per this Agreement must be preapproved by the University

7. RFP Written Responses

7.1. As part of their written proposal, respondents should address the below items:

7.1.1. Project goals, timeline, and deliverables

7.1.1.1. Acknowledgement of review of the project goals, timeline, and deliverables

7.1.1.2. Respondent may propose a different approach to the goals and timeline. If proposing a different approach for MSU's consideration, the proposal should be detailed and provide sufficient information for MSU to compare to proposed goals, timeline, and deliverables

7.1.1.3. Respondent to provide outline and examples of final reports and deliverables

7.1.2. Detailed resumes and references for resources to be assigned to MSU.

7.1.2.1. There should be at least one executive level, and one mid-management reference for each relevant engagement. References shall include: Name, Phone and Email of contact.

7.1.3. Details of qualifications of your organization that especially qualifies you as consultant, or enables your organization, to render distinctive service for this Project

7.1.4. Details regarding consultant(s) roles and availability

7.1.4.1. 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.

7.1.4.2. University expects the selected respondent to commit the selected consultant (or team) to provide continuous service until the project is completed.

7.1.5. The University prefers a combination of on-site and off-site work. Provide details of your firm's availability for service and the breakdown of on-site/off-site work.

8. Required Documents for RFP Submission

8.1. Written Response per Paragraph 8
8.2. Respondent Information Sheet
8.3. Signed Pricing Proposal
8.4. Implementation and Training Plan
8.5. Master Service Agreement (if requesting redlines)

9. Virtual Respondent Interviews

9.1. As part of University's evaluation process, MSU reserves the right to require virtual interviews with a respondent to follow-up on respondents written proposal.
9.2. MSU shall, at its sole discretion, identify respondents it desires to interview and will coordinate a date and time for a virtual meeting.

10. Payment Terms

10.1. Invoice payment terms for the agreement resulting from this RFP shall be 2.75% 10, NET 30 from date of receipt of invoice.
10.1.1. Failure to accept these payment terms may result in a respondent being deemed non-responsive.

11. Invoicing

11.1. Invoice Submissions
11.1.1. Each invoice is to be billed on a separate sheet of paper
11.1.2. Each invoice must be billed within 30 days after the completion of the stated work
11.1.3. All invoices are to be emailed or mailed to MSU Accounts Payable. Do not mail or email invoices to Administration Building or MSU Client, they will not be paid and will delay receipt of payment
11.1.4. If invoicing for reimbursement of travel expenses, receipts for actual travel costs shall be provided as supporting documentation along with the invoice
11.1.5. More information on MSU invoice submission requirements can be found at: https://procurement.msu.edu/for-suppliers/policies-requirements/invoicing-payments
11.2. Invoice Requirements
11.2.1. Every invoice must show
11.2.1.1. Company Name
11.2.1.2. University Purchase Order Number
11.2.1.3. Itemized/Breakdown of costs being invoiced

MICHIGAN STATE UNIVERSITY

PRICING

In order to more accurately compare proposals, bidders shall return a pricing proposal per the below.

Failure to return a signed version of this form as a separate attachment may result in a bidder being disqualified.

In addition to this form, bidders are free to also include other pricing information they feel would be of interest to the University (i.e. options, pricing breakdown, etc.). Bidders may indicate a dollar value for each cost (including $0 / no charge) or that cost is "included" in other costs. Bidders should also ensure that licensing fees will not be charged until the scope of work for implementation services has been completed and the solution has gone live in the production environment.

One Time Fees (Required)	Total Cost USD
One time implementation fees:	
Training fees:	
Consulting fees:	

You must fill out the above Proposed Cost matrix to ensure that all submissions are unbiased.

You may present your pricing as you would normally within your bidding process in your format, showing all of the different costs for services and options you have; however, those prices must be on a separate page giving us the ability to separate them out individually.

The signature below confirms that this proposal is valid for 180 days after the due date.

Supplier
Signature: _____
Name:_____
Title: _____
Date: _____

MICHIGAN STATE UNIVERSITY

MASTER SERVICE AGREEMENT

(Attached as a separate document)

Please refer to Section 9 of the RFP Instructions when reviewing the Master Services Agreement terms and conditions.