Attachment A

to

RFP No. 4724

Mississippi Department of Transportation

Technical Requirements

ITS Project No. 49157

Employee Engagement Solution

[I. General 1](#_Toc207198482)

[A. How to Respond 1](#_Toc207198483)

[B. Procurement Goals and Objectives 1](#_Toc207198484)

[C. Statement of Understanding 2](#_Toc207198485)

[D. Hosting Environment 2](#_Toc207198486)

[E. Vendor Qualifications 5](#_Toc207198487)

[II. Functional/Technical Requirements 6](#_Toc207198488)

[A. User Management & Access Control 6](#_Toc207198489)

[B. Assessment & Survey Management 6](#_Toc207198490)

[C. Survey Distribution & Response Collection 7](#_Toc207198491)

[D. Results & Reporting Dashboards 7](#_Toc207198492)

[E. Insights & Recommendations 7](#_Toc207198493)

[F. Team Collaboration & Coaching Tools 7](#_Toc207198494)

[G. Content & Resource Management 8](#_Toc207198495)

[H. Integration & Data Sync 8](#_Toc207198496)

[I. AI Capabilities 8](#_Toc207198497)

[J. Workflow Automation & Notification 8](#_Toc207198498)

[K. Survey & Assessment Scheduling 9](#_Toc207198499)

[L. Analytics & Benchmarking 9](#_Toc207198500)

[M. Administrative Tools 9](#_Toc207198501)

[N. User Interface & Accessibility 9](#_Toc207198502)

[O. Training 9](#_Toc207198503)

[P. Maintenance/ Support 10](#_Toc207198504)

1. General
2. How to Respond
3. Beginning with Item 19, label and respond to each outline point in Attachment A as it is labeled.
4. The State is under the impression that Vendors have read and agree to all items in this RFP. Vendors should take exception to items to which they disagree.
5. The Vendor must respond with “WILL COMPLY” or “EXCEPTION” to each point in this section. In addition, many items in this RFP require detailed and specific responses to provide the requested information. Failure to provide the information requested will result in the Vendor receiving a lower score for that item or, at the State’s sole discretion, being subject to disqualification.
6. “WILL COMPLY” indicates that the Vendor can and will adhere to the requirement. This response specifies that a Vendor or vendor’s proposed solution must comply with a specific item or perform a certain task.
7. If the Vendor cannot respond with “WILL COMPLY,” then the Vendor must respond with “EXCEPTION.” (See Section V of RFP No. 4724, for additional instructions regarding Vendor exceptions.)
8. Where an outline point asks a question or requests information, the Vendor must respond with the specific answer or information requested.
9. In addition to the above, the Vendor must provide explicit details about how the proposal meets or exceeds each specification.
10. Procurement Goals and Objectives
11. The Mississippi Department of Transportation (MDOT) is committed to fostering a high-performing, inclusive, and responsive workplace culture. In support of this goal, MDOT is seeking a cloud-based Employee Engagement Application to enhance its ability to regularly and efficiently gather actionable insights from its workforce.
12. The objective is to implement a centralized, secure, and user-friendly digital platform that enables the agency to administer employee surveys and engagement initiatives. This solution will be used to assess employee satisfaction, identify workforce trends, support strategic decision-making, and promote continuous improvement in organizational effectiveness.
13. The application will play a critical role in MDOT's broader human resources and organizational development efforts by:
    * + Enabling real-time, anonymous feedback from employees across various divisions and districts;
      + Supporting the creation and deployment of surveys targeting topics such as communication, leadership effectiveness, training needs, and overall job satisfaction;
      + Providing analytical tools to interpret trends, measure engagement over time, and generate actionable reports for agency leadership; and
      + Facilitating communication and transparency by closing the feedback loop between employees and management.
14. Statement of Understanding
15. Throughout this document, references to this RFP will mean RFP No. 4724, including Attachment A and all accompanying exhibits and/or appendices.
16. Unless otherwise specified, references to “Customer” will mean the Mississippi Department of Transportation (MDOT) throughout this document.
17. Unless otherwise specified, throughout this document, references to “State” can be used interchangeably to represent the State of Mississippi, the Customer, and the State of Mississippi Department of Information Technology.
18. Unless otherwise specified, throughout this document, references to the proposed solution will represent the collective services, system, or solution(s) being sought by the State.
19. Vendors should expect to find the request for their cost proposal in Section VIII, Cost Information Submission form in RFP 4724, rather than in this Attachment A document.
    1. Vendors must propose tier pricing for the items listed in Section VIII, Cost Information Submission or any functional equivalents. Any cost not listed in this section that is required may result in the Vendor providing those products or services at no charge to the State or face disqualification. The State reserves the right to purchase all, a portion of, or none of these items.
20. For providing reference information, Vendors should expect to find Section IX Reference Forms in RFP No. 4724, rather than in this Attachment A document.
21. Vendors must agree to provide best practices, industry-standard tools, and methodologies. The Vendor acknowledges that the State will not accept proprietary formats.
22. ITS acknowledges that the specifications within this RFP are not exhaustive. Rather, they reflect the known requirements that must be met by the proposed system. Vendors must specify withing their RFP response what additional components may be needed and are proposed in order to complete each configuration.
23. Hosting Environment
24. Customer is seeking a government cloud-based solution. The cloud-hosted environment must be capable of supporting the Employee Engagement Solution application at maximum user capacity as well as maintaining the system’s database functions. Startup capacity is estimated to be 2,600 users. The solution must be scalable to accommodate additional users.
25. Data Ownership - The State shall own all right, title and interest in all data used by, resulting from, and collected using the services provided. The Vendor shall not access State User accounts, or State Data, except (i) in the course of data center operation related to this solution; (ii) response to service or technical issues; (iii) as required by the express terms of this service; or (iv) at State ’s written request.
26. Data Protection - Protection of personal privacy and sensitive data shall be an integral part of the business activities of the Vendor to ensure that there is no inappropriate or unauthorized use of State information at any time. To this end, the Vendor shall safeguard the confidentiality, integrity, and availability of State information and comply with the following conditions.
    1. All information obtained by the Vendor under this contract shall become and remain property of the State.
    2. At no time shall any data or processes which either belong to or are intended for the use of State or its officers, agents, or employees be copied, disclosed, or retained by the Vendor or any party related to the Vendor for subsequent use in any transaction that does not include the State.
27. Data Location - The Vendor shall not store or transfer State data outside of the United States. This includes backup data and Disaster Recovery locations. The Vendor will permit its personnel and contractors to access State data remotely only as required to provide technical support.
28. Encryption - The Vendor shall encrypt all non-public data in transit regardless of the transit mechanism.
    1. For engagements where the Vendor stores non-public data, the data shall be encrypted at rest. The key location and other key management details will be discussed and negotiated by both parties. Where encryption of data at rest is not possible, the Vendor must describe existing security measures that provide a similar level of protection. Additionally, when the Vendor cannot offer encryption at rest, it must maintain, for the duration of the contract, cyber security liability insurance coverage for any loss resulting from a data breach. The policy shall comply with the following requirements:
       1. The policy shall be issued by an insurance company acceptable to the State and valid for the entire term of the contract, inclusive of any term extension(s).
       2. The Vendor and the State shall reach agreement on the level of liability insurance coverage required.
       3. The policy shall include, but not be limited to, coverage for liabilities arising out of premises, operations, independent contractors, products, completed operations, and liability assumed under an insured contract.
       4. At a minimum, the policy shall include third party coverage for credit monitoring, notification costs to data breach victims, and regulatory penalties and fines.
       5. The policy shall apply separately to each insured against whom claim is made or suit is brought subject to the Vendor’s limit of liability.
       6. The policy shall include a provision requiring that the policy cannot be cancelled without thirty (30) days written notice.
       7. The Vendor shall be responsible for any deductible or self-insured retention contained in the insurance policy.
       8. The coverage under the policy shall be primary and not in excess to any other insurance carried by the Vendor.
       9. In the event the Vendor fails to keep in effect at all times the insurance coverage required by this provision, the State may, in addition to any other remedies it may have, terminate the contract upon the occurrence of such event, subject to the provisions of the contract.
29. Breach Notification and Recovery - Unauthorized access or disclosure of non-public data is considered to be a security breach. The Vendor will provide immediate notification and all communication shall be coordinated with the State. When the Vendor or their sub-contractors are liable for the loss, the Vendor shall bear all costs associated with the investigation, response and recovery from the breach including but not limited to credit monitoring services with a term of at least 3 years, mailing costs, website, and toll-free telephone call center services. The State shall not agree to any limitation on liability that relieves a Vendor from its own negligence or to the extent that it creates an obligation on the part of the State to hold a Vendor harmless.
30. Notification of Legal Requests - The Vendor shall contact the State upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require access to the data of the State. The Vendor shall not respond to subpoenas, service of process, and other legal requests related to the State without first notifying the State unless prohibited by law from providing such notice.
31. Termination and Suspension of Service - In the event of termination of the contract, the Vendor shall implement an orderly return of State data in CSV or XML or another mutually agreeable format. The Vendor shall guarantee the subsequent secure disposal of State data.
    1. Suspension of services: During any period of suspension of this Agreement, for whatever reason, the Vendor shall not take any action to intentionally erase any State data.
    2. Termination of any services or agreement in entirety: In the event of termination of any services or of the agreement in its entirety, the Vendor shall not take any action to intentionally erase any State data for a period of 90 days after the effective date of the termination. After such 90-day period, the Vendor shall have no obligation to maintain or provide any State data and shall thereafter, unless legally prohibited, dispose of all State data in its systems or otherwise in its possession or under its control as specified in 26.d below. Within this 90-day timeframe, Vendor will continue to secure and back up State data covered under the contract.
    3. Post-Termination Assistance: The State shall be entitled to any post-termination assistance generally made available with respect to the Services unless a unique data retrieval arrangement has been established as part of the Service Level Agreement.
    4. Secure Data Disposal: When requested by the State, the provider shall destroy all requested data in all of its forms, for example: disk, CD/DVD, backup tape, and paper. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST) approved methods. Certificates of destruction shall be provided to the State.
32. Background Checks - The Vendor warrants that it will not utilize any staff members, including sub-contractors, to fulfill the obligations of the contract who have been convicted of any crime of dishonesty. The Vendor shall promote and maintain an awareness of the importance of securing the State's information among the Vendor's employees and agents.
33. Security Logs and Reports - The Vendor shall allow the State access to system security logs that affect this engagement, its data, and/or processes. This includes the ability to request a report of the activities that a specific user or administrator accessed over a specified period of time as well as the ability for an agency customer to request reports of activities of a specific user associated with that agency. These mechanisms should be defined up front and be available for the entire length of the agreement with the Vendor.
34. Contract Audit - The Vendor shall allow the State to audit conformance including contract terms, system security and data centers as appropriate. The State may perform this audit or contract with a third party at its discretion at the State’s expense.
35. Sub-contractor Disclosure - The Vendor shall identify all of its strategic business partners related to services provided under this contract, including but not limited to, all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Vendor, who will be involved in any application development and/or operations.
36. Sub-contractor Compliance - The Vendor must ensure that any agent, including a Vendor or subcontractor, to whom the Vendor provides access agrees to the same restrictions and conditions that apply through this Agreement.
37. Processes and Procedures - The Vendor shall disclose its non-proprietary security processes and technical limitations to the State so that the State can determine if and how adequate protection and flexibility can be attained between the State and the Vendor. For example: virus checking and port sniffing — the State and the Vendor shall understand each other’s roles and responsibilities.
38. Operational Metrics - The Vendor and the State shall reach agreement on operational metrics and document said metrics in the Service Level Agreement. At a minimum the SLA shall include:
    1. Advance notice and change control for major upgrades and system changes
    2. System availability/uptime guarantee/agreed-upon maintenance downtime
    3. Recovery Time Objective/Recovery Point Objective
    4. Security Vulnerability Scanning
39. Vendor Qualifications
40. Vendor must be capable of and have previous experience in developing and implementing Employee Engagement solutions of similar size and scope. At least two vendor references submitted in Section IX of RFP No. 4724 must substantiate this experience.
41. Vendors must have provided such solutions for at least three years.
42. The vendor must provide an introduction and general description of its company's background and years in business providing such services.
43. The vendor must specify the location of the organization's principal office and the number of executive and professional personnel employed at this office.
44. The vendor must specify the organization's size in terms of the number of full-time employees, the number of contract personnel used at any one time, the number of offices and their locations, and its structure (for example, state, national, or international organization).
45. The vendor must disclose any company restructurings, mergers, and acquisitions over the past three (3) years and any planned future restructurings or mergers.
46. Vendor headquarters must be located in the United States and provide U.S.-based customer support.
47. Functional/Technical Requirements

In addition to the proper response required and described in Section I.A above, Vendor must provide explicit details about how the proposal meets or exceeds each specification. Failure to provide the information requested will result in the Vendor receiving a lower score for that item or, at the State’s sole discretion, being subject to disqualification.

1. User Management & Access Control
2. The Vendor will be responsible for implementing and configuring the proposed solution. The comprehensive solution proposed by the Vendor must address the general and functional requirements outlined in this RFP, including all applicable State and Federal requirements.
3. The system must provide the ability to create, edit, and deactivate user accounts.
4. The system must allow role-based access control for different user types (e.g., Admin, Manager, Employee).
5. The application must support at least one of the following authentication methods: (1) Direct integration with Microsoft Active Directory using LDAP/LDAPS for authentication and user/group management, (2) Security Assertion Markup Language (SAML) 2.0 integration via Active Directory Federation Services (ADFS), or (3) Modern OAuth 2.0/OpenID Connect implementation supporting standard authorization flows with major identity providers. The solution must support Single Sign-On (SSO) capabilities and integrate with the organization's existing identity management infrastructure. The vendor must specify which of the above authentication method(s) their solution supports and provide detailed documentation on the implementation approach.
6. The system must allow access to employee data to be configured based on organizational hierarchy (e.g., Division Directors access only their division) and role-based exceptions (e.g., Executive or HR staff with agency-wide access), ensuring appropriate visibility across the organization.
7. The system must allow administrators to modify permissions for existing user roles and create new custom user roles to support flexible access control.
8. Assessment & Survey Management
9. The system must provide a library of standard assessments and surveys.
10. Survey Distribution & Response Collection
11. The system must provide the ability to distribute surveys via email, direct links, and mobile interfaces.
12. The system must allow scheduling of automated survey reminders.
13. The system must allow, track, and display real-time response rates.
14. The system must support anonymous and confidential survey responses.
15. The system must allow administrators to distribute surveys to targeted employee groups, such as individuals, teams, departments, job titles, or project-based teams.
16. Results & Reporting Dashboards
17. The system must provide real-time dashboards for visualizing survey results.
18. The system must allow filtering of results by team, department, role, or location.
19. The system must support exporting reports in formats such as PDF, Excel, and CSV.
20. The system must display historical trends and comparisons across survey cycles.
21. The system must allow users to drill down from high-level dashboard displays into more detailed analysis and data views for deeper insights.
22. The system must provide dashboards that incorporate employee strengths data, allowing managers and teams to view individual and collective strengths to support better team planning, coaching, and collaboration.
23. The system must provide reporting tools that include heat maps to visually display engagement scores, strengths data, or survey results across teams, departments, or other organizational units.
24. Insights & Recommendations
25. The system must generate personalized feedback reports based on assessment results.
26. The system must provide AI-driven insights and predictive analytics on engagement and performance trends.
27. The system must provide actionable recommendations for managers based on survey results.
28. The system must use natural language processing (NLP) to perform sentiment analysis on open-text survey responses.
29. The system must provide strategic recommendations for assigning employees to roles or teams based on their strengths and development profiles.
30. The system must provide insights into missing or underrepresented strengths within teams or departments to help identify potential gaps and guide development or hiring decisions.
31. Team Collaboration & Coaching Tools
32. The system must provide shared dashboards for teams to view collective strengths and engagement data.
33. The system must include built-in coaching tools and feedback modules.
34. The system must provide managers with tailored learning resources and coaching guides.
35. The system must provide the ability for employees to set goals.
36. The system must support succession planning by incorporating objective talent assessments, readiness-based development paths, and continuous feedback mechanisms to identify and prepare employees for future leadership roles.
37. Content & Resource Management
38. The system must allow tagging and categorization of content for easy discovery.
39. The system must recommend resources to users based on their assessment results and engagement scores.
40. The system must include training and development courses that are based on real data from large groups of employees over time.
41. The system must provide personalized development paths/plans that guide employees through structured learning experiences based on their strengths, roles, or engagement levels.
42. Integration & Data Sync
43. The system must integrate with MDOT’s Human Resource Management System (HRMS), a custom in-house solution.
    1. The system must be able to leverage active employee records and organizational assignments from HRMS, so the system can reflect current staff and reporting structure.
    2. The system must have the ability to upload or transfer these records on a set period basis, such as through an automated data feed.
44. The system must provide APIs for importing and exporting user and survey data.
45. The system must support real-time data synchronization.
46. The system must support uploads from spreadsheets.
47. The system must support exports of data.
48. AI Capabilities
49. The system must provide predictive analytics to identify potential risks such as disengagement or turnover.
50. The system must offer a chatbot assistant for navigating results and receiving feedback.
51. The system must retain memory of prior user interactions to provide contextually relevant responses and dynamically adjust future conversations.
52. Workflow Automation & Notification
53. The system must allow configuration of automated workflows based on survey results.
54. The system must send notifications for upcoming surveys, overdue actions, and new insights.
55. Survey & Assessment Scheduling
56. The system must provide scheduling options for recurring surveys such as annual, quarterly, or pulse.
57. Analytics & Benchmarking
58. The system must provide analytics tools for tracking engagement and performance over time.
59. The system must allow benchmarking of results against industry standards or peer organizations.
60. The system must allow benchmarking of results by:
    1. high performing units
    2. geographic location
    3. job classification/role type
    4. organizational history
    5. employee tenure
    6. organizational level
    7. employee engagement segments
61. The system must leverage vendor-provided benchmarking datasets derived from large, diverse, and validated sources to allow comparisons
62. The system must support custom Key Performance Indicator tracking and visualizations.
63. Administrative Tools
64. The system must provide audit logs and activity tracking for administrative actions.
65. The system must support data anonymization and privacy tools for compliance purposes.
66. User Interface & Accessibility
67. The system must be accessible to employees from the public internet without requiring a VPN connection.
68. The system must provide a responsive mobile-friendly web interface accessible from modern smartphones and tablets.
69. The system must provide a native mobile application for iOS and Android platforms for improved accessibility and usability.
70. Training
71. The awarded Vendor must provide training and knowledge transfer to approximately ten (10) MDOT system administrators and designated power users to ensure the consistent and optimum operation of the proposed solution. Vendor must address how training will be performed and if there are any limitations.
72. At time of installation, the awarded Vendor must provide all documentation and technical manuals needed for the proposed solution.
73. Maintenance/ Support
74. Vendor must provide availability for system support, at minimum, from 8:00 AM – 5:00 PM Central Time, Monday through Friday.