Attachment A

to

RFP No. 4588

Mississippi Department of
Transportation

Technical Specifications

ITS Project No. 47946

TRAFFIC SIGNAL ANALYSIS SYSTEM

TABLE OF CONTENTS

TABLE OF CONTENTS

ATTACHMENT A

I. General

A. How to Respond

1. Beginning with Item 23, label and respond to each outline point in Attachment A as it is labeled.

2. 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.

3. 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.

4. "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.

5. If the Vendor cannot respond with "WILL COMPLY," then the Vendor must respond with "EXCEPTION." (See Section V of RFP No. 4588, for additional instructions regarding Vendor exceptions.)

6. Where an outline point asks a question or requests information, the Vendor must respond with the specific answer or information requested.

7. In addition to the above, the Vendor must provide explicit details about how the proposal meets or exceeds each specification.

B. Overview and Background

8. The Mississippi Department of Transportation (MDOT) seeks proposals from qualified vendors to provide a hosted traffic signal analysis solution. This solution will aid in the monitoring, analysis, and optimization of traffic signal performance across the state.

C. Procurement Goals and Objectives

9. The traffic signal analysis solution selected by this RFP will allow the MDOT to enhance traffic flow, reduce congestion, and improve transportation efficiency.

10. The primary objectives of the traffic signal analysis solution are:

    a. To provide real-time monitoring and analytics of traffic signals.

    b. To offer data-driven insights for optimizing traffic signal timings.

    c. To support decision-making processes for traffic signal maintenance and upgrades.

    d. To improve overall traffic flow and reduce congestion.

    e. To provide a user-friendly interface for traffic signal management personnel.

D. Statement of Understanding

11. Throughout this document, references to this RFP will mean RFP No. 4588, including Attachment A to RFP No. 4588, and all accompanying exhibits and appendices.

12. Unless otherwise specified, references to Customer will mean the Mississippi Department of Transportation (MDOT) throughout this document.

13. Unless otherwise specified, throughout this document, references to the State can be used interchangeably to represent the State of Mississippi, the Customer, and the Mississippi Department of Information Technology Services.

14. 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.

15. Vendors should submit their cost proposals in Section VIII, Cost Information Submission form in RFP No. 4588, rather than in this Attachment A document.

16. Vendors should submit references in Section IX, Reference forms in RFP No. 4588, rather than in this Attachment A document.

17. The State expects the Vendor to be capable of implementing a solution that will enable the State to comply with the goals and requirements of the solicitation.

18. Vendors must agree to provide best practices, industry-standard tools, and methodologies. The Vendor acknowledges that the State will not accept proprietary formats.

19. The Vendor will be responsible for implementing 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.

20. The solution must be compatible with current Microsoft products available through the MDOT enterprise agreement. These include, but are not limited to, Microsoft Office 365, SharePoint, Azure, etc.

21. The Vendor must propose a single-release implementation designed to minimize interruptions to business operations. Any interruption to current operations must be scheduled to prevent loss of service and must be approved by MDOT.

E. Glossary of Terms

Abbreviation	Definition/Formal Name
Contractor	The organization to which a contract is awarded based on responses to this RFP.
CST	Central Standard Time
Incident	An incident is defined as an unplanned interruption to an IT service or a reduction in quality. Failure of a configuration item that has not yet affected service is also an incident, such as one of two mirrored disks failing. An incident is defined as an unplanned interruption to an IT service or a reduction in the quality of an IT service. Failure of a configuration item that has not yet affected service is also an incident, for example, one of two mirrored disks failing.
ITS	Mississippi Department of Information Technology Services
PM	Project Manager
RFP	Request for Proposal
AOG	Arrival on Green
LOS	Level of Service

F. Current Overview and Configuration

22. The hosted solution that is awarded as a result of this RFP will be the first Signal Analytics solution purchased by MDOT. There is no incumbent vendor-hosted application.

G. Hosting Environment

23. 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 the State’s written request.

24. 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:

    a. All information obtained by the Vendor under this contract shall become and remain property of the State.

    b. 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.

25. 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.

26. Encryption:

a. The Vendor shall encrypt all non-public data in transit regardless of the transit mechanism.

b. 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:

i. 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).

ii. The Vendor and the State shall reach agreement on the level of liability insurance coverage required.

iii. 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.

iv. At a minimum, the policy shall include third party coverage for credit monitoring, notification costs to data breach victims, and regulatory penalties and fines.

v. 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.

vi. The shall include a provision requiring that the policy cannot be cancelled without thirty (30) days written notice.

vii. The Vendor shall be responsible for any deductible or self-insured retention contained in the insurance policy.

viii. The coverage under the policy shall be primary and not in excess to any other insurance carried by the Vendor.

ix. 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.

27. 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.

28. 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.

29. 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.

    a. 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.

    b. 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 ninety (90) days after the effective date of the termination. After such ninety (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 item 29(d) (below). Within this ninety (90) day timeframe, Vendor will continue to secure and back up State data covered under the contract.

    c. 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.

    d. 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.

30. 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.

31. 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.

32. 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.

33. 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.

34. 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.

35. 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.

36. 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:

    a. Advance notice and change control for major upgrades and system changes.

    b. System availability/uptime guarantee/agreed-upon maintenance downtime.

    c. Recovery Time Objective/Recovery Point Objective.

    d. Security Vulnerability Scanning.

37. Customer is seeking a government cloud-based solution. The cloud-hosted environment must be capable of supporting the Traffic Signal Analysis System application at maximum user capacity as well as maintaining the system's database functions. Startup capacity is estimated to be approximately ten (10) users.

38. The solution must be scalable to accommodate additional users. If Vendor's solution is priced per user, Vendor must include a unit cost per license/user in Section VIII. Otherwise, additional users will be provided at no cost to the Customer.

39. For a Vendor-hosted solution, the Vendor must meet the following minimum requirements at their proposed cost.

    a. Vendors must provide Managed Services (government cloud), including migrating any on-premise services.

    b. Vendor must be a provider/reseller of hosting services (government cloud).

    c. Vendor must provide professional services such as monitoring, help desk support, security, etc.

d. Vendor must provide cloud hosting details and pricing in RFP, Section VIII, Cost Information Submission.

H. Qualifications

40. Vendor must be capable of and have previous experience in providing and implementing Traffic Signal Analysis solutions of similar size and scope. At least two vendor references submitted in Section IX of RFP No. 4588 must substantiate this experience.

41. Vendors must have provided such solutions for at least three (3) 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.

I. Vendor Implementation Team

47. The Vendor must demonstrate that all team members have the necessary experience for the development, configuration, implementation, testing, user training, maintenance, and support of the services required by this RFP. At a minimum, the Vendor's response should include team member roles, functional responsibilities, and experience with projects similar in size and scope to the services required by this RFP.

48. Vendor must identify the key staff members who will be responsible for executing the various aspects of the project, including, but not limited to, the Project Manager, Development Team, Business Analyst(s), and Traffic Signal Engineer.

49. For each participating key staff member, provide a summary of qualifications, years of experience, and length of employment with your company.

50. The Vendor must ensure that each team member assigned to this project can communicate clearly in English, both verbally and in written form.

II. Functional/Technical Requirements

A. Web Access

51. The solution must be web accessible to Customer staff and authorized external system users.

52. The solution must provide a user account management interface that allows for password complexity policies and self-service password reset. User management activity should be logged and available for reporting. Logging should, at a minimum, provide details such as timestamp, user, IP, and action performed.

53. The solution must offer web portal access to credentialed users for customer-defined functions. The portal must be intuitive and easy to navigate.

54. The solution must be browser-neutral and compatible with the current and two preceding versions of common browsers, including Chrome, Microsoft Edge, Firefox, Safari, and Microsoft Explorer 11.

55. The solution must be accessible to all end-user equipment, such as desktops, laptops, tablets, and other devices.

56. Vendors must specify any downloads, plug-ins, or additional software (add-ons) (e.g. Java, Flash, etc.) required to access the proposed solution.

57. For any necessary downloads, plug-ins, or add-ons, instructions for access and installation must be easily accessible to participants as a part of the proposed solution. The Vendor must describe how the additional software is presented to the user and detail the software's downloading and installation process. The Vendor should include a sample screenshot or sample instructions with the Vendor's response to this requirement.

58. For any necessary downloads, plug-ins, or add-ons, the Vendor must describe the process for educating users on installation and maintenance, including new users as they are added.

59. Section VIII, Cost Information, must include any costs associated with using and maintaining these downloads, plug-ins, or additional software.

B. Mobile Access

60. The solution must be accessible to iOS and Android mobile devices.

61. The solution must have offline functionality, which allows users to access, add, and edit data. When connectivity is restored, modifications must synchronize to the database.

62. The solution must include mobile applications for iOS and Android platforms for use in the field by Customer employees.

63. The solution must be compatible with Microsoft tablets, Android tablets, iOS devices, and related devices for the current and two immediately preceding versions.

64. The solution must incorporate mobile viewing for credentialed users.

65. The solution must accommodate system management functions on mobile platforms.

66. The solution must provide real-time data exchange with field devices having adequate access.

C. User Interface and User Experience

Describe in detail how the proposed system will:

67. Deliver an intuitive, user-friendly interface for traffic signal management and operations personnel.

68. Ensure the interface is accessible via web and mobile devices.

69. Provide customizable dashboards and visualization tools.

D. Interactive Functionality

70. The solution must provide a dashboard displaying signal performance measures. At a minimum, performance measures must include:

    a. Total Intersection Control Delay,
    b. Intersection Control Delay per Vehicle,
    c. Average Intersection Control Delay,
    d. Level of Service (LOS) of all Network Signals,
    e. Travel Time along Specified Corridors,
    f. Arrival on Green,
    g. Split Failure count/percentage,
    h. Off-Peak Split Failures,
    i. Hourly Turning Movement Counts by movement.

71. The solution must deliver performance measures to user email daily, weekly, and monthly.

72. The solution must provide a map view of all network signals displaying the performance measures at each.

73. The solution must give users access to the signal network allowing for the identification of potential issues.

E. Functional/Technical

74. Describe how the System will be implemented. Vendor must provide a detailed description overview that includes but is not limited to the items below:

    a. Design and deploy a hosted traffic signal analysis platform.
    b. Integrate the platform with existing traffic signal infrastructure.
    c. Ensure compatibility with a variety of traffic signal controllers and sensors.

75. Describe how the System will collect data and manage data. Vendor must provide a detailed description overview that includes but is not limited to the items below:

    a. Collect real-time data from traffic signals and related sensors.
    b. Store and manage data in a secure, scalable, and accessible manner.
    c. Ensure data integrity and accuracy.

76. Describe the Analytics and Reporting components of the System. Vendor must provide a detailed description overview that includes but is not limited to the items below:

    a. Provide real-time analytics on traffic signal performance.
    b. Generate detailed reports on traffic flow, signal timings, and congestion.
    c. Offer predictive analytics to anticipate and mitigate traffic issues.

77. Describe the Optimization Tools available in the System. Vendor must provide a detailed description overview that includes but is not limited to the items below:

    a. Develop and deploy tools for optimizing traffic signal timings.
    b. Allow for automated and manual adjustments based on data insights.
    c. Support simulation of different traffic scenarios and signal strategies.

F. Reports and Dashboards

78. The solution must offer pre-designed, standard reports related to best practices, whether they are specified by this RFP.

79. The solution must accommodate the creation and modification of standard reporting templates defined by the Customer.

80. The solution must accommodate user-defined reporting to create custom reports from all data elements for which the Customer requires tracking and reporting.

81. The user-defined reporting tool must be intuitive and easy for the user to comprehend.

82. The solution must provide the ability to save user-generated reports under user profiles.

83. The solution must allow authorized Customer staff to create their reports using an interface that does not require specialized knowledge of a third-party tool such as Crystal Reports.

84. The solution must allow Customer Staff to create and save customized reports and queries.

85. The solution must provide ad hoc reports of all users with system access, including the level of access and the date/time of last access.

86. The solution must be capable of exporting reports into file formats, including PDF, MS Excel, and MS Word.

87. The solution must be able to distribute reports through the workflow as email attachments.

88. The solution must provide dashboards that can be configured according to individual users' roles and preferences.

89. The solution must provide configurable dashboards on throughput performance measures and system activities such as those determined by Customers, etc.

90. The solution must provide configurable dashboards for users to manage open tasks.

91. The solution must provide dashboard views that provide pertinent information related to workloads and tasks to assist in visualizing and prioritizing work.

92. The solution must automatically generate reports on a configurable schedule and distribute them to selected users as determined by the Customer.

G. Notifications and Alerts

93. The solution must auto-generate emails or notifications based on conditions and thresholds set by the Customer.

94. The solution must provide email and correspondence templates for notification purposes.

95. The Vendor must detail how the solution provides task management functions that issue alerts for pending, due, or past-due tasks. This function should interface with the dashboard function to give users a visual representation of their tasks' status.

96. The Vendor must detail how the task logs assign daily tasks, task details, due dates, task status, and all other details pertinent to task management.

H. Search Function

97. The solution must offer best practice, full-featured, configurable data search functions that can be scheduled to run automatically and because of an individual request from an authorized user.

98. The solution must allow users to search by any indexable attribute required by the Customer.

99. The solution must be able to search on all data elements and have full keyword search capability.

100. The solution must be able to produce search results that represent the search term and subtle variations of it.

101. The solution must offer pre-defined searches common to traffic signal management activities.

102. Searches must be exportable or downloadable to common file formats such as Excel, PDF, XML, and CSV.

103. Users must be able to save frequently used searches for repeated use.

104. Users must be able to search by groupings or related matters such as outcomes, settlements, dispositions, etc.

105. Users must be able to search for items opened or closed during specific time frames.

106. Users must be able to search for upcoming events, deadlines, or other quantifiable parameters determined by the Customer.

107. The solution must provide global search functionality. At a minimum, this function should allow a user to search for any data or combination of data in the system. The results should be presented in a prioritized structure determined by the relevance to the search criteria. All connected or relatable data based on the search criteria should be presented within the prioritized results.

I. Document Management

108. The solution must offer a full-featured document management system (DMS) that accommodates generating, scanning, indexing, manipulating, editing, and storing paper and electronic documents.

109. The solution must be able to upload documents in formats commonly accepted by the Customer processes. Common Customer document formats are All Microsoft Office formats, .pdf, and all photo formats, including JPEG, TIFF, GIF, and PNG.

110. The solution must accommodate the printing and exporting of maintained and managed documents.

111. The solution must allow users to upload and attach documents to targeted records. This must also apply to mobile users.

112. Stored documents must be searchable by keywords, such as application, customer, parcel ID, address, and other indexed attributes.

113. The solution must allow permission-based review and editing of documents in the document manager.

114. The document management solution must accept the migration/import of documents and other digital assets presently being used by the Customer. Common Customer document formats include All Microsoft Office formats, .pdf, and all photo formats, including JPEG, TIFF, GIF, and PNG.

J. Audit Function

115. For tracking and audit purposes, the solution must assign unique identifiers to all users.

116. The solution must timestamp all actions taken by users and reflect the activity in the audit trail.

117. The solution must maintain an audit trail of data changes, including but not limited to previous and new values, change dates, and the identity of the person making the change.

118. Audit trails must be accessible in real-time by authorized Customer staff.

119. The solution must also be able to produce an audit trail of each user's historical security access changes.

120. The base solution must offer common audit trail functions inherent to best practice solutions and must, at a minimum, include:

    a. Ability to audit based on activity type (view, modify);
    b. Ability to set audit requirements based on data type or service type;
    c. Ability to set audit retention schedule based on data type or service type;
    d. Ability to audit user activity, including but not limited to logins, logouts, and changes within a record;
    e. Ability to restrict access to auditing data;
    f. UI for query/search and reporting of audit data; and
    g. The ability for users to customize audit reports.

K. Archival

121. Per the Customer’s retention schedule requirements, the solution must retain, in a non-proprietary format, a complete repository of all records, documents, and transactions for the current operating year and the five (5) years prior, or as specified by Customer.

122. Authorized Customer users must have access to all related archived records, documents, and transactions.

L. Administrative Management

123. The base solution must offer administrative management features and functionality common to all best practice Traffic Signal Analysis solutions, whether specified by this RFP/Attachment A.

124. The proposed solution must provide configurable, role-based administrative tools and controls.

125. The solution must assign a unique name and number to identify and track user identity.

126. The solution must allow authorized users to set security and permissions by user or user group, including customized access permissions.

127. The solution must be highly configurable and, at a minimum, allow authorized users to generate, modify, and delete user accounts.

128. The solution must be highly configurable and, at minimum, allow authorized users to configure business rules, data elements, screens, workflows, triggers, navigation, and dashboards.

129. The proposed solution must accommodate common administrative functions such as creating and maintaining user accounts, backing up and restoring files, exporting files, generating reports, etc.

130. Customer administrators must be able to use input workflows to test new and modified types of transactions (TOTs). The TOTs can be any of those ingested by or created as output by any other workflow.

M. Calendar Function

131. The Vendor must describe the solution’s full-featured calendar functions that are common to all best practices for Traffic Signal Analysis.

132. At a minimum, the solution should offer calendar functions as described below:

    a. Can generate calendars based on Traffic Signal Analysis data (i.e.: peak travel times); Calendar events can be sent to Outlook calendars. If the event is updated, the Outlook event is automatically updated.

    b. Configurable meeting notification and event fields display.

    c. Calendars are exportable.

    d. Events can be displayed in calendar style.

III. SYSTEM/SOLUTION DESIGN

A. Data Management

133. 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.

134. The Vendor agrees that the State shall own all rights, titles, and interests 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 during data center operations related to this solution, in response to service or technical issues as required by the express terms of this service or at the State’s written request.

135. The Vendor agrees to maintain and archive State data in non-proprietary formats to facilitate any future transition from the hosted solution to another solution.

B. Data Migration

136. The Vendor must acknowledge and agree that the Customer is the sole owner of all database content migrated from existing databases and any future database

content created within the awarded Vendor solution, with exclusive rights to use the database content without restriction.

137. If necessary, the Vendor must agree that such migrated and future created database content will be accessible in a non-proprietary format acceptable to the Customer.

138. The solution must accommodate all document formats requiring migration with existing records. Document formats currently in use include all Microsoft Office formats, .pdf, and all photo formats.

139. All migrated data must be searchable and reportable.

140. If conversion and migration costs are not included in the solution's base quote, the Vendor must present them as separate line items in Section VIII, Cost Information Submission.

C. Backup Services

141. The Vendor must be able to configure, schedule, and manage all data backups, including but not limited to files, folders, images, system state, databases, and enterprise applications.

142. The Vendor must maintain backup system security and application updates.

143. The Vendor must provide cloud backup options.

144. The Vendor must agree that the proposed solution will be backed up (data and system configurations) daily for continuity of operations considerations.

145. The Vendor must agree that the proposed solution will permit system administrators to selectively create full and incremental backups of all files without impacting the system's functionality.

146. The Vendor must encrypt all backup files and data and manage encryption keys. At a minimum, the backup options must encompass a strategy of daily incremental and weekly full backups. All cloud instances must include options for snapshots and backups of snapshots.

147. The encrypted backup should be moved to another geographical cloud region. Regardless of the backup method, weekly full backups must include system State information. The customer retention requirement for all backups is 52 weeks. Backup retrieval must be started within two hours of notification from the Customer. The Vendor must monitor all disaster recovery instances, including replication and instance performances.

148. The solution must be capable of running backup reports weekly or in whatever sequence the Customer requires. For example, the report should reveal which jobs were completed, failed, restarted, etc.

149. The solution must be capable of on-demand and auto-run reporting for backup reporting.

150. The Vendor must be willing to provide backups on demand related to development, database changes, or emergencies.

D. Business Continuity/Disaster Recovery

151. If the Vendor's host site experiences unsafe or inoperable conditions, the Vendor must be prepared to resume normal Customer operations within two business days of becoming compromised. So that the Customer can assess the Vendor's ability to meet this requirement, the Vendor must submit, with its proposal, a preliminary Continuity of Operations Plan (COOP). COOP services include but are not limited to providing cloud computing, system data, and documentation to ensure essential services in the event of a disaster declaration. Essential services are defined as those functions that enable the Vendor to provide normal Customer operations under any circumstances.

152. At a minimum, the Preliminary COOP must:

    a. Outline a decision process for determining appropriate actions in implementing COOP plans and procedures to resume essential operations within two business days of failure.
    b. Describe procedures to restore system functionality and to protect the integrity of system data and other assets.
    c. Describe plans to mitigate disruptions to operations and
    d. Outline plans for a timely and orderly recovery from an emergency and to resume full service to users.

153. Upon implementation, the Customer and the awarded Vendor will update the COOP to:

    a. Revise plans and procedures as appropriate.
    b. Identify essential functions.
    c. Identify and describe alternate facilities.
    d. Identify vital records and databases.
    e. Document testing, training, and monthly exercises and drills.
    f. Establish a roster of fully equipped and trained State personnel with the authority to perform essential functions and activities and
    g. Establish reliable processes and procedures to acquire resources necessary to resume essential operations and functions within two days of the disaster declaration.

154. In the event of a declared disaster, the Customer expects the Vendor to be completely responsible for the restoration of essential operations.

155. The Vendor will be expected to invoke the appropriate disaster recovery plan within four hours of the disaster declaration and the disruption of normal operations.

156. Customers must be able to log on to the failover system at the disaster recovery site at 100% operational capacity within two (2) business days of the declaration of disaster.

157. In the event of a disaster declaration, the Vendor must maintain regular and consistent communications with the Customer, keeping all relevant managers and responders informed and updated on efforts to restore normal operations.

158. The Vendor must agree that the proposed solution will maintain synchrony between the primary Customer site and the failover site to ensure that every

transaction successfully enrolled in the operational site is still available in case of a switchover to the alternate site.

IV. Implementation Requirements – Statement of Work

A. Vendor Acknowledgement

159. This section outlines the Customer minimum expectations of the awarded Vendor for implementing the selected solution. Implementation deliverables will reveal the Vendor’s expertise in project management, proposed solution process management, improvement, data migration, acceptance testing, etc. The customer expects the proposed preliminary implementation plans to be refined by the awarded Vendor and Customer project managers during implementation.

160. Upon award, MDOT will lead the implementation, adhering to the specified requirements and the agreed-upon elements of the Vendor’s proposal, as well as any negotiated changes or updates that may occur over the project's term.

B. General Scope

161. The Vendor must agree to:

a. Deliver a fully functional hosted traffic signal analysis platform.

b. Integrate the platform with existing traffic signal infrastructure.

c. Deliver comprehensive training materials and sessions to Customer personnel.

d. Provide detailed documentation of the system, including user guides and technical manuals.

e. Deliver regular reports on system performance and traffic analytics.

162. The Vendor must agree to implement the awarded solution to achieve the following minimum goals:

a. Enhance functional, technical, and administrative capabilities of the incumbent system the Customer’s traffic signal management.

b. Identify and establish workflows based on Customer feedback and automate manual processes.

c. Migrate existing database content to the selected solution.

d. Maintain historical data integrity if the proposed solution changes current Customer data formats.

163. The Vendor must extensively test the proposed solution to identify and correct deficiencies in base capabilities, customizations, integrations, interfaces, migrations, and Customer processes. Such efforts must include but may not be limited to:

a. On-site Testing.

b. COOP Testing.

c. User Acceptance Testing; and

d. Final Acceptance Testing.

164. The Vendor will be responsible for any interface, integration, conversion, migration, or other issues that may arise during implementation.

165. The Vendor must train system users and provide complete system documentation and user documentation.

C. Compliance Standards (Fed or State oversight, compliance regs, etc.)

166. Ensure compliance with relevant state and federal regulations.

167. Conduct regular security audits and vulnerability assessments.

D. Project Management Plan

168. Project Management Plan (PMP): The customer desires to implement the proposed solution rapidly after contract execution. So that the Customer can assess the Vendor’s ability to successfully implement the proposed solution, the Vendor must submit a preliminary PMP. At a minimum, the PMP must address design and development, all implementation tasks, data conversion and migration, estimated hours per task, major project milestones, quality assurance checkpoints, testing, and end-user training. The preliminary PMP must be submitted with the Vendor’s proposal.

169. Vendor’s PMP must include a preliminary Integrated Master Schedule (IMS). The IMS must estimate the time necessary to complete all implementation phases from the point of contract execution through completion of go-live, final system acceptance, and user training.

170. The PMP, which will require Customer approval, must reveal plans for multiple environments, including design and development, user testing, production, end-user training, and help desk support. All customizations, integrations, and interfaces must be tested and validated in the user-testing environment.

171. The Vendor’s PMP must reflect industry best practice standards and must detail the Vendor’s plans for planning, monitoring, supervising, tracking, and controlling all project activities.

172. The Vendor’s PMP must describe the organizational structure of the implementation team, team member roles and responsibilities, resources, processes, and all other information necessary for the Customer to assess your ability to manage the proposed solution.

173. Upon award, the Vendor and Customer will jointly modify the proposed PMP and IMS as appropriate to meet implementation objectives. The customer expects the Vendor to work with the customer project manager to ensure effective project management during all implementation phases and until final acceptance.

174. Regarding this procurement, state all Vendor assumptions or constraints regarding the proposed solution, overall project plan, timeline, and project management.

175. Identify any potential risks, roadblocks, and challenges you have encountered in similar implementations that could negatively affect the timely and successful completion of the project. Recommend a high-level strategy to mitigate these risks.

176. A Vendor’s PMP must address interface, integration, conversion, migration, or other issues that may arise during implementation.

177. The customer will have limited resources available to the awarded Vendor for implementation.

E. System Design Document

178. Before implementation, the awarded Vendor must submit a System Design Document (SDD) for review and State approval. The SDD must:

    a. Include a conceptual model of the system architecture. This can be illustrated by flowcharts.

    b. Include descriptions and illustrations of modules that handle specific system tasks.

    c. Include descriptions and illustrations of components that provide a function or group of related functions.

    d. Include descriptions and illustrations of interfaces that share boundaries across the components where the system exchanges related information.

    e. Include descriptions and illustrations of data flow and the management of this information.

    f. Include complete workflows for all operational user and administrative functions.

    g. Include database scheme, listing all the tables, fields, and characteristics.

179. When the SDD document has been approved by the State, the Vendor may proceed with implementation.

180. So that the Customer can assess the Vendor's ability to prepare an SDD, the Vendor must submit a preliminary SDD or a sample SDD from a prior project of similar size and scope. The Vendor may redact sample plans from prior implementations if necessary. The preliminary SDD must be submitted with the Vendor's proposal.

F. Data Conversion and Migration

181. So that the Customer can assess the Vendor's ability to migrate Customer legacy data to the proposed solution, the Vendor must submit a preliminary Data Migration Plan (DMP). Highlight any known risk factors and present risk mitigation plans. The preliminary Data Migration plan must be submitted with the Vendor's proposal.

182. The DMP must specifically show how the Vendor intends to accurately and completely migrate Customer data, including conversion if necessary. The Vendor agrees to work with the Customer to define and execute data cleanup efforts before conversion/migration.

183. The Vendor must be specific about the proposed methodology, tools, data, facilities, personnel, and other resources required for the migration. Regarding personal and other resources, be specific about whether the resources are supplied by the Vendor, Customer, or other. The Vendor should keep in mind that the Customer has limited available resources.

184. The Vendor must detail data migration testing plans to validate the successful migration of data.

185. The Vendor must work with the Customer project implementation team to update and modify the data migration plan as appropriate.

186. The Vendor must agree that final data migration and data migration testing plans are subject to approval by the Customer.

187. The Vendor must propose a set of system acceptance validations/tests that will demonstrate that the Vendor has complied with the Data Migration Plan. This set of system acceptance validations/tests, along with the Data Migration Plan, must be approved by the Customer before any data migration occurs.

188. Upon award, the Data Migration Plan will be amended to meet specific migration needs determined by the Vendor and Customer. During/following conversion completion, the Vendor/Customer must perform the acceptance tests in the Data Migration Plan. The customer will review the acceptance plan results and provide an acceptance or rejection letter signed by the proper Customer authority to the Vendor. Only if the Vendor receives the acceptance letter will the conversion be considered complete and accepted.

G. User Acceptance Testing Plan

189. The Vendor agrees to conduct a User Acceptance Testing Plan (UAT) to prove that the proposed solution fully meets the requirements of RFP No. 4588.

    a. Vendor agrees that UAT procedures will include proving all end-to-end workflows and all necessary Customer interfaces.

    b. The Vendor agrees that UAT will provide a full suite of reports generated during the UAT period to validate the reporting functions.

    c. Vendor agrees that all customizations, integrations, and interfaces must be tested and validated in the user testing environment.

190. The Vendor must agree to regular status meetings with the Customer project management team to review progress on UAT.

    a. The Vendor agrees to submit meeting agendas, presentation materials, and subsequent meeting minutes.

191. The Vendor must submit, with his proposal, a preliminary, comprehensive UAT plan (UATP) to demonstrate the Vendor’s ability to conduct user acceptance testing for the proposed solution.

192. Vendor’s UAT plan must incorporate the following minimum components:

    a. UAT Test Procedures and Methodologies.

    b. UAT Test Report; and

    c. Training Materials.

193. Upon award, the Vendor agrees to finalize the preliminary UAT plan with input from the Customer project team.

    a. Vendor agrees that the final UAT plan requires approval from Customer.

    b. Vendor agrees that Customer expects to witness the execution of the UAT.

    c. Vendor agrees that Customer retains the right to determine the success or failure of individual UAT tests.

    d. Vendor must provide the facilities, equipment, and personnel to support the services identified in UAT.

194. The Vendor must agree to provide the equipment and personnel to identify and resolve discrepancies between the results of the legacy system(s) and the results of the delivered system(s).

195. The Vendor must agree to take corrective measures at no additional cost to the Customer when such discrepancies result in a failure of the Vendor-delivered system(s).

H. User Training and Documentation

196. The solution must provide thorough online tutorials/training geared toward the proposed solution users. The solution must track the progress of participants enrolled in training.

197. The Vendor must provide training documentation and keep it updated as appropriate. The web-accessible format is acceptable to the Customer.

198. For general training purposes, the Vendor must provide a mock system containing Customer data for hands-on training for internal and external users. Web-accessible format is acceptable to Customer.

199. Prior to go-live, Vendor must provide on-site training for three to five (3-5) primary system administrators (SAs) in all facets including but not limited to oversight, reporting, tasks, workflows, security, archival and audit trail functions. Further, SAs must be prepared to offer training to any external users (train-the-trainer).

200. Prior to go-live, Vendor must agree to adequately train Customer staff users in how to successfully perform their respective tasks and workflows.

201. Vendor must agree to train Customer staff users and administrators in the effective use of the document management system.

202. Training costs should be included in the Vendor's base offering in RFP No. 4588, Section VIII Cost Information Submission. Training that is considered to be outside the base offering must be presented as a separate line item in the cost information submission.

I. Change Management and Control

203. Vendor must agree that upon award, Vendor will describe, justify, and submit all proposed changes to the agreed upon project deliverables to Customer for approval. Such proposed changes include but are not limited to project scope, any and all implementation requirements, technical, functional, and configuration requirements, and/or all other agreed upon project deliverables.

204. The Project Manager must develop a Change Management Plan (CMP) for Customer which will be executed during implementation and followed throughout the lifecycle of the Traffic Signal Analysis project. At a minimum, the CMP must include the following components:

    a. Readiness assessments;
    b. Communication and communication planning;
    c. Change management activities/events and related roadmaps;
    d. Coaching and manager training for change management;
    e. Developing and providing all facets of user training, including train the trainer;
    f. Mitigation of change resistance to the awarded solution;
    g. Data collection, feedback analysis, and corrective actions;
    h. Celebrating and recognizing success; and

i. After-project review.

205. Vendor must agree to follow the State's process for change control, which consists of the following minimum components:

a. Change Request Identification via Change Request Form - Documentation of change details such as type of change, benefits of change, resources, time and cost estimates, authorizations, etc. (Vendor);

b. Change Request Assessment (State);

c. Change Request Analysis (State/Vendor);

d. Change Request Approval (State);

e. Change Request Implementation (Vendor, overseen by State); and

f. Change Log – Project details such as project number, priorities, target date, status, etc. (Vendor).

J. System Documentation

206. Vendor must provide complete system documentation and keep it updated as appropriate. Web-accessible format is acceptable to Customer.

K. Final Acceptance Review

207. Vendor agrees that upon the successful completion of all implementation phases, including end user training, Customer will conduct a Final Acceptance Review (FAR) to determine whether or not Vendor has satisfied the terms and conditions of the awarded contract, which includes the requirements of this RFP No. 4588, Attachment A.

V. SOFTWARE ADMINISTRATION AND SECURITY

A. General

208. For hosted services, the Traffic Signal Analysis system design must be compliant with the State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy. The State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy is located on the ITS website at www.its.ms.gov.

209. Solution must provide all software and system administration security features common to best practice Traffic Signal Analysis management solutions, whether or not specified by this RFP.

210. Solution must provide controlled access to features and functions by configurable, role-based permissions as defined by Customer.

211. Solution must allow the system administrator to set rights for access to data by individual or group.

212. Solution must prevent unauthorized access to the system.

213. Solution must auto terminate sessions after a specified time of inactivity.

214. Solution must accommodate two-factor authentication.

215. Solution must accommodate administrator user rights to any and all workflows and tasks as determined by Customer.

216. Authorized Customer staff must be able to restrict specific user groups from being able to view or print certain types of documentation.

217. Roles, security, and access rights must be easily configurable without Contractor assistance.

218. The proposed solution must adhere to all current, relevant security, and privacy standards.

219. The proposed solution must offer up-to-date, best practice identity management tools to govern user access, such as forced password changes, historical password checks, and the setting of temporary passwords, etc. User management activity must be logged and be available for reporting. Logging must, at a minimum, provide details such as timestamp, user, IP, and action performed

220. The Vendor shall describe how their proposed solution adheres to established security and privacy standards and other Federal and State laws, regulations, and policies.

221. The Vendor must describe their established business and technical protocols to ensure that the transmission and storage of information remains encrypted while in transit and at rest.

222. At the State's request, the Vendor shall invoke a process for masking, sanitizing, scrambling, or de-sensitizing sensitive data (e.g., PHI/PII) when extracting data from the production environment for use in another environment for testing purposes.

B. Security Audit

223. The Vendor must complete Risk Assessments and Security Audit reports on an annual basis and when additions or changes to functionality affect the security framework and architecture, or when a new vulnerability is identified.

224. The Vendor must cooperate and assist the State in responding to all Federal and/or State, audit and review requests. The Vendor must provide audit support including random sample generation, data extracts, and hard-copy documents, and shall provide any requested data or information.

225. The Vendor must make themselves available for third party auditors that ensure compliance with State and Federal security and privacy rules. The Vendor must provide a mitigation plan for all reported deficiencies. Major and critical deficiencies shall be corrected within established and agreed upon timelines.

VI. Support and Maintenance

A. Customer Support

226. The Vendor must provide a continual, around the clock (24/7/365), manned network operating center (NOC) support and monitoring. This includes but is not limited to operating system support, network monitoring and health performance, network availability, and network security reporting. These services must be offered within the continental United States.

227. Vendor must provide a toll-free telephone number for Customer staff to call 24/7/365 and an always-accessible website for trouble reporting. All telephone customer support must originate in the Continental United States and all support staff must be able to communicate clearly in the English Language.

228. Vendor must disclose instances where a third party or sub-contractor is being used for any portion of customer support services, including the intake of reported problems.

229. Vendor must keep the appropriate Customer management and technical support staff updated on the status of trouble resolution.

230. Vendor agrees to provide adequate training for the effective access and use of support services as requested by the State.

231. Vendor agrees to provide always-updated documentation of all support processes.

232. Vendor agrees that ongoing maintenance and support includes the correction of deficiencies.

233. Vendor agrees that deficiencies may be identified as a result of Vendor's own monitoring or by the State. State discovered deficiencies will be reported to Vendor's customer support for trouble resolution.

B. Issue Tracking

234. The Vendor must use an industry standard tracking system to thoroughly document issues and requests for Customer.

235. Describe how operational trouble issues are submitted, prioritized, tracked, and resolved.

236. Describe how software performance issues are submitted, prioritized, tracked, and resolved.

237. Describe how user support issues are requested, prioritized, tracked and resolved.

238. Detail your escalation procedures for responding to trouble tickets, software performance, and user support issues.

239. The Vendor must provide a customer portal for Customer to track help desk ticketing and incident resolution.

240. For issue tracking, solution must be capable of on demand as well as auto-run reporting.

241. The Vendor must provide a monthly issue tracking report as defined by Customer. For example, the report must detail and comment on any open tickets at month's end, all issues opened and closed within the past month, and other details as required by Customer.

C. Service Availability and Restoration

242. For the initial term and any extended terms of service, the Vendor must agree that, except as the result of a catastrophic event, Vendor will provide least ninety-nine-point ninety-nine percent (99.99%) availability of all Traffic Signal Analysis services, to be measured monthly.

243. Vendor agrees to include as unavailable time, any scheduled outages for preventive maintenance and planned upgrades where the Customer users do not have access to and the use of awarded services.

D. System Monitoring

244. Vendor agrees to provide monitoring services to cover all the services provided by the Vendor, including but not limited to:

a. Network connectivity (i.e., whether the network is up or down, and real-time bandwidth usage);

b. Full stack application monitoring;

c. Services running on the operating systems;

d. Performance indicator;

e. Network latency;

f. Utilization (e.g., memory, disk usage);

g. Trending (for minimum of one year);

h. Sharing of the monitored data with Customer through a portal;

i. High Availability—provider must have capabilities to detect failover to another region or availability zone in the event Customer workload and services failover; and

j. Vendor must provide detailed examples of how it has integrated alerts that are triggered by monitoring technologies into their support processes.

E. Service Level Agreements

245. Customer requires notifications of service outages or degraded performance. The Vendor must communicate notifications via a support ticket, email, telephone call, or by all three methods, depending upon the severity of the situation. Upon service restoration, the provider shall provide fault isolation and root-cause analysis findings in restoration notices to Customer points of contact.

246. Vendor must provide root-cause analysis notifications within two business days of the incident. The Vendor must use proven technology, processes, and procedures to escalate problems to Customer points of contact via a call tree-based solution, depending on the severity and type of issue.

247. The Vendor must provide a work effort estimate once a root-cause analysis is complete and be willing to expedite issues which rate “Critical” or “Severe” depending on the root-cause.

248. The provider shall follow the problem severity guidelines specified in Table 1 for assigning severity levels for incident creation.

ATTACHMENT A

Table 1 - Deficiency Priority Levels

Priority Level	Description of Deficiency	Response Timeframe	Resolution Time
1 **Critical**	System is down (unscheduled downtime) or is practically down (e.g., extremely slow response time) or does not function at all, as determined by State. There is no way to circumvent the problem; a significant number of State users, including distributors and recipient agencies are affected. A production business system is inoperable.	One hour from intake	Eight consecutive hours from intake
2 **Severe**	A component of the solution is not performing in accordance with the specifications (e.g., slow response time), creating significant State business impact, its core functionality is not available, or one of system requirements is not met, as determined by State.	Four hours from intake	24 hours from intake
3 **Moderate**	A component of the solution is not performing in accordance with the specifications; there are unexpected results, moderate or minor operational impact, as determined by State.	24 hours from intake	14 days from intake
4 **Low**	As determined by the State, this is a low impact problem, that is not significant to operations or is related to education. Some examples are: general *how to* or informational solution software questions, understanding of reports, general *how to create reports,* or documentation requests.	48 hours from intake	Resolve educational issues as soon as practicable by Vendor. Low impact software or operational issues to be resolved by next version release or six months, unless otherwise agreed to by State and Vendor.

F. Remedies for Failure to Meet Service Levels

249. Vendor agrees that service credits will accrue for unscheduled downtime, including Vendor's failure to meet system availability requirements or response time requirements for curing deficiencies.

250. For purposes of assessing service credits, response timeframes will be measured from the time the Vendor is properly notified until the State determines that the deficiency has been resolved.

251. For purposes of assessing service credits, Vendor agrees that credits will be measured in monthly cumulative minutes for unresolved deficiencies and unscheduled downtime.

252. Vendor agrees that Priority Levels 1 and 2 response time deficiencies will be considered unscheduled downtime and will entitle the State to service credits in accordance with Table 2, Service Credit Assessments.

253. Without limiting any other rights and remedies available to State, Vendor agrees to issue service credits in accordance with the measures prescribed by Table 2, Service Credit Assessments.

254. Vendor agrees that service credits will be calculated separately for each applicable deficiency and will be assessed at the end of each month of system maintenance.

255. Vendor agrees that after 30 days of continued, deficient response time, according to the SLA, the State will consider the conditions to be equal to unscheduled downtime and the service credits in Table 2 will go into full force and effect.

256. Vendor agrees that service credits are not penalties and, when assessed, will be deducted from the State's payment due to the Vendor.

Table 2 – Service Credit Assessments

Length of Continuous Unscheduled Downtime	**Service Credits**
1 to 4 hours	One day of Service Credits equal to 1/30th of Monthly Fees
4 to 48 hours	Two days of Service Credits equal to 1/15th of Monthly Fees
48 to 96 hours	Five days of Service Credits equal to 1/6th of Monthly Fees
Each additional block of 96 hours thereafter	Additional Five days of Service Credits equal to 1/6th of Monthly Fees

G. Patching

257. The Vendor must provide patching capabilities for all Customer systems in the cloud. Patching must cover all Microsoft and non-Microsoft vulnerabilities.

258. The Vendor must manage deployment of new patches in Customer environment before production deployment and must be capable of excluding patches from normal patching based on requests from Customer. This may include service packs and other application-specific patches.

259. The Vendor must provide Customer with a list of patches to be applied before each patching event.

260. From time to time, Customer may request that specific patches be performed outside of the normal monthly patching cycle. The provider must be capable of support these out-of-cycle patch requests.

H. Software/Product Updates

261. Once available, Vendor must provide all software updates necessary to keep current with the proposed solution’s technology standards, industry standards, third party software upgrades, enhancements, updates, patches, and bug fixes, etc.

262. Such Software updates shall include but not be limited to enhancements, version releases, and other improvements and modifications to the core solution software, including application software.

263. Vendor agrees that maintenance services will also include maintaining compatibility of the solution software with any and all applicable contractor provided interfaces.

264. Vendor agrees that prior to installation of any third-party software or any update thereto, Vendor must ensure compatibility, promptly upon release, with the then current version of the software.

265. Vendor agrees to ensure compatibility with all required or critical updates to third party software, including without limitation, service and compatibility packs, security patches, and updates to operating systems.

266. Vendor agrees that third party application software incorporated by the Vendor is subject to the same maintenance and service obligations and requirements as the application software components that are owned or are proprietary to the Vendor.

I. Technology Refresh and Enhancements

267. Vendor agrees to conduct joint technology reviews with the State to guarantee that the software and system security are adequate for State purposes and are consistent with then-current technology used in similar systems.

J. Additional Requirements

268. 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, here, what additional components may be needed and are proposed in order to complete each configuration. If any component(s) necessary for operation of the requested system is omitted from Vendor’s proposal, Vendor must be willing to provide the component(s) at no additional cost.

VII. RFP DELIVERABLES

269. Vendor must agree to provide the deliverables described in Table 3 below. So that the State can evaluate Vendor capabilities, make preliminary deliverables as detailed as possible to show compliance with the specific RFP requirements. Post award and prior to implementation, Vendor and Customer will amend deliverables as appropriate. Customer approval is required for all deliverables prior to implementation.

Table 3 - Deliverables

Deliverables
Implementation Requirements (Section IV)
1. Project Management Plan (PMP) (Item C)
2. System Design and Development (SDD) (Item D)
3. Data Migration Plan (DMP) (Item E)
4. User Acceptance Testing Plan (UATP) (Item F)
5. User Training Documentation (Item G)
System manuals and project documentation - complete and all inclusive.