Attachment A

to

RFP 4422

Department of Environmental Quality (MDEQ)

Laboratory Information Management Solution (LIMS)

Technical Requirements

ITS Project No. 46675

TABLE OF CONTENTS

TABLE OF CONTENTS

I.   GENERAL

A.   How to Respond to this Section

1.   Beginning with Item 10 this section, label and respond to each outline point in this section as it is labeled in the RFP.

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 in 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 must perform a certain task.

5.   If the Vendor cannot respond with "WILL COMPLY", then the Vendor must respond with "EXCEPTION". (See Section V, 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, Vendor must provide explicit details as to the manner and degree to which the proposal meets or exceeds each specification.

B.   Mandatory Provisions in Technical Requirements for this RFP

8.   Certain items in the technical specifications of this RFP are MANDATORY. Vendors are specifically disallowed from taking exception to these mandatory requirements, and proposals that do not meet a mandatory requirement is subject to immediate disqualification.

9.   Mandatory requirements are those features classified as "MANDATORY" in this Attachment A. Meeting a mandatory requirement means the Vendor has provided a detailed response that demonstrates that the Vendor meets the qualifications and experience required and/or the requested functionality exists in the base solution at time of proposal submission.

C.   General Overview and Background

MDEQ has a laboratory located in Pearl, MS, which employs scientists and analysts who examine water samples, soil samples, and other environmental elements to determine the levels or absences of contaminants. The Laboratory Information Management System (LIMS) is the system used to manage and correlate the data to make these determinations. Labworks LLC has been MDEQ's Laboratory Information Management Solution (LIMS) for over 18 years. Labworks has enhanced their current products and developed new products which has made MDEQ's lab more efficient, improved performance and functionality. The LIMS system has been uniquely customized to meet the measurement, scientific analysis, and inspection requirements enabling accurate reporting to the Environmental Protection Agency (EPA), and seamlessly integrate with existing MDEQ applications. MDEQ seeks a Laboratory Information Management System that has the

same functionality as their current LIMS. The awarded vendor will need to have the ability to migrate MDEQ's current database into the new system.

D. Procurement Goals and Objectives

10.   Note: The terms MDEQ, State, and Office of Pollution Control (OPC) Lab may be used interchangeably.

11.   The State seeks a customizable, commercial, off-the-shelf lab information management solution (LIMS) capable of meeting the needs of the OPC Laboratory as defined in this RFP.

12.   MDEQ is presently hosting the existing LIMS and seeks to procure an on-premise solution where MDEQ will continue to be the host.

13.   The State seeks an industry tested LIMS solution that will provide flexible configuration, increased lab automation, ease of implementation and intuitive utilization.

14.   The State seeks a solution that is currently being used in other States or public entities of similar size and scope for lab automation and information management purposes.

15.   The State seeks a vendor knowledgeable in best practice lab automation to work with the OPC to eliminate manual processes and workflows.

16.   The State seeks to maximize automation and interoperability between existing lab equipment and the awarded solution.

17.   MDEQ seeks a solution designed to:

   a. Meet multiple customer data needs;
   b. Meet rapid response times associated with emergency response;
   c. Achieve better efficiency in storing and retrieving large amounts of analytical data;
   d. Standardize laboratory data collection, including the ability to collect and report quality control data associated with measurement quality objectives;
   e. Manage the increased complexity associated with laboratory deliverables;
   f. Integrate complex analytical instrumentation and automation into data collection and reporting; and
   g. Provide sample tracking and legal audit trails for data.

18.   The OPC will use the solution to store and access sample data generated through sample collection, field-testing, and various environmental analytical testing methods. The data produced will be reviewed and validated before being sent to the final user within MDEQ.

19.   Because of the limitations of the current solution, the requirements of this RFP seek to address currently known lab information management and technological deficits and to automate OPC manual processes. As it relates to the needs of the OPC Lab, the State expects the proposed LIMS to represent best practices and technologies currently available, whether or not a particular feature or function is specifically required by this RFP.

E. Vendor Qualifications / Supporting Documentation

20. In response to Section IX of RFP No. 4422, Vendor must provide references that represent successful LIMS implementations of similar size, scope, and complexity. References furnished in response to this section must substantiate experience delivering and supporting LIMS solutions to public entities charged with the full spectrum of environmental laboratory requirements and functions during the last three (3) years

21. Vendor must provide an introduction and general description of its company's background and years in business providing LIMS solutions of similar size and complexity.

22. Vendor must specify the location of the organization's principal office and the number of executive and professional personnel employed at this office.

23. 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 structure (for example, state, national, or international organization).

24. Vendor must disclose any company restructurings, mergers, and acquisitions over the past three (3) years.

25. Vendor should indicate whether or not business/solution is ISO 9001:2000 certified.

F. Vendor Implementation Team

26. Vendor must demonstrate that all team members have the necessary experience for design, installation, implementation, training, and support of the services required by this RFP.

   a. Identify the primary, key staff who will be responsible for the execution of the various aspects of the project including but not limited to: Project Manager, Application Development, and Implementation Team members.

   b. Describe team member roles, functional responsibilities, and experience with projects similar in size and scope to the services required by this RFP.

   c. For each participating team member, provide a summary of qualifications, years of experience and length of employment with your company.

   d. For each participating team member, provide contact information for three references who would be willing to verify qualifications, experience, and performance.

   e. Vendor must ensure that each team member assigned to this project has the ability to communicate clearly in the English language both verbally and in written form.

G. Regulatory Compliance

27. Proposed solution must position MDEQ/OPC to be and remain compliant with CFR 40 Part 136 and any other relevant Federal or State regulations. The below hyperlink to CFR 40 Part 136 was active at the time of publication. If the hyperlink has changed, Vendor remains responsible for proposing a solution designed for compliance with the cited regulations as well as other regulations applicable to environmental laboratories of similar size and scope.

   CFR 40 Part 136 – Guidelines Establishing Test Procedures for The Analysis of Pollutants: https://www.ecfr.gov/current/title-40/chapter-I/subchapter-D/part-136

II. CURRENT LABORATORY ENVIRONMENT

A. Analyses by Lab Type

28. The OPC Lab provides sampling and testing for multiple projects covering the entire state of Mississippi. EPA requires most of the projects, and all projects must meet EPA testing and method requirements. The projects performed by the OPC Lab include Ambient surface water monitoring, Coastal water monitoring, Beach monitoring, benthic index and stream quality monitoring, compliance and enforcement monitoring, fish tissue consumption.

29. OPC Lab services are handled by four separate laboratories, each providing specific functions as described in Table 1 below.

Table 1 –Analyses by Lab Type

Metals Lab		
Aluminum	Copper	Silver
Antimony	Iron	Sodium
Arsenic	Lead	Strontium
Barium	Magnesium	Thallium
Beryllium	Manganese	Tin
Boron	Mercury	Titanium
Cadmium	Molybdenum	Vanadium
Calcium	Nickel	Zinc
Chromium	Potassium	
Cobalt	Selenium	
Wet Chem Lab		
TOC (Total Organic Carbon)		
BOD (Biochemical Oxygen Demand)		
COD (Chemical Oxygen Demand)		
TSS (Total Suspended Solids)		
Alkalinity		
Oil and Grease		
Cyanide		
Hardness		
Microbiology Lab		
Fecal Coliform		
E Coli		
Organics Lab		
Pesticides		
PCBs (Polychlorinated Biphenyls)		
Volatiles		
Semi-Volatiles		
PAH (Polycyclic Aromatic Hydrocarbons)		
DRO (Diesel Range Organics)		
GRO (Gasoline Range Organics)		

30. Proposed solution must accommodate all types of analyses typical to environmental testing and method requirements.

B. Annual Volumes

31. Proposed solution must accommodate current annual lab volumes and must be scalable to accommodate future increases. Minimum annual lab functions currently include:

    a. Processing more than 3,000 samples from specific sources;
    b. Making more than 50,000 analytical determinations; and
    c. Making as many as 250 different determinations on one sample.

III. HOSTING AND IT ENVIRONMENT

A. Hosting

32. The current solution is hosted by MDEQ. MDEQ intends to continue as the host for the proposed solution. MDEQ will be responsible for hosting, support, and maintenance of the IT infrastructure, including disaster recovery and business continuity.

33. Proposed solution must operate under optimal conditions and performance within the MDEQ host environment. Below is a description of the current MDEQ host environment.

Table 2 - *MDEQ Host Environment*

Server Specifications
Host Server is running SQL Server 2017. MDEQ can upgrade to most recent release.
Host Server – 16 GB RAM, 4 Cores
Backups
Backups are managed by MDEQ OIT.   Backups are automated offsite to a remote server.

34. Proposing vendors whose solution will not operate optimally within MDEQ's current host environment must specify what is required for optimal host conditions. Vendor must provide sufficient detail for MDEQ to fully evaluate the recommended specifications and the related costs to provide the environment.

B. Data Ownership

35. 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.

C. Data Protection

36. 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.

D. Data Location

37. 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.

E. Encryption

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

39. 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:

   a. 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).

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

   c. 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.

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

   e. 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.

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

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

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

   i. 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.

F. Breach Notification and Recovery

40. 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.

G. Notification of Legal Requests

41. 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.

H. Termination and Suspension of Service

42. 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 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 Item 42.c below. Within this 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.

I. Background Checks

43. 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.

J. Security Logs and Reports

44. 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.

K. Contract Audit

45. 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.

L. Sub-contractor Disclosure

46. 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.

M. Sub-contractor Compliance

47. 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.

N. Processes and Procedures

48. 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.

O. Operational Metrics

49. 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

P. Application Software Administration and Security

50. Proposed solution must provide all software and system administration security features common to best practice LIMS solutions, whether or not specified by this RFP.

51. Proposed solution must provide controlled access to features and functions by configurable, role-based permissions as defined by MDEQ.

52. Proposed solution must allow the system administrator to set rights for access to data by individual or group.

53. Proposed solution must prevent unauthorized access to the system.

54. Proposed solution must accommodate administrator user rights to any and all workflows and tasks as determined by MDEQ.

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

56. Proposed solution must prevent users from permanently deleting records.

57. Authorized MDEQ staff must be able to change a record status to inactive.

58. Authorized MDEQ staff must be able to hide a record and/or related documentation from general view.

59. Authorized MDEQ staff must be able to assign rules for data entry and validation rules for all entry points. Authorized MDEQ staff must be able to add, edit, and delete rules.

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

61. Proposed solution must adhere to all current, relevant security and privacy standards.

62. Describe your best practices for Secure Dev Ops. Describe your methods for ensuring seamless integration of security testing and protection throughout the software development and deployment lifecycle of the proposed solution.

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

64. Proposed solution must accommodate the need for authorized system administrators to perform necessary administrative functions including but not limited to creating and maintaining user accounts, backing up and restoring files, exporting files, and generating reports, etc.

65. Proposed solution must offer up-to-date, best practice identity management tools to govern user access, such as forced password changes, historical password checks, the setting of temporary passwords, etc.

66. Proposed solution must auto terminate sessions after a specified time of inactivity.

67. Proposed solution must accommodate two-factor authentication.

Q. Product/Software Updates

68. Describe your release management methodology and processes for updating your software for all types of releases, including but not limited to:

    a. Security Updates: At a minimum, vendor must meet the below security Update requirements:

       1. The vendor must implement all applicable security patches and updates with a severity level of High as defined by the National Vulnerability Database within 24 hours. Medium and Low severity level patches and updates must be implemented within 30 days. Reference hyperlink at the time of the publication of this RFP: National Vulnerability Database

       2. The vendor must implement all applicable patches and updates listed in the Mississippi Department of Information Technology Services Security Advisories within 30 days.   Reference hyperlink at the time of the publication of this RFP: Security Advisories

    b. System Maintenance;

    c. System Enhancements;

    d. Education and Training;

69. Describe how new functions and features are released and how much control clients have over which new features are implemented.

70. 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.

    a. 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.

    b. The State requires notice in advance of software updates.

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

72. 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.

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

74. 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.

75. Enhancements and updates must be included with annual maintenance fees. Vendor must include the related cost in Section VIII, Cost Information Submission of this RFP.

R. Patching

76. The Vendor must provide patching capabilities. Patching must cover all Microsoft and non-Microsoft vulnerabilities.

77. The Vendor must manage deployment of new patches in the MDEQ environment before production deployment and must be capable of excluding patches from normal patching based on requests from MDEQ. This may include service packs

and other application-specific patches. All patches must be proven in a test environment before they are deployed to the production environment.

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

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

IV. FUNCTIONAL/TECHNICAL REQUIREMENTS

A. General

80. Proposed solution must be configurable to allow additional tables, queries, forms, reports, macros, and modules, etc. as determined by MDEQ/OPC.

81. Proposed solution must have the ability to add functions to the program main menu and all other screens allowing the database administrator to keep the LIMS current with user needs.

82. The software shall be licensed to accommodate up to fifteen users at two separate locations at startup. Vendor must provide per user costs in Section VIII Cost information Submission of RFP 4422 in the event MDEQ needs to add new users in the future.

83. All software updates shall be compatible with user definable configuration, as long as user definable configuration is done in accordance with contractor recommendations.

84. Proposed solution must utilize a SQL database, such as Oracle or Microsoft SQL server, to store information in tables. Any proposed LIMS with a database engine that is not fully SQL compatible will not be considered.

85. Proposed solution must replicate the business processes associated with the current LIMS, such as receiving, recording, scheduling, tracking, and reporting results on environment samples for clients. The solution must also store quality control and quality assurance information.

86. Proposed solution must be designed for use in an environmental laboratory and must be capable of managing the lab's data including but not limited to:

    a. Sample tracking;
    b. Sample scheduling;
    c. Data entry and storage of quality control/quality assurance information;
    d. Electronic data transfer from instrument to LIMS;
    e. Electronic data transfer to user clients;
    f. System security features; and
    g. Customized hardcopy and softcopy report generation.

87. Proposed solution must provide enhanced electronic capabilities such as LIMS/instrument interfaces, electronic data reporting, and test scheduling. Refer to Table 3 for a description of the current lab instruments in use at the MDEQ labs.

88. Proposed solution must provide electronic data handling and sample tracking consistent with the requirements of an environmental laboratory.

89. Proposed solution must provide the ability to automatically log and schedule samples for a client/project in advance of the sample collection event. This feature shall address a variety of scheduling frequencies, including hourly, daily, weekly, biweekly, monthly, semi-annually, and annually or via a special study.

90. Proposed solution must be able to import and export electronic data elements. Examples of common OPC data elements are Study, Location Code, Sample Location, Sample Number, Collection MM/DD/Year, Sample depth, QA Type, Alkalinity, Ammonia, Chemical Oxygen Demand, and Total Nitrate, etc.

91. Proposed solution must maintain an inventory of all chemicals used in the environmental laboratory, including but not limited to chemical name, expiration date, location of storage, and vendor used for procurement.

92. Under no circumstances shall any data or equipment associated with the proposed solution reside outside the continental United States, nor shall any data or equipment associated with this proposed solution be accessible to people outside the continental United States.

B. Access

93. Proposed solution must be browser neutral and must be compatible with the current version and two preceding versions of common browsers including Chrome, Microsoft Edge, Firefox, and Safari.

94. Proposed solution must include mobile access/functionality for IOS and Android platforms for use in the field by authorized MDEQ employees.

95. Proposed solution must accommodate project management functions on mobile platforms.

96. Proposed solution must be compatible with Microsoft tablet, Android tablet, IOS and related devices for the current and two immediately preceding versions.

97. Vendor must provide end to end data encryption known as At Rest or In Motion Encryption for LIMS data accessed by MDEQ.

98. Proposed solution must provide real-time data exchange with MDEQ mobile devices having adequate access.

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

   a. 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. Vendor must describe how the additional software is presented to the user and detail the process for download and installation of the software. Vendor should include a sample screen shot or sample instructions with Vendor's response to this requirement.

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

   c. Any costs associated with the use and maintenance of these downloads, plug-ins or additional software must be included in Section VIII: Cost Information Submission of RFP No. 4422.

C. Sample Tracking

100. Proposed solution must provide a laboratory sample numbering format which is user configurable instead of selecting from a fixed list of formats.

101. Proposed solution must store unique field sample identification numbers that are configurable by the user and linked to the LIMS sample number.

102. Proposed solution must integrate with portable field collection devices that utilize Windows Mobile Technology, allowing field collectors to collect field data and upload that data from any location that provides Internet access.

103. Proposed solution must automatically calculate the sample hold times associated with the minimum time available for initiation of sample analysis based upon user input.

104. Proposed solution must be capable of following the progress of samples throughout the analytical process and include integrated barcoding, sample login, chain of custody, price quoting and billing.

105. Proposed solution must group samples into work lists, preparation batches, and QC batches by user definable selection criteria such as by batch, sample number, client, project, test, method, department, etc.

106. Proposed solution must provide a query function to retrieve sample information by work order, sample number, client, analysis, project test, department, date range, site, or other information for many functions throughout the LIMS.

107. Proposed solution must have the ability to read a variety of bar code fonts and generate bar code labels representing laboratory and field sample identification numbers.

108. Proposed solution must provide sample log-in and sample tracking functions capable of distinguishing samples being analyzed in-house versus those submitted to other governmental and/or contract laboratories. In-house analyses, as well as samples submitted to other laboratories, shall be tracked separately. The LIMS shall also enable the user to change the status of a sample from "in-house" to "contractual."

109. Proposed solution must generate sample backlog reports identifying current sample workloads.

110. Proposed solution must identify samples with completed client requested analysis and designate for sample disposal.

D. Quality Control/Assurance Information

111. Proposed solution must provide integration of simple calculations for the generation of sample analytical results.

112. As determined by OPC, authorized users must be able to transfer LIMS data to archive database(s) which will be hosted by MDEQ. Authorized LIMS users must be able to view and/or retrieve LIMS data stored in the MDEQ-hosted archives.

113. Proposed solution shall track quality control, including sample replicates, matrix spikes, quality control check standards and blanks.

114. The user shall have the ability to create quality charts based upon quality control data that has been entered into the solution.

115. Proposed solution shall link all quality control data to the associated sample, test data and batch run.

116. Proposed solution shall calculate quality control results and automatically flag all quality control data which is not within user defined quality control limits.

E. Lab Instruments

117. Proposed solution must store and maintain records pertaining to the lab instruments' calibration data, as well as historical records on all instrumental repairs. Records pertaining to formal and informal training obtained by analysts shall be stored and maintained.

118. Presently the transfer of data from lab instruments to the current LIMS is a manual process. The current on-site lab instruments and their functions are detailed in Table 3 below. Of the 15 lab instruments named in Table 3, it is OPC's understanding that only five are capable of transmitting directly to the current/future LIMS. Where possible, OPC expects to automate the transfer of data from the capable instruments to the awarded LIMS solution. Vendors must review the list of instruments and advise whether or not they are capable of enabling such automation and provide a detailed description of their proposed methodology. If such automation is not part of the base offering, Vendors must provide pricing as an optional line item in Section VIII Cost Information Submission of RFP No. 4422.

Table 3 - Current OPC Lab Instruments, **Descriptions, Functions**

Wet Chemistry: Barcodes only used in Wet Chem – These instruments are capable of directly sending data to a LIMS solution, but this is currently a manual process for OPC. OPC intends to automate this process in the future. (Room 830)
TOC Solids – Dell Precision T3500, Interfaces with Windows XP– Shimadzu TOC-Vcsh
TOC Water – Optiplex 790 (92451), Interfaces with Windows 10 – SUEZ Sievers MS310C
Thermo Gallery – Optiplex XE3, Interfaces with Windows 10
Lachat QuickChem (2012) – Optiplex 790 (92771), Interfaces with Windows 7
Lachat QuickChem (2015) – Optiplex 9020 (92606), Interfaces with Windows 7
Semi-Volatiles: Manual lab processes involved. OPC does not intend to send data directly to LIMS. (Room 824)
PCBs – Optiplex 760, Windows XP – Agilent 6890
Pest QQQ – HP Z230, Windows 7 – Agilent 7890/7010
TTO/DRO – HP, Windows XP – Agilent 6890/5973
Semi-volatiles – HP Compaq, Windows NT – Agilent 6890/5973
Volatiles - Semi-Volatiles: Manual lab processes involved. OPC does not intend to send data directly to LIMS. (Rooms 831 and 824)
Volatiles – HP Compaq, Windows XP – Agilent 6890/5973
GRO – HP Compaq, Windows XP – Agilent 6890
Organic Extraction Lab and Semi-Volatiles: Manual lab processes involved. OPC does not intend to send data directly to LIMS. (Room 818)
GC/FID – Gateway, Windows NT – Agilent 6890

Metals and Semi-Volatiles: Manual lab processes involved. OPC does not intend to send data directly to LIMS. (Rooms 828 and 824)
ICP-MS – Optiplex 780, Windows Vista – Agilent 7700
Mercury Low-Level – Think Centre M80T, Windows 10 – CETAC QuickTrace M-8000
Mercury Fish Tissue and Sediment/Soil – DMA 80

F. Workflow

119. Proposed solution must accommodate configurable workflows and business rules that are common to best practice LIMS solutions, regardless of whether or not they are specified by this RFP.

120. MDEQ LIMS processes follow prescribed steps, depending on the type of required action. Proposed solution must allow multiple, configurable workflows and processes in accordance with all MDEQ data driven parameters and established procedures.

121. Proposed solution must provide flexible workflow routing to accommodate MDEQ processes involving multiple sample types with differing workflows.

122. Proposed solution must provide configurable triggers that will initiate event and/or data driven workflow actions.

123. Proposed solution must provide configurable time standards that initiate and route workflows based on multiple variables such as event aging and failure to comply with compliance actions. Such events and conditions will be defined by MDEQ.

124. Proposed solution must allow authorized users to redirect workflows in response to circumstances that require temporary or permanent changes.

125. Solution business rules and workflows must allow multiple, related triggers.

126. Proposed solution must automatically calculate service deadlines; this feature must be configurable.

127. Workflow routing must accommodate, track, and report on due dates as defined by MDEQ.

128. Proposed solution must distribute LIMS information and/or tasks to relevant parties simultaneously.

129. Proposed solution must display workflows in simple, graphic formats which are easily understood by system users.

130. Workflow graphics must indicate the current status of a work item in the workflow.

131. Proposed solution must allow workflows to be saved as templates to be reused for other types of LIMS actions.

132. Proposed solution must provide the ability to create and modify workflows using built-in administrative tools.

133. Workflows must be capable of routing LIMS functional responsibilities to specific staff member work queues.

134. MDEQ will consider it an advantage if the solution allows workflows to be configured with drag-and-drop tools through a graphic user interface.

135. Authorized MDEQ staff must be able to re-assign and/or override workflow tasks as necessary to manage workloads and processes.

G. Chain of Custody/Enforcement Actions

136. Proposed solution must be configurable to accommodate chain of custody handling, tracking, and reporting details related to typical environmental compliance and enforcement actions. Vendor must provide a detailed description of the chain of custody functionalities inherent to the proposed solution. If chain of custody functionality is not part of the base offering, Vendor must propose separate line item pricing in the Section VIII Cost Information Submission of RFP No. 4422.

H. Document Manager

137. Proposed solution must offer a full featured document management system (DMS) that accommodates generating, manipulating, editing, and uploading/storing paper and electronic documents.

138. Proposed solution must be able to upload documents in formats commonly accepted by environment lab processes. Common MDEQ document formats are: All Microsoft Office formats, .pdf, and all photo formats including JPEG, TIFF, GIF, and PNG.

139. Proposed solution must accommodate printing and/or exporting of maintained and managed documents.

140. Proposed solution must allow users to upload and attach documents to targeted records.

141. Stored documents must be searchable by key words, such as sample numbers, study names, dates, county codes, collectors and other indexed attributes.

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

I. Search Functions

143. Proposed solution must offer all search features and functionality common to best practice LIMS solutions, whether or not they are specified by this RFP.

144. Proposed solution must offer full featured, configurable data search functions that can be scheduled to run automatically and/or as a result of an individual request from an authorized user.

145. Proposed solution must be able to produce search results that represent the search term, as well as subtle variations of the search term.

146. Proposed solution must offer pre-defined searches that would be common to environmental lab activities.

147. Proposed solution must have search functionality that allows keyword searches within the full system data base.

148. Searches must be exportable or downloadable to common file formats such as Excel, .pdf, xml, and csv.

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

150. Users must be able to search for upcoming events, deadlines, or other quantifiable parameters as determined by MDEQ.

J. Reports and Dashboards

151. Proposed solution must offer pre-designed, standard reports common to best practice MDEQ LIMS activities, whether or not they are specified by this RFP.

152. Proposed solution must provide all tracking and reporting functionality necessary to meet the mandated reporting requirements associated with MDEQ activities. Such reports include but are not limited to draft reports, final lab reports, backlog reports, pending analyses, and compliance reports, etc.

153. Proposed solution must accommodate the creation and modification of standard reporting templates as defined by MDEQ.

154. Proposed solution must accommodate user defined reporting for the purpose of creating custom reports from any and all data elements for which MDEQ requires tracking and/or reporting. User defined reporting tool must be intuitive and easy for the user to comprehend and must not require specialized knowledge of a third party tool such as Crystal Reports.

155. Proposed solution must provide the ability to save user-generated reports under user profiles.

156. Proposed solution must allow MDEQ Staff to create and save customized reports and queries.

157. Proposed solution must be capable of exporting reports into several file formats including but not limited to .pdf, MS Excel, MS Word.

158. Proposed solution must be able to distribute reports through the workflow as email attachments.

159. Proposed solution must provide configurable dashboards that can be customized to serve the needs of individual users.

160. Proposed solution must provide configurable dashboards on throughput performance measures and system activities, such as active users, action items, deliverables, etc.

161. Proposed solution must provide configurable executive dashboards.

162. Proposed solution must be able to automatically generate reports on a configurable schedule and distribute them to selected users.

163. For Vendor reference, a document providing examples of existing reports that the solution must be able to produce is posted on the ITS website directly beneath the RFP No. 4422 documents. It is titled Examples of Compliance Reports. These examples are representative and are not all inclusive.

164. The proposed solution must:
    a. Offer fully configurable reports.
    b. Automatically report numeric results to the number of significant figures and decimal places as specified by the user.
    c. Have the ability to enter text values into the result field.
    d. Automatically report as "less than" any numerical data value which is less than the method detection limit specified by the user.

K. Ticklers

165. Proposed solution must provide all tickler capabilities common to best practice LIMS solutions including but not limited to the following:

    a. Ticklers can be directed to a specific person or people, with a due date and a description of the task to be accomplished.

    b. Ticklers can be updated and modified, e.g., assign new due date, add recipient, etc.

    c. Priorities can be set for ticklers.

    d. Authorized users can configure tickler displays, including the ability to set an expiration date.

    e. Satisfied ticklers can be filtered from display but remain accessible.

    f. Ticklers can provide notification to users of unsatisfied overdue ticklers.

    g. Ticklers can be directed to multiple recipients.

166. If possible, solution should allow:

    a. Tickler content to be saved as a file note;

    b. All ticklers in a workflow to be displayed, showing due dates and which are satisfied; and

    c. Configurable user notification when a new tickler is received

L. Notifications

167. Proposed solution must offer configurable notifications and alerts common to best practice LIMS solutions.

168. Proposed solution must provide email and/or correspondence templates for notification purposes.

169. Proposed solution must provide task management functions that will issue alerts for pending, due, or past due tasks. This function should interface with the dashboard function to give users a visual representation of the status of their tasks.

170. Task logs must reveal daily assigned tasks, task details, task due dates, task status, and all other details pertinent to task management.

M. Calendar Functions

171. MDEQ prefers a solution with full featured calendar functions that would be common to best practice environmental LIMS solutions.   MDEQ will consider it a plus if Vendor's solution offers such functions. Vendor must indicate which of the common calendar functions below are offered by the proposed solution.

    a. Generate calendars based on management event requirements;

    b. Calendar event can be sent to Outlook calendars. If event is updated, Outlook event is automatically updated;

    c. Configurable meeting notification and event fields display;

    d. Calendars can be shared with participating entities, as determined by MDEQ;

    e. Calendars are exportable;

    f. Events can be displayed in calendar style; and

    g. Users can subscribe to calendar events.

N. Audit Functions

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

    a. Ability to audit based on activity type (View, Modify, Delete);

    b. Ability to set audit requirements based on data type or sample type;

    c. Ability to set audit retention schedule based on data type or sample type;

    d. Ability to audit user activity including but not limited to logins, logouts, and changes within a record, date/time of the change, original value, new value, and the reason the data was changed.

    e. Ability to restrict access to auditing data;

    f. UI for query/search and reporting of audit data; and

    g. Ability to produce customized reports for all audited activities. Must accommodate common output formats described herein.

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

174. Proposed solution must time stamp all actions taken by users and reflect the activity in the audit trail.

175. Proposed solution must have capability to produce audit trail reports that capture LIMS user activities.

V. IMPLEMENTATION

A. Project Management Plan and Integrated Master Schedule

176. MDEQ desires to implement the proposed solution as rapidly as possible after contract execution. So that MDEQ can assess Vendor's ability to successfully implement the proposed solution, Vendor must submit a preliminary Project Management Plan (PMP) with the proposal. At a minimum the PMP must address design and development, all implementation tasks, data conversion, migration, estimated hours per task, major project milestones, quality assurance checkpoints, testing, and end-user training for all facets of the solution.

177. Vendor's PMP must reflect industry best practice standards and must detail Vendor's plans for planning, monitoring, supervising, tracking, and controlling all project activities.

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

179. Upon award, the Vendor and MDEQ will jointly modify the proposed plan as appropriate to meet implementation objectives. MDEQ expects the Vendor to work with the MDEQ and MIS Project Managers to ensure effective project management during all phases.

180. Vendor will be responsible for any integration, conversion, migration, or implementation issues that may arise during implementation.

181. As it relates to this procurement, state all Vendor assumptions or constraints regarding the proposed solution and overall project plan, timeline, and project management.

182. 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.

183. The plan must include multiple environments, including Development, Hosting, User Testing, Production, and Training.

184. In the user testing environment, all customizations, integrations, and interfaces must be tested and validated.

B. Data Conversion and Migration

185. Vendor must successfully migrate all existing MDEQ LIMS data to the awarded solution. All current LIMS data is in SQL 17 format. MDEQ estimates 601 MBs of LIMS data.

186. If conversion to the awarded solution is required, Vendor is responsible for data conversion and Vendor must present a detailed Data Conversion Plan for the State's approval prior to commencing conversion processes.

187. Vendor must provide verifiable, statistical information, such as record counts to prove the successful conversion of legacy data.

188. Vendor must acknowledge and agree that MDEQ is the sole owner of any and all database content migrated from the current solution to the proposed solution, and any future database content created within the awarded vendor solution, with exclusive rights to use the database content without restriction.

189. Vendor must agree that such migrated database content and future created database content will be maintained in a non-proprietary format that is acceptable to MDEQ.

190. Proposed solution must accommodate all document formats that will require migration with existing records. Document formats currently in use include but are not limited to: All Microsoft Office formats, .pdf formats, and all photo, video, and audio formats.

191. If conversion and migration costs are not included in the base quote for the solution, vendor must present such costs as separate line items in the Section VIII Cost Submission Summary.

C. Data Migration Plan

192. So that MDEQ can assess Vendor's ability to migrate and map MDEQ legacy data to the proposed solution, 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.

193. The Data Migration Plan must specifically show how Vendor intends to migrate and map MDEQ data accurately and completely, including conversion if necessary. Vendor agrees to work with MDEQ to define and execute data cleanup efforts prior to conversion/migration.

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

195. Vendor must detail data migration testing plans to validate the successful migration and mapping from the incumbent solution to the proposed solution.

196. Vendor must work with the MDEQ project implementation team(s) to update and modify the preliminary data migration plan as appropriate.

197. Vendor must agree that final data migration and data migration testing plans are subject to approval by the MDEQ.

198. Vendor will ensure that the results of a data audit are applied to the agreed scope to develop a series of rules for transferring all designated source data and ensuring that it is accurately manipulated to fit the target.

199. Vendor agrees that before any actual code is written, the mapping specifications and supporting documentation will be clearly understood and approved by MDEQ prior to migration of data.

200. 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 MDEQ before any data migration occurs.

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

D. Development and Testing Environments

202. Vendor must provide development and testing environments. As the host, MDEQ will provide the IT infrastructure and browser-based access to the development and testing environments provided by the awarded vendor.

203. Vendor must provide an operable test environment containing viable legacy data to prove that workflows, triggers, calendars, document manager, and other integral components function as expected.

204. Vendor must submit a proposed Acceptance Testing Plan (ATP) for review and approval by the State.

E. User Acceptance Testing

205. Once the State approves the written acceptance testing plan, Vendor agrees to conduct/support User Acceptance Testing (UAT) to prove that the proposed solution fully meets the requirements of this RFP/Attachment A, including all interfaces and/or integrations.

206. Vendor's user acceptance testing must provide for parallel testing which will compare the results of the awarded solution against the existing LIMS. Prior to acceptance, the awarded solution must run in parallel testing mode with the existing LIMS for a minimum of five business days without errors.

207. So that MDEQ can assess Vendor's ability to conduct user acceptance testing, Vendor must submit with this proposal a preliminary User Acceptance Testing Plan (UAT). MDEQ will accept a sample UAT Plan from a previous implementation of similar size and scope and Vendor may redact the plan if necessary.

208. At a minimum, the UAT Plan must incorporate the following components:

    a. UAT Test Procedures and Methodologies, including final acceptance testing to confirm that the awarded solution performs in accordance with the requirements of this RFP;

    b. Provisions for parallel testing of the awarded solution against the current LIMS;

    c. UAT Test Report; and

    d. Training Materials;

209. At a minimum, the UAT Plan must:

    a. Include both scripts and normal operations to test end-to-end workflows, customizations, and integrations; all MDEQ interoperability and interfaces must be tested and validated;

    b. Provide a full suite of reports generated during the UAT period to validate the reporting functions; and

    c. In the user testing environment, all customizations, integrations, and interfaces must be tested and validated.

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

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

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

    c. Vendor must provide the personnel to support the services identified in the UAT, including Final Acceptance Review (FAR).

211. Vendor agrees to regular status meetings with MDEQ project management team to review progress on UAT.

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

213. The Vendor must provide technical staff during acceptance testing to assist in demonstrating the functions of the system.

F. Implementation and Final Acceptance

214. Project status will be considered complete when the work products described and required by this RFP have been delivered, tested, and accepted by the MDEQ project manager.

215. Implementation of the awarded solution must be accomplished with minimal interruption of normal day-to-day operations of MDEQ. MDEQ and the awarded Vendor will jointly determine implementation time frames.

216. Prior to final acceptance, MDEQ and the awarded vendor must agree upon and document the roles and responsibilities pertaining to the upkeep, maintenance, and support of the awarded solution.

217. Following implementation, MDEQ will conduct Final Acceptance of the awarded solution. Final Acceptance shall mean written notice from the State that it has accepted the System following a 30-day Acceptance Period of production deployment during which time the system has conformed in all material respects to the applicable specifications, including any approved change orders for the system, with all defects discovered during the Acceptance Period fixed by the Vendor and

tested and accepted by MDEQ. This Final Acceptance period includes, without limitation, correction of errors, design deficiencies, performance deficiencies, and incorrect or defective documentation, including those found during Conversion/Migration, Acceptance Testing, Implementation, and the Final Acceptance period.

G. User Training and Documentation

218. Awarded Vendor must provide complete user training documentation and keep it updated as appropriate. Web-accessible format is acceptable to MDEQ for training documentation.

219. Awarded Vendor must provide thorough online tutorial/training geared toward MDEQ users.

220. Prior to go-live, Vendor must agree to adequately train up to 15 MDEQ staff users and administrators in how to use the system to successfully perform their respective tasks and workflows. Vendor must use a train-the-trainer approach. If on-site training is not included in the base offering, vendor must submit a fully loaded daily rate as a separate line item on Section VIII, Cost Information Submission of RFP No. 4422.

221. Awarded Vendor must train MDEQ staff users and administrators in the effective use of the proposed solution.

222. Awarded Vendor must train the primary system administrators in all facets of system use, including but not limited to oversight, reporting, security, workflow, archival, and audit trail functions.

223. Proposed solution must provide on-line training modules to address system customization that may be performed by MDEQ authorized users.

224. Awarded Vendor must provide pre-implementation training.

225. For any training that is not included in the cost of the base offering, Vendor must provide itemized costs in Section VIII of RFP No. 4422, Cost Information Submission.

226. Vendor must be responsible for continual training and support of all system users deemed necessary by MDEQ for the success of the LIMS operations and processes for the life of the Agreement.

VI. WARRANTY, MAINTENANCE, AND SUPPORT

A. Warranty

227. The warranty period is a one-year period during which the Vendor must warrant, at no cost to MDEQ, all work performed as stated in RFP 4422, Attachment A, Vendor's proposal, and any subsequent Statement(s) of Work. The warranty period must include the necessary vendor support to correct any deficiencies found and to provide any other consultation as needed.

228. For any phased implementations or processes, the warranty period for each phase or process will begin only when Vendor has fully implemented the phase or process and MDEQ has accepted the phase or process as functioning properly and in coordination with any previously implemented phase(s) or process(es).

229. The Vendor must agree to warrant all proposed application software to be free of errors for a minimum period of one year after acceptance. During this period, the

Vendor must agree to correct, at his own expense, any discovered errors. If the system fails during warranty period due to a defect, the Vendor will offer a workaround solution within 24 hours and a full fix within five business days.

230. The Vendor must state and discuss the full warranty offered during the warranty period on all proposed software and services and indicate if it is longer than the minimum.

231. This warranty must cover all components for which services were provided, including all programs, forms, screens, reports, subroutines, utilities, file structures, documentation, interfaces, conversions, configurations, or other items provided by the Vendor.

232. The Vendor must agree that all corrections made during the warranty period are integral to work associated with this project and will therefore be made at no additional charge.

B. Customer Support

233. The Vendor must provide a continual, around the clock (24/7/365), manned network operating center (NOC) to support all vendor roles and responsibilities related to the ongoing and successful use of the awarded solution. Such services include but are not limited to application software administration and security, product software updates, upgrades, updates, and patches. These services must originate and be maintained within the continental United States.

234. Vendor must provide a toll-free telephone number for MDEQ 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. In addition to live telephone support, other acceptable formats for technical support are web-based live chat and email.

235. 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.

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

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

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

239. Vendor's Cost Information Submission, Section VIII of this RFP, must specify costs to provide the proposed support on an annual basis for up to three years.

C. Issue Tracking

240. The Vendor shall use an industry standard tracking system to thoroughly document issues and requests for MDEQ.

241. Describe how operational trouble issues (unrelated to hosting) are submitted, prioritized, tracked, and resolved.

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

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

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

245. The Vendor shall provide a customer portal for MDEQ to track help desk ticketing and incident resolution.

246. The Vendor must provide a monthly issue tracking report as defined by MDEQ. 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 MDEQ.

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

D. Service Level Agreements

248. The provider shall follow the problem severity guidelines specified in Table 4 for assigning severity levels for incident creation.

Table 4 – Severity Levels for Incident Creation

Priority Level	Description of Deficiency	Resolution Time	Status Updates
1 **Critical**	A problem with the Software which renders the Software inoperative or causes a significant and ongoing interruption to Customer's business activities.	2 Hours	Daily until workaround or correction available.
2 **Severe**	A problem with the Software which degrades or disrupts operation but does not cause a significant and ongoing interruption to Customer's business activities.	4 Hours	Every two days until workaround or correction available.
3 **Moderate**	A problem with the Software which has only a minor impact on Customer's business activities, or for which an acceptable work-around is readily available.	1 Day	As necessary or upon request.
4 **Low**	General questions, suggestions and feedback pertaining to use and operation of the Software.	1 Day	As necessary or upon request.

E. Remedies for Failure to Meet Service Levels

249. Vendor agrees that service credits will accrue for unscheduled application downtime unrelated to hosting, including Vendor's failure to meet application 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 hours/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 5, 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 5, 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 5 will go into full force and effect.

256. In the event of repeated violations of a single SLA measure or multiple failures across SLA measures over two consecutive months, the State reserves the right to renegotiate SLA measures and/or escalate the applicable reductions by 50% of the stated liquidated damages after non-responsiveness.

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

Table 5 – 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

VII. OTHER

A. Additional Requirements

258. ITS acknowledges that the specifications within this RFP are not exhaustive. Rather, they reflect the known requirements that must be met by the proposed solution. Vendors must specify, here, what additional components may be needed and are proposed in order to complete each configuration.

259. If any component necessary for operation of the requested solution is omitted from Vendor's proposal, Vendor must be willing to provide the component(s) at no additional cost.

B. Change Management and Control

260. Vendor must agree that upon award, Vendor will describe, justify, and submit all proposed changes to the agreed upon project deliverables to MDEQ 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.

261. Vendor must describe their change control process. At a minimum, Vendor's process should reveal how change requests will be documented, submitted, assessed, and approved by the State.

262. All change requests require approval by the State prior to implementation. The awarded Vendor and the State will identify the appropriate team members involved in the evaluation and approval of change requests.

263. All approved changes must be detailed and logged by the Vendor and must remain accessible by the State for review online.

C. Change Order

264. After implementation and acceptance of the services procured by this RFP, MDEQ may require additional services, such as enhancements or other system related needs. Vendor must include a fully loaded change order rate as a separate line in the Vendor's Cost Information Submission, Section VIII of RFP No. 4422.

VIII. TABLE OF DELIVERABLES

265. Vendor must agree to provide the deliverables in Table 6 below so that the State can evaluate Vendor capabilities. Preliminary deliverables should be as detailed as possible to show compliance with the specific RFP requirements. Post award, and prior to implementation, Vendor and MDEQ will amend deliverables as appropriate. MDEQ approval is required for all deliverables prior to implementation.

Table 6 - Deliverables

Deliverable/Title
1. Implementation Requirements - Section V
Project Management Plan (PMP) – Item A
Data Conversion Plan (If necessary) – Item B
Data Migration Plan (DMP) – Item C
Acceptance Testing Plan (ATP) – Item D
User Acceptance Testing (UAT Plan) – Item E
User Training and Documentation – Item G
2. System manuals and project documentation - complete and all inclusive.