ATTACHMENT H

SCOPE OF WORK

5.1. Background

The Montgomery County Police Department – Forensic Science and Evidence Management Division consists of a full-service Crime Laboratory offering analysis in the following disciplines: Crime Scene/Blood Pattern Analysis, Electronic Crimes, Firearms, Forensic Biology, Forensic Chemistry and Latent Prints. The laboratory employs over 50 personnel operating primarily at our laboratory located at 100 Edison Park Drive, Gaithersburg, MD, 20878. Our laboratory is accredited by ANSI-ASQ National Accreditation Board (ANAB) and licensed by the Maryland Department of Health, Office of Health Care Quality. Requirements provided by ISO/IEC 17025 as well as the FBI's Quality Assurance Standards guide our laboratory policies and procedures. On average, the laboratory processes approximately 15,000-20,000 items of evidence per year.

5.2. Intent

The County intends to enter into a contract with a single qualified Contractor to provide and install a cloud-based Laboratory Information Management System (LIMS), with technical support and maintenance. The LIMS must be a commercially available, configurable, state-of-the-art application already operational and not under development.

5.3. Scope of Services/Specifications/Work Statement

The County intends to enter into a contract with a single qualified Contractor to provide and install a cloud-based Laboratory Information Management System (LIMS), with technical support and maintenance. The Project Implementation Period begins upon contract execution, and the County requires that the LIMS system be fully operational no later than December 2027. Due dates listing the number of days refers to business days unless otherwise indicated throughout this RFP.

Each requirement below is assigned a number and can be found within Attachment D – Mandatory Requirements. Attachment D is to be completed by the Offeror as a Submission Requirement. If questions arise regarding acronyms or definitions of technical terms, please reference Attachment F – Definitions and Attachment G – Acronyms.

The Contractor's LIMS system must meet the following requirements:

5.3.1. Ability to assign role-restricted access to data (cases, requests, etc.) for internal investigations.

5.3.2. Ability to undo functions on pages to account for accidental user interface errors.

5.3.3. Provide an intuitive and easy-to-use menu structure and screen layout throughout the system.

5.3.4. Ability to use digital worksheets/templates capturing analysis information within each unit to support fully paperless laboratory processes throughout the lifecycle of completing the case request.

5.3.5. Ability to track and report metrics at the unit, analyst and lab wide level for the following but not limited to: service requests accepted and received, backlog of cases, completed cases, number of samples and items examined, number of various types of conclusions reported for samples/items of evidence, turnaround time for all aspects of analysis to include technical and administrative reviews.

5.3.6. Create reports showing evidence inventory for analysts, designated locations, units and lab wide.

5.3.7. Capture data necessary for our laboratory to participate in the Laboratory Reporting and Analysis Tool (LabRAT) to ensure our participation in Project FORESIGHT.

5.3.8. Ensure data is updated daily for accurate reporting and visualization within the dashboard allowing for configurable visualization of accurate statistics.

5.3.9. Ensure the system provides the ability to upload documents or images as case file attachments regarding to chain of custody or case file notations.

5.3.10. Meet the chain of custody requirements: log detailing a chronological trail of what, who, when and how an item of evidence has been handled and must consist of name of individual and not just user ID, locations, date and time. Provide a solution to meet the chain of custody requirements such as data returns from providers that are not an actual physical item of evidence.

5.3.11. Ability to reassign new analysts to opened/not completed cases if necessary.

5.3.12. Ability to block evidence from further exams/units to ensure the proper order of forensic testing is conducted to maximize the item’s evidentiary potential.

5.3.13. Provide immediate notification to user if case identifier already exists in this system prior to creating a new case record.

5.3.14. Require a user password when editing records of custody and a text box required to provide explanation of the change to include audit trail.

5.3.15. Ability to maintain parent/child relationship through chain of custody and then return child items to parent containers if desired while maintaining accurate chain of custody records.

5.3.16. Interface with MCPD’s RMS and evidence management systems to auto populate information such as but not limited to investigator, incident address, agency case number, etc.

5.3.17. Provide a confirmation dialogue box once all information is entered for our submitters so there is a verification step of all the request data prior to submitting.

5.3.18. Ability for users to request analysis on an item previously analyzed by the unit.

5.3.19. Ability for the laboratory to communicate with the case submitter if corrections are needed to the submission prior to its acceptance to avoid having to reject the submission and require the submission to be redone.

5.3.20. Ability to reject evidence or individual items of evidence in a submission along with canned phrases or free text that can be selected depending on the rejection to generate a record for the case and notification provided directly to the submitter.

5.3.21. Ability for submitters and laboratory staff to update case status regarding court dates, assigned attorneys, termination, identify the need for analysis of additional evidence and notification sent to the applicable unit/analyst assigned the case.

5.3.22. Allow for completion of a satisfaction survey, automatically route it to designated individuals, and produce summary reports of survey results across selected time frames.

5.3.23. Allow for the completion of a complaint document, automatically route it to designated individuals, and produce summary reports of survey results across selected time frames.

5.3.24. Ability for the laboratory to send and track mass notifications to our customers involving but not limited to laboratory submission updates or new technologies.

5.3.25. Ability to track reagents/standards by name, lot number assigned, unit and expiration date.

5.3.26. Ability to flag notifications to avoid the usage of an expired reagent.

5.3.27. Ability to track all changes made to a case file with date/time stamp including user ID, what the change was including a reason.

5.3.28. Create barcode labels for reagents and supplies for tracking purposes.

5.3.29. Ability to create authorization and competency templates for each unit that detail the specific testing and equipment the individual is permitted to use for casework.

5.3.30. Ability to prevent instrument use if it is out of compliance with required maintenance or a performance issue is identified.

5.3.31. Ability to track cases that are sent to another laboratory for processing, assigned to a grant and create a manifest to be sent to the outsourced laboratory.

5.3.32. Ability to assign instruments to a specific grant number for tracking purposes for usage.

5.3.33. Ability to track consumables linked to a grant number.

5.3.34. Enable users to develop, update, and track grant-related metrics to ensure compliance with grant award requirements, included but not limited to Capacity Enhancement Backlog Reduction (CEBR), Coverdell and Sexual Assault Kit Testing programs.

5.3.35. Ability to show case record as expunged if required.

5.3.36. Ability to track and prioritize cases based on court dates.

5.3.37. Ability to calculate appropriate evidence hold times and notify individuals if the time has surpassed our set requirement.

5.3.38. Ability to save Case reports in PDF format.

5.3.39. Ability to allow pre-populating drop down fields for canned responses throughout the unit worksheets and reports as needed.

5.3.40. Ability for the laboratory to select if numerical entries are rounded.

5.3.41. Ability to allow results entry manually or electronically. User generating work must have the option to specify whether test results are manually entered or pulled directly from an instrument.

5.3.42. Ability for statistical functions and calculations to be utilized during unit workflows.

5.3.43. Ability to output the analyses using the digital worksheets in all common file formats such as Adobe Acrobat, Microsoft Excel, Microsoft Excel Data Only, CSV, Microsoft Word, and Rich Text.

5.3.44. Provide for batch processing of casework that allows bi-directional communication with applicable unit instrumentation.

5.3.45. Ability to produce case reports which meet ISO 17025:2017 and ANAB 3125 Standards.

5.3.46. Include a title distinguishing the various report types within each unit such as NIBIN Screening or FEU Analysis for example.

5.3.47. Provide for full configurability regarding the content contained within each unit report.

5.3.48. Ability for each draft report to be viewable.

5.3.49. Ability to link discovery/MPIA documentation to a specific case(s).

5.3.50. Ability to assign status of discovery/MPIA requests to individuals and track the status of the request through completion.

5.3.51. Ability to create a testimony review form and assign it to internal and external users for completion. It can then be subsequently routed to designated individuals

as well as provide reports summarizing information contained within for varying time frames.

5.3.52. Ability to track various metrics for testimony such as date and time spent in court, preparation time, wait time, time testifying, etc. but not limited to the examples stated.

5.3.53. Ability to receive evidence electronically from existing Property and Evidence System, TraQ7 to avoid duplicate entry to data fields.

5.3.54. Ability to create equipment inventory for each unit.

5.3.55. Allow the addition of FARO scans to each associated case record.

5.3.56. Ability to work with digital images and allow for annotation as needed.

5.3.57. Ability to perform calculations with results from one field into another field, such as summing individual weights to give a total net weight, calculating a net weight by subtracting the weight of empty packaging from the gross weight of the material and the packaging.

5.3.58. Ability to capture sampling information, when only a subset of the population is tested. For example, one hundred (100) tablets were received, but only three (3) were tested.

5.3.59. Ability for Supervisors to update Drug Constituent tables with new compounds and update any relevant tables that results may be pulled from during analysis.

5.3.60. Ability to integrate with various instruments and software utilized in the analysis such STRmix, CODIS, Qualtrax, CrimePad, Evidence.com etc.

5.3.61. Ability for CODIS hit reporting and associated statistics to be reported for any selected time frames.

5.3.62. Provide for the logging of NIBIN hits as an attachment to the case record and associated items.

5.3.63. Interface with Photoshop for information exchange in designated units.

5.3.64. Provide digital Image annotation tools to include brushes, line/arrow, text, zoom, pan, and rotate.

5.3.65. Maintain original digital image and annotated/edited image separately.

5.3.66. Maintain digital image history showing user, date/time stamps, actions taken (edits, annotations, downloads, Photoshop requests, etc.).

5.3.67. Provide for built-in document scanning functionality for both documentation and digital images.

5.3.68. Ability to distinguish multiple separate requests under the same laboratory number for ease in viewing as well as tracking.

5.3.69. Allow for a passcode for digital evidence to be provided during the generation of a submission request.

5.3.70. Allow different submitters to request submissions for the same item of evidence if needed for parallel investigations.

5.3.71. Ability to enable sequential unmasking throughout the submission and analysis process.

5.3.72. Ability to utilize NLETS datacenters ensuring FBI CJIS policies, standards and guidelines are met.

5.3.73. Provide for Dashboards that are specific to users and are configurable in displaying real-time data and statistics.

5.3.74. Ability to link Safety Data Sheet (SDS) to reagent name and lot #.

5.3.75. Ability to track reagent inventory to manage the consumption, restocking, relocation and disposal.

5.3.76. Ability to automatically decrement supplies/inventory based on usage within a unit, recognize low levels and provide notifications to users.

5.3.77. Ability to auto-flag if case type warrants a case management meeting.

5.3.78. Allow specific macros not included within LIMS to reside in LIMS for use in analysis if needed.

5.3.79. Provide reciprocity when linking cases so that if a case number is linked in one case record, the linked case is automatically added to the other record, include a reason for the linkage and ability to upload a document to multiple cases at one time.

5.3.80. All reports must include the associated chain of custody of the reported evidence and be automatically generated and included with the report to the customer.

5.3.81. Provide the capability to manage (i.e. track, control, plan) the chemical drug standard/reagent inventory - Chemical name, vendor, lot #, molecular formula, molecular weight, schedule, storage conditions, amount received, when received, when verified, for each use, record date, user, initial weight, weight after use, if consumed, date consumed.

5.3.82. Ability to survey applicable customers that received CODIS hits with a configurable template to gather information required by the State annually.

5.3.83. Ability to import and utilize .NIST files (fingerprint images, demographic information).

5.3.84. Provide for electronic signatures and apply it to reports, results and documents as defined by the County.

5.3.85. Allow the County to expand data fields within the database.

5.3.86. Allow County defined fields that are accessible throughout the system.

5.3.87. Support user-friendly data entry with text-editing features similar to standard word-processing software, including grammar and spell check, undo, delete and copy/paste functions.

5.3.88. Produce a Comprehensive Audit Log that allows for the recordation of system activities sufficient to enable the examination of the sequence of activities of an operation, a procedure, or an event in a transaction from its inception to final results. The Audit log must track login attempts, password changes, workflow steps, automatic and manual notifications sent from within the application, as well as additions, modifications, deletions, views, searches, and prints for reports and records in the system.

5.3.89. Allow the County to capture, retain and view images. Formats include but are not limited to BMP, DDS, GIF, JFIF, JPE, JPEG, JPG, PDF, PNG, PSD, PSPIMAGE, TGA, THM, TIF, TIFF, and YUV. The system must allow images to be attached to any record in the system and to be searched and printed.

5.3.90. The LIMS must support the current licensure/accreditation status of our laboratory which is: accreditation by ANSI (American National Standards Institute) National Accreditation Board (ANAB) to ISO:17025 (2017) and compliant with the Federal Bureau of Investigation (FBI) DNA Quality Assurance Standards and licensure by Maryland Department of Health (MDH).

5.4. Contractor's Qualifications

5.4.1. The Contractor must have a minimum of five years' experience working for an agency comparable in size, demographics and population as Montgomery County, Md., engaged in the secure handling of forensic data used by law enforcement. This experience should include, but is not limited to, the implementation, development, ongoing support, and configuration of large-scale, complex forensic Laboratory Information Management Systems.

5.4.2. The Contractor must provide evidence of current contract award of their LIMS within at least three accredited forensic laboratories similar in size to Montgomery County and with equivalent disciplines by providing references from each laboratory demonstrating their experience in forensic data systems and in forensic laboratory information management systems.

5.5. Contractor's Responsibilities

5.5.1. *High Level Requirements*

5.5.1.1. Contractor must acquire, operate, and maintain all hardware, software and network support related to providing the Software as a hosted service and must ensure all hardware and software is up to date, with the most recent security updates and versions installed and updated as available. The Contractor must establish, maintain, and manage the hosting environment(s).

5.5.1.2. Cloud based applications must be accessible from various client devices through a thin client interface such as a Web browser or a program interface.

5.5.1.3. System must be device adaptable meaning that the application adjusts for iPhone, iPad, computer screen resolution and multiple browsers and is optimized for those devices so that users do not have to scroll left and right or try to use PC based webs screens on a phone. Browers include but are not limited to Google/Chrome, Firefox, Safari, IAE/Edge, etc).

5.5.1.4. Contractor must certify that the proposed cloud environment is and will continue to be compliant with the FBI's Criminal Justice Information Services (CJIS) Security Policy Version 5.8 (or more recent if applicable) dated June 1st, 2019 [CJISD-ITS-DOC-08140-5.8], Criminal Justice Information Services Division, Federal Bureau of Investigation, U.S. Department of Justice. See https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center).

5.5.1.5. Contractor must provide integration with County Active Directory Security (Single sign on). The LIMS system must use single sign on, ADFS, and Group security.

5.5.1.6. Contractor must provide Proactive Production Support Monitoring and alerting of the entire infrastructure deployed in the Cloud, including the secure Network in the Cloud infrastructure at the primary and secondary sites.

5.5.1.7. Contractor must provide a network diagram depicting all the devices, device types, and interfaces that the LIMS will connect to and through, including, but not limited to all blocked ports, hubs, switches, routers, firewalls, and any other network equipment.

5.5.1.8. Contractor must provide detailed architecture of all hardware and software, firmware and versions utilized in managing the Cloud Infrastructure and is responsible for maintaining all of these.

5.5.1.9. Contractor must provide a fully integrated Test environment that is fully functional with interfacing for adequate testing of the entire System as defined by the County. This includes integration into all interfaces, and to a test version of the LIMS. This environment is used by the County to test new versions and or configuration changes.

5.5.1.10. Contractor must provide a fully integrated Disaster Recovery Environment that is fully functional and is an exact duplicate of the Production Environment. This environment must be stood up in minutes and must be

available for Production Use when the Production Environment is compromised, and Failover is required.

5.5.1.11. Contractor must provide a complete replica of the Cloud hosted production database to an on-premises copy or Cloud accessible that is separate and distinct from the Production application. This replica must be an exact replica, leaving no tables out or restricted in any manner for data access. All data and relationships within the LIMS system must be accessible to the County electronically with full access to query the data. The recent data dictionary for the database must be provided to the County and modifications to this core documentation must be provided to the County when made available to Contractor staff.

5.5.1.12. The Contractor may be permitted to utilize services of a subcontractor for specific requirements, such as for Data Visualization, upon written approval by the County, pursuant to the County's General Terms and Conditions. If subcontractors are utilized, the Contractor must address this specifically in their proposal and provide specifics for the areas in which a subcontractor is involved. Use of subcontractors is subject to County written approval.

5.5.1.13. Contractor must provide all access logs of systems upon County request.

5.5.1.14. Contractor must secure manufacturer or provider's standard warranty and extended warranty options for hardware and software provided under the Contract, the details for which must be described in the Offeror's Technical Proposal. Any warranty period for goods and services will not commence until the acceptance of the products or services by the County. Notwithstanding anything to the contrary, all defective items must be replaced at no additional cost to the County.

5.5.2. System Installation – Cloud

5.5.2.1. System installation is one of the early processes in the Project implementation phase and has a significant impact on critical dependency on several key activities. Cloud virtual provisioning will be the responsibility of the Contractor.

5.5.2.2. The administration services of the cloud environment are the responsibility of Contractor, including support, operation, and maintenance of the underlying infrastructure. Access to any resources by the County will not be allowed except through the applications and programmatic connections.

5.5.2.3. Contractor must provide a secure VPN communication between the County and Contractor Cloud Solution, adhering to County Security policies. It is preferred that site-to-site VPN connections between the County and the Contractor Cloud environment be on a dedicated circuit that is not shared with general internet users on the agency side. The Couty will be responsible for their side of the VPN tunnel and Contractor will be responsible for the Cloud side. County and Contractor must work together for implementation and support each other in production incidents.

5.5.3. Contractor's Project Manager

5.5.3.1. The Contractor shall provide a Project Manager who will work with our Project Manager over the life cycle of the project. The Contractor's Project Manager will be responsible for tasks that include, but are not limited to, submitting invoices, providing project status reports, updating the project schedule, identifying risks and issues and providing suitable solutions in a timely manner agreed upon by prior to the project start. The Contractor Project Manager must be dedicated to the County and accessible at all times to avoid delays in the project.

5.5.3.2. The Contractor must provide a full-time Project Manager that is assigned to the Project for the duration of the project. This Project Manager must be available to the County Project manager as needed.

5.5.3.3. The Contractor Project Manager must prepare presentation materials and facilitate the project kickoff meeting where both Project Managers will provide a high-level overview of the project schedule, high level description of deliverables, roles and responsibilities, a preliminary project schedule, and review all project management processes.

5.5.3.4. The Contractor Project Manager must provide a weekly update to the County Project Manager of task completion, delays, issues, and risks so the County can maintain an up-to-date project information weekly.

5.5.3.5. The Contractor Project Manager will provide all Contractor task owners Email and phone numbers.

5.5.3.6. The Contractor Project Manager must provide monthly written status Reports to the County. Status reports must include updates of all major deliverables, work completed the previous month, work to be completed the following month, issues (description, date identified, individuals assigned and date to be resolved), outstanding risks, mitigation strategies and responsible individuals.

5.5.4. Infrastructure

5.5.4.1. Contractor must provide the County with the size of the connection needed to support each environment to ensure that the throughput does not cause any issues. The detail of specification and resulting size configuration will be worked jointly in the first 30 days of the project.

5.5.4.2. The Contractor must provide User Guides and Administration Guides for all licensed software and interfaces purchased by County in electronic format, (native format Word, Excel, PowerPoint, Visio, MS Project) in the first 30 days of the project.

5.5.4.3. Contractor must provide all technical documentation and administration guides on the System to ensure the County has sufficient knowledge to support the infrastructure.

5.5.4.4. The Contractor will provide the application programming interface (API) documentation for any interface under County oversight. The API must document the integration process. API Documentation must be provided within the first forty-five (45) days of the project.

5.5.4.5. Contractor is required to complete a peak volume testing which will force a load condition on the LIMS System from all sources simultaneously. This test will require coordinating security scanning, backup, purging and heavy use load simultaneously to measure how the LIMS system handles the load. This test requires live connectivity across County Networks to identify threshold threats to the processing. The approach will be to coordinate a “shift change scenario” where we have as many end users as possible all log into the system at the same time, while other background processing is occurring on the infrastructure. This test is defined to force the worst possible scenario without any component failures. This test must be performed prior to Go Live.

5.5.4.6. The Contractor must prepare software releases and stage each release in the system testing environment at the County for validation prior to implementing in any production environment. The County will have the ability to manage the timing of the distribution of these releases. (Note: To support this requirement, the Contractor must propose, provide and fully describe their solution for these new software releases).

5.5.4.7. The Contractor may operate in the production environment only upon authorization to operate (ATO) from the County.

5.5.4.8. Contractor must provide all components in its architecture that require licensing and keys that must be managed and updated so there is zero downtime due to a failure to maintain licensing and security. This information must include the vendor, expiration dates, contacts, and any costs and be provided to the County.

5.5.4.9. The Contractor must either provide an Enterprise Service Bus at no cost to the County or utilize the County Enterprise Service Bus. The exact deployment must be determined in the first forty-five (45) business days of the project. These transfers must be established and tested jointly with County and Contractor defining all configuration parameters.

5.5.4.10. Contractor must create and maintain all SSL certificates and licensing for Cloud-based architecture and must provide that information to the County for a secondary tracking mechanism.

5.5.4.11. Contractor must provide infrastructure uptime that allows the Contractor to meet its overall 99.9995% uptime for the services of the LIMS. Services is use of software and not infrastructure uptime. County expects infrastructure to be stable and up.

5.5.5. Acceptance, Maintenance, and Support

5.5.5.1. Contractor must provide the County with the size of the connection needed to support each environment to ensure that the throughput does not cause any issues. The detail of specification and resulting size configuration will be worked jointly in the first 30 days of the project.

5.5.5.2. Acceptance and the Contractor's ongoing maintenance and support obligations are defined as follows:

5.5.5.2.1. Notice of Final Acceptance will be transmitted to the Contractor upon the County's full acceptance of the Contractor's LIMS system, installation and system 'Go-Live.'

5.5.5.2.2. Software maintenance includes all software changes, modifications, updates, patching, bug fixes, vulnerability fixes, and enhancements applicable to all system modules licensed without further charge to all licensed users maintaining a renewable software support contract.

5.5.5.2.3. The Contractor must be responsive in vulnerability issues identified by the County and make all reasonable efforts to remedy the vulnerability in accordance with the County's IT Security Manual. Responsive means meeting County requirements for security compliance.

5.5.5.2.4. Upon notice by the County of a defect with the Software (where defect can be verified), there are reasonable efforts to correct or provide a working solution for the problem.

5.5.5.2.5. Contractor must notify the County of any material errors or defects in the deliverables known or made known to the Contractor from any source during the life of the Contract that could cause the production of inaccurate or otherwise materially incorrect results. The Contractor must initiate actions as may be commercially necessary or proper to effect corrections of any such errors or defects.

5.5.5.2.6. Contractor must notify the County of any vulnerabilities of which it is or becomes aware, that could allow unauthorized access, disclosure, or modification of data, applications, or systems. The Contractor must fix all vulnerabilities in accordance with the County's IT Security Manual (review related section(s) within the County's IT Security Manual AP 6-7 within RFP #1181605 Attachment I.

5.5.5.2.7. Contractor will provide to the County at no additional charge all new releases and bug fixes (collectively referred to as "Updates") for any software deliverable developed or published by the Contractor and made available to its other customers. The County retains the right to accept or reject updates.

5.5.5.2.8. Contractor must have adequate security and detection software and perform scanning and monitoring as part of support. These toolsets must be approved by the County and meet County IT security requirements.

5.5.5.2.9. Contractor Maintenance must not impose any downtime of services on the County. Applications and infrastructure must be maintained with no infrastructure or service downtime. The County expects 99.9995% service uptime, not just infrastructure uptime.

5.5.6. Technical Support and Service Level Agreement

5.5.6.1. The Contractor must provide a Technical Support team member twenty-four (24) hours per day, seven (7) days per week, three-hundred and sixty-five (365) days per year, based on the Tier defined in the Service Level Agreement.

5.5.6.2. Contractor Personnel providing technical support must be familiar with the County's account (i.e., calls must not be sent to a general queue).

5.5.6.3. The County must be notified by email *and* phone by the Contractor of problems encountered at other locations, along with the solution to those problems, when relevant to County software, as soon as known by the Contractor.

5.5.6.4. The Contractor must meet the Response and Resolution/Recovery time requirements defined below in the following table:

Response and Resolution/Recovery Time Requirements Table

Service Priority	**Response Time**	**Resolution Time**	**Response Availability**	**Work Outage**	**Users Affected**
Critical	Less than 15 minutes	Within one (1) hour of first report	24 hours per day, seven days a week, 365 days per year	Major portions of the system are inaccessible. Systems or users are unable to work, or to perform some portion of their job.	Users or internal System functionalities are significantly impaired.
High	Less than thirty (30) minutes.	Within four (4) hours after first report.	24 hours per day, seven days per week.	Major portions of the system are inaccessible. Systems or users are unable to perform a small portion of their job but are able to	Affects the majority of users .

				complete most tasks.	
Normal	Within two (2) hours.	Within one (1) day (24 hours) after the first report. If the outage is not resolved a resolution plan must be in place.	24 hours per day, seven days per week.	Specific non-critical features are not operating as specified. Systems or users are unable to perform a small portion of their job, but are able to complete most tasks.	Affects a number of users.
Low	Within two (2) hours.	Within three (3) days (72 hours) after the first report. If the outage is not resolved a resolution plan must be in place.	24 hours per day, seven days per week.	Lower priority features that can be done manually are not operating as specified. Often a request for service with ample lead time.	Affects a number of users.

5.5.6.5. *Service Level Agreement Pertinent Definitions:*

5.5.6.5.1. *Incident* is defined as the following:
"Any situation or issue or breach or potential breach related to the system operation and is not an enhancement request that is reported to the Contractor. The Contractor must utilize a tracking system, (e.g. help desk ticket system), to track, update, and report the status of all reported incidents."

5.5.6.5.2. *Incident Response Time* is defined as the following:
"The period of time between the reporting of an Incident to the first response/acknowledgement from the Contractor."

5.5.6.5.3. *Incident Resolution Time* is defined as the following:
"The period of time from when the issue was reported to the Contractor to when it is resolved to the satisfaction of the County."

5.5.6.5.4. *Recovery Time Objective (RTO)* is defined as the following:

"The maximum acceptable amount of time for restoring a network or application and regaining access to data after an unplanned disruption."

5.5.6.5.5. *Recovery Point Objective (RPO)* can be defined as the following: "The maximum amount of data loss an organization can tolerate after an unplanned event, typically expressed as the amount of time before the event when data can be recovered successfully. For example, critical operations might have an RPO of zero to one (0-1) hour, while less frequently updated data like specification documents could have an RPO of twelve to twenty-four (12-24) hours."

5.5.6.5.6. *Monthly Charges* can be defined as the following: "For purposes of SLA credit calculation, Monthly Charges are defined as the charges invoiced during the month of the Incident for the monthly fixed services, or, in the event of annual billing, l/12 of the annual invoice amount."

5.5.6.6. *Response and Resolution/Recovery Time Requirements Table*

	Critical Data	RPO/Data Loss Tolerance in hours
Critical Data	Case Records All other areas of the LIMS	0-1
Other Data or Project Artifacts	For example: Equipment Maintenance Items TBD	12-24

5.5.6.7. *Service Level Agreement (SLA) Requirements*

5.5.6.7.1. Complying with all performance measures and must also ensure compliance by all subcontractors. Meet the RTO and RPO times in the event of an unplanned outage or disaster.

5.5.6.7.2. Provide a monthly report to monitor and detail response times and resolution times.

5.5.6.7.3. Log Incidents into the help desk software system shared by Contractor and the County software and assign an initial severity level (i.e., Critical, High, Normal, or Low.)

5.5.6.7.4. Respond to and update all Incidents, including recording when a Incident is resolved and its resolution. Appropriate County personnel must be notified when an Incident is resolved.

5.5.6.7.5. The County must make the final determination regarding Incident severity.

5.5.6.7.6. Contractor must review any Incident with the County to establish the remediation plan and relevant target dates.

5.5.6.7.7. Contractor's Help Desk must incorporate County Service Desk number to facilitate cross reference between the County and Contractor systems. This field must be mandatory, and the Contractor must enforce that a County service desk incident number is provided.

5.5.6.8. *SLA Effective Date (SLA Activation Date)*

5.5.6.8.1. SLAs set forth herein must be in effect beginning with the commencement of monthly services as of the completion of the implementation. If system implementation is done in phases, the SLA will be in effect beginning with acceptance of functionality/module(s)/component(s) included in the first phase.

5.5.6.8.2. Beginning on the SLA Activation Date, for any performance measurement not met during the monthly reporting period, the SLA credit for that individual measurement must be applied to Monthly Charges.

5.5.6.9. *Service Level Reporting*

5.5.6.9.1. The County will monitor contractor performance.

5.5.6.9.2. The Contractor must provide summarized SLA performance and detailed monthly reports evidencing the attained level for each SLA. All monthly reports must highlight any SLA performance criteria that did not meet the compliance requirement designated in the SLA. The Contractor must provide an explanation of why any SLA was not met. For any Incidents that did not resolve the Contractor must provide an explanation of how and when it will be met in the future.

5.5.6.10. *SLA Service Credits*

5.5.6.10.1. Monthly reports must be delivered via e-mail to the Contract Administrator and County Project.

5.5.6.10.2. Beginning on the SLA Activation Date, for any performance measurement not met during a reporting period, the SLA credit for that individual measurement must be applied to the Annual Charges.

5.5.6.10.3. Service credits will be cumulative for each missed service requirement. The County, at its option for amounts due to the County as service credits, may deduct such from any money payable to the Contractor or may bill the Contractor as a separate item. In the event of a catastrophic failure affecting the entire Solution, in addition to all other

rights and remedies available to the County, all affected SLAs must be credited to the County.

5.5.6.10.4. The parties agree that any assessment of service credits must be construed and treated by the parties not as imposing a penalty upon the Contractor, but as compensation to the County for the Contractor's failure to satisfy its service level obligations.

5.5.6.11. *Root Cause Analysis*

5.5.6.11.1. The County has the right, at its sole discretion, to direct the Contractor to perform and deliver a root cause analysis in connection with any SLA measurement that yields an SLA credit. Such root cause analysis must be provided within thirty (30) days of the request.

5.5.6.11.2. In addition, for each 'Critical' or 'High' priority Incident, the affected parties will perform a root cause analysis and institute a process of problem management to prevent recurrence of the issue.

5.5.6.12. *Service Level Measurements Table (System Performance)*

5.5.6.12.1. Service level credits for missed Service Level Requirements apply to the Contract resulting from this Solicitation. Offeror must address the table below with its proposed service level metrics and SLA credits, and must be included in the Offeror's Technical Response.

5.5.6.12.2. The County alone has the unilateral right to reallocate percentages among the various SLAs annually on the anniversary of the Contract, provided that such reallocation will not exceed the cap identified.

5.5.6.12.3. The Contractor must comply with the service level measurements in the following table:

Service Level Measurements Table

	Service Requirement	**Measurement**	**Service Level Agreement (SLA)**	**SLA Credit**
1	Incident Response Time-Critical	Average Response Time for Critical Priority Incidents.	< 15 minutes	1%

2	Incident Response Time-High	Average Response time for High Priority Tickets	< 30 minutes	1%
3	Incident Response Time - Normal	Average Response Time for Normal Priority Incidents	< 2 hours	1%
4	Incident Response Time-Low	Average Response Time for Low Priority Incidents	< 4 hours	1%
5	Incident Resolution/ RTO Time Critical	Resolution/Recovery Time for Critical Priority Incidents	< 1 hour	1%
6	Incident Resolution / RTOTime-High	Resolution/Recovery Time Objective for High Priority Incidents	< 4 hours	1%
7	Incident Resolution / RTOTime-Normal	Resolution Time for Normal Priority Incidents	< 24 hours	1%
8	Incident Resolution / RTO Time-Low	Resolution Time for Low Priority Incidents	< 72 hours	1%
9	Service Availability	All application functionality and accessibility must be maintained at 99.9995% uptime of services performance levels. Contractor	99.9995	2%

		must minimize or eliminate unscheduled network downtime to .5% or less. Planned maintenance is counted as downtime and not excluded from this calculation. Expectation is maintenance requires no service downtime.		
8	Disaster Recovery	Contractor must provide complete recovery and continuity of operations within 24 hours of an outage or disaster, including those requiring a System/network failover. Disaster in this reference is a complete failure in the primary instance that requires remediation beyond the expected near automatic failover of the primary to the secondary environment. Expectation is failover can be completed within minutes, short of a complete disaster.	24 hours	5% at 24 hours and l minute; 5% for every eight (8) hour period after that
9	Notification of Security Incident	Notification of a Security Incident within sixty (60) minutes of occurrence	60 minutes	5%

5.5.6.13. *Security Requirements*

5.5.6.13.1. Contractor Solution must meet County Security Requirements and be reviewed by County per County Administrative Procedures (AP 6-1) as attached in Contract.

5.5.6.13.2. Contractor must participate in security testing. Contractor is required to provide access to the County to perform penetration, scanning and other security testing. Contractor is required to meet County Security requirements and be able to identify security threats to the Cloud infrastructure.

5.5.6.13.3. Security testing is performed early in the testing cycle to identify security threats and allow the project team to address concerns, and again later prior to go live to validate those threats identified have been

mitigated. This testing is performed by the security team and is intended to find deficiencies so they can be corrected prior to go live. Finding issues in this test phase is desired as it is part of the hardening process of the infrastructure. This testing will be executed on the Production Environments and may be executed against the test/staging environments.

5.5.6.13.4. Security testing will be iterative to identify issues, remedy issues, and validate the removal of issues. Montgomery County Security team will attempt intrusion testing into our infrastructure to identify any vulnerabilities that need to be addressed. Security Testing is performed on all environments, with particular scrutiny on the production and disaster recovery environments.

5.5.6.13.5. Contractor must ensure a secure environment for all County data and any hardware and software (including but not limited to servers, network and data components) provided or used in connection with the performance of the Contract according to a written security policy ("Security Plan") no less rigorous than that of the County and using best practices that comply with an accepted industry standard, such as the NIST cybersecurity framework.

5.5.6.13.6. The Security Plan must detail the steps and processes employed by the Contractor as well as the features and characteristics which will ensure compliance with the security requirements of the Contract. Such a Security Plan must be provided to the County for its review with solicitation response. If awarded a contract, the Security Plan must be provided on an annual basis or whenever updates are made.

5.5.6.13.7. To ensure appropriate data protection safeguards are in place, the Contractor must implement and maintain the following controls during the Contract Term (the Contractor may augment this list with additional controls):

5.5.6.13.7..1. Establish separate production and test environments for systems supporting the services provided under the Contract and ensure that production data is not utilized in test or training environment(s).

5.5.6.13.7..2. Apply hardware and software hardening procedures as recommended by Center for Internet Security (CIS) guides, Security Technical Implementation Guides {STIG), or similar industry best practices to reduce the systems' surface of vulnerability, eliminating as many security risks as possible and documenting what is not feasible or not performed according to best practices. Any hardening practices not implemented must be documented with a plan of action and milestones including any compensating control. These procedures may include but are not limited to removal of unnecessary software, disabling or removing unnecessary services, removal of unnecessary usernames or logins, and

the deactivation of unneeded features in the Contractor's system configuration files.

5.5.6.13.7..3. Ensure that County data is not commingled with non-County data through the proper application of compartmentalization Security Measures.

5.5.6.13.7..4. Apply data encryption to protect Sensitive Data at all times, including in transit, at rest, and also when archived for backup purposes. Unless otherwise directed, the Contractor is responsible for the encryption of all Sensitive Data.

5.5.6.13.7..5. Apply data encryption to all Contractor managed or controlled County data when the data is in transit

-

5.5.6.13.7..6. Utilize encryption algorithms for encrypting data that comply with current Federal Information Processing Standards (FIPS), “Security Requirements for Cryptographic Modules.”

5.5.6.13.7..7. Enable appropriate logging parameters to monitor user access activities, authorized and failed access attempts, system exceptions, and critical information security events as recommended by the operating system and application manufacturers and information security standards.

5.5.6.13.7..8. Retain the aforementioned logs and review them at least daily to identify suspicious or questionable activity for investigation and documentation as to their cause and remediation, if required. The County must have the right to inspect the logs and the Contractor or subcontractor's performance to confirm the effectiveness of these measures for the services being provided under the Contract.

5.5.6.13.7..9. Ensure system and network environments are separated by properly configured and updated layer seven firewalls.

5.5.6.13.7..10. Restrict network connections between trusted and untrusted networks by physically or logically isolating systems from unsolicited and unauthenticated network traffic.

5.5.6.13.7..11. Security by default "deny all" and only allow access by exception.

5.5.6.13.7..12. Review, at least annually and after changes, the aforementioned network connections, documenting and confirming the business justification for the use of all service, protocols, and ports allowed, including the rational or compensating controls implemented for those protocols considered insecure but necessary.

5.5.6.13.7..13. Perform regular internal and external vulnerability testing of operating system, applications, and all network devices utilized in this Contract. Such testing is expected to identify outdated software versions; missing software patches; device or software misconfigurations· and to validate compliance with or deviations from the security policies applicable to the Contract. Contractor must evaluate all identified vulnerabilities for potential adverse effects on security and integrity and remediate the vulnerability no later than 30 days following the earlier of vulnerability's identification or public disclosure, or document why remediation action is unnecessary or unsuitable. The County must have the right to conduct vulnerability testing and inspect the results of similar Contractor performed vulnerability testing to confirm the effectiveness of these measures for the services being provided under the Contract.

5.5.6.13.7..14. Enforce strong user authentication and password control measures to minimize the opportunity for unauthorized access through compromise of the user access controls. At a minimum, the implemented measures should be consistent with the most current County Information Security Policies, including specific requirements for password length, complexity, history, and account lockout.

5.5.6.13.7..15. Ensure County data is not processed, transferred, or stored outside of the continental United States ("U.S."). The Contractor must provide its services to the County and the County's end users solely from data centers in the U.S. Unless granted an exception in writing by the County, the Contractor must not allow Contractor Personnel to store County data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. Contractor Personnel may access County data remotely only as required to provide technical support and with the prior approval of the County.

5.5.6.13.7..16. Ensure Contractor Personnel must not connect any of their own equipment to County IT assets without prior written approval by the County. Any such approval may be revoked, rescinded, or curtailed at any time for any reason. The Contractor must coordinate requests for approval with the Contract Administrator and is subject to all County approval processes as they may be revised from time to time.

5.5.6.13.7..17. Ensure that anti-virus and anti-malware software is installed and maintained on all systems and end points supporting the services provided under the Contract that the anti-virus and anti-malware software is automatically updated; and that the software is configured to actively scan and detect threats to the system for remediation. The Contractor must

perform routine vulnerability scans and take corrective actions for any findings.

5.5.6.14. *Data Backup and Disaster Recovery*

5.5.6.14.1. Unless specified otherwise, throughout the Contract term, the Contractor must maintain or cause to be maintained disaster avoidance procedures designed to safeguard County data and other confidential information, Contractor's processing capability and the availability of hosted services. Any force majeure provisions of the Contract do not limit the Contractor's obligations under this provision.

5.5.6.14.2. The Contractor must have robust contingency and disaster recovery (DR) plans in place to ensure that the services provided under the Contract will be maintained in the event of disruption to the Contractor/subcontractor's operations (including, but not limited to, disruption to information technology systems), however caused.

5.5.6.14.3. The Contractor must furnish a DR site. The DR site must be at least one hundred (100) miles from the primary operations site and have the capacity to take over complete production volume in case the primary site becomes unresponsive.

5.5.6.14.4. The contingency and DR plans must be designed to ensure that services under the Contract are restored after a disruption within twenty four (24) hours from notification, with a recovery point objective of one hour or less prior to the outage in order to avoid unacceptable consequences due to the unavailability of services.

5.5.6.14.5. The Contractor must test the contingency/DR plans at least twice annually to identify any changes that need to be made to the plan(s) to ensure a minimum interruption of service. Coordination must be made with the County to ensure limited system downtime when testing is conducted. At least one (1) annual test must include backup media restoration and failover/fallback operations at the DR location. The Contractor must send the Contract Administrator a notice of completion following completion of DR testing.

5.5.6.14.6. Such contingency and DR plans must be available for the County to inspect and practically test at any reasonable time, and subject to regular updating, revising, and testing throughout the term of the Contract.

5.5.6.14.7. The Failover and Recovery Testing is a multiday test where the infrastructure is failed to the disaster Recovery Site to allow the County to verify that all business functionalities can be performed from the Disaster Recovery site, all interface processing is intact, and the failover activities allowed the County users to recover from the failover without data loss. The County will run on this environment for a period of time as negotiated with Contractor, and then the recovery plan will be executed. This fail forward to the Production systems will also validate full business functionality and interfacing is achieved with no data loss upon recovery to

the primary site. Any issues will be documented, rectified and the test scheduled for repeat, until the Failover and recovery can be performed in a manner that protects the County and County processing. When this has been completed, the County will sign off on the Disaster Recovery Plan which includes failover and failback, as well as key business indicators for stable processing. This occurs after the Contractor indicates they are complete with the build and configuration of the system. This is interactive testing, and results will be logged as issues that need to be addressed in order to move into further testing cycles. The contractor must support this test period in order to meet the deliverable of a proven Disaster Recovery contingency plan and must provide the Disaster Recovery Plan to the County.

5.5.6.14.8. The Contractor must provide remote support and guidance for the duration of this testing. Script sign-off is a precursor to administration of the Disaster Recovery Test.

5.5.6.14.9. County leads the testing, and Contractor must assist if County needs guidance.

5.5.6.14.10. Contractor must detail the backup technology and strategy in their proposal and articulate how this solution will meet County RPO and RTO.

5.5.6.14.11. Establish snapshots as defined by the County that allow the county to go back to a Point in time. This must meet County RPO objective.

5.5.6.14.12. Perform routine backup verification to prove backup and restoration of services is fully functional and provide proof of exercise and success to the County.

5.5.6.14.13. Perform backups of the web, application, and database servers per service levels.

5.5.6.15. *Data Ownership and Access*

5.5.6.15.1. The Contractor may not access County data other than as necessary to perform the services under this Contract.

5.5.6.15.2. The Contractor must limit access to and use of County data to Contractor Personnel whose responsibilities require such access or use and must train such Contractor Personnel on the confidentiality obligations set forth herein.

5.5.6.15.3. At no time must any data or processes - that either belong to or are intended for the use of the County or its officers, agents or employees - be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the County.

5.5.6.15.4. The Contractor must not use any information collected in connection with the services furnished under the Contract for any purpose other than fulfilling such services.

5.5.6.15.5. Provisions in these sections must survive expiration or termination of the Contract. Additionally, the Contractor must include the provisions of this section (or the substance thereof) in all subcontracts.

5.5.6.16. *Employee Identification and Criminal Background Check*

5.5.6.16.1. Provisions in these sections must survive expiration or termination of the Contract.

5.5.6.16.2. The Contractor's staff that have access to the County data and County facilities are subject to the Police Background Check requirements.

5.5.6.16.3. The County Contractor Administrator reserves the right to reject any candidate based on County Background Check Results.

5.5.6.16.4. Contractor Personnel must display his or her company ID badge in a visible location at all times while on County premises. Upon request of authorized County personnel, each Contractor Personnel must provide additional photo identification.

5.5.6.16.5. Contractor Personnel must cooperate with County site requirements, including but not limited to, being prepared to be escorted at all times, and providing information for County badge issuance.

5.5.6.16.6. Contractor must remove any Contractor Personnel from working on the Contract where the County determines, in its sole discretion, that Contractor Personnel has not adhered to the Security requirements specified herein.

5.5.6.16.7. County Is Responsible for Background Checks.

5.5.6.16.8. A criminal background check for any Contractor Personnel with access to any County system containing PII must be completed prior to each Contractor Personnel providing any services under the Contract.

5.5.6.16.9. The Contractor resources are subject to Criminal Justice Information System (CJIS) County and federal criminal background check, including fingerprinting, for all Contractor Personnel on the project before they can begin work.

5.5.6.17. *Source Code Escrow applies to the Contract.*

5.5.6.17.1. *Source Code Escrow Package is defined as the following:* *"*A complete copy in machine-readable form of the source code and executable code of the software licensed to the County." and,

*"*Complete instructions for compiling and linking every part of the source code into executable code for purposes of enabling verification of the completeness of the source code as provided below.

5.5.6.17.2. The Offeror selected for the contract award must consent to a source code escrow agreement established by the County, or the County must approve any source code escrow agent/agreement provided for on behalf of the County by the Offeror that the County will become a party to.

5.5.6.17.3. If the County will be required to sign any agreement directly with the Escrow Agent, Contractor must work with the County to: (1) select an Escrow Agent in accordance with County Procurement Regulations; and (2) negotiate any modifications to the agreement needed to comply with County laws, regulations and policies.

5.6. County's Responsibility

5.6.1. *County's Responsibility for LIMS*

5.6.1.1. County's Project Manager is the principal County contact who will manage a team of County Project personnel. The County's Project Manager will maintain a collaborative relationship with the Contractor Project Manager to facilitate clear communications and maintain the project schedule.

5.6.1.2. County is responsible for the infrastructure within Montgomery County Network including the communication to and from Contractor connection point, the backups and the security of any on-premises infrastructure server and the communication for VPN (County Side).

5.6.1.3. The County will provide information to Contractor staff on network infrastructure, including any firewalls within the overall network that the system will operate and necessary port access for the system to operate in accordance with the Design.

5.6.1.4. County will provide remote connectivity to Contractor.

5.6.1.5. The County LIMS Administrator will oversee implementation by the Contractor of the LIMS.

5.6.1.6. County will conduct background checks of applicable Contractor employees.

5.7. Reports/Deliverables

5.7.1. *Communication*

5.7.1.1. For every deliverable, the Contractor must request the County Project Manager's confirmation receipt of that deliverable by sending an e-mail identifying the deliverable name and date of receipt.

5.7.1.2. Unless specified otherwise, written deliverables must be compatible with Microsoft Office, Microsoft Project or Microsoft Visio within two (2) versions of the current software version. At the Contract Administrator's discretion, the Contract Administrator may request one hard copy of a written deliverable.

5.7.1.3. All documents for review and/or approval between both parties are subject to be returned to the other party within five (5) business days of receipt unless mutually agreed to extensions. Payment milestones may require further review in the County. In this instance, ten (10) business days will become the default timeline for return of the identified documents in the case that an alternate timeframe has not been agreed to.

5.7.1.4. The Contract Administrator will issue to the Contractor a Notice of Acceptance or rejection of each deliverable formally in writing. The Contractor must include the signed acceptance with invoice submission to receive payment.

5.7.1.5. In the event of rejection, the Contract Administrator will formally communicate in writing any deliverable deficiencies or non-conformities to the Contractor, describing in those deficiencies what must be corrected prior to acceptance of the deliverable in sufficient detail for the Contractor to address the deficiencies. The Contractor must correct deficiencies and resubmit the corrected deliverable for acceptance within the agreed-upon time period for correction.

5.7.1.6. Contractor must provide the County with the reports of Contractor executed performance testing in their lab for each release provided.

5.7.1.7. Contractor must provide SOC1 and SOC2 audit Reports annually.

5.7.1.8. Contractor must provide the Hardware Specifications for the Infrastructure for review and approval by the County.

5.7.2. *Project Management Plan Reports and Deliverables*

5.7.2.1. The Contractor must produce a Project Management Plan in Microsoft Word that outlines the project goals, the processes to be executed, and how they will be monitored and controlled to accomplish these goals. The Project Management Plan outlines the scope, budget, resources, goals, timeline, communications matrix, risk register, and project deliverables. This plan must be agreed to and baselined and may in conjunction with the Project Schedule baseline constitute a payment milestone.

5.7.2.2. The initial delivery initial delivery must occur within forty (40) business days of the Notice to Proceed, and it must be updated monthly, with approval from the County Project Manager.

5.7.2.3. The contractor must collaborate with the County to provide the Project Management Plan within twenty (20) business days of Contract Signature. This includes but is not limited to Configuration Management, Roles and

Responsibility (RASCI), Risk Management Plan, Change Management Plan, and Quality Management.

5.7.2.4. The Contractor must deliver to the County a Configuration Management Plan that can be used for the project implementation of any future software re-installation or upgrades. The County and Contractor must approve the Configuration Management Plan. Both parties must adhere to the Configuration Management Plan.

5.7.2.5. Contractor must collaborate with the County to provide a RASCI chart outlining roles and responsibilities between organizations and with specific resources and present that at the kickoff meeting.

5.7.3. User and Administration Guides

5.7.3.1. The Contractor must provide User Guides and Administration Guides for all licensed software and interfaces purchased by County in electronic format, (native format Word, Excel, PowerPoint, MS Project).

5.7.3.2. The Contractor must provide the Standard System User Guides as a Microsoft Word document providing instructions that assist Department Personnel in the daily use and administration of the Offeror-furnished system.

5.7.3.3. The Contractor must provide the Standard System Administration Guides as a Microsoft Word document providing instructions that assist Department Personnel in the daily use and administration of the Offer-furnished system.

5.7.3.4. The initial delivery of the Standard Users and Administration Guides is upon onset of project and is updated as needed until final acceptance.

5.7.4. Project Budget Overview

5.7.4.1. The Contractor must provide the total budget broken down into phases/modules/or some other agreed-upon structure to show monthly spend against budget including variance.

5.7.5. Risk Register

5.7.5.1. The Contractor must provide a Risk Management Plan descriptive listing in Microsoft Excel, of risks and issues identified by the Offeror, quantified and calculated, and mitigation strategies for each risk.

5.7.6. Business Process Analysis

5.7.6.1. The Contractor must provide a Microsoft Word, Excel, and/or Visio document that describes the various County business processes in place (as is) and workflows that describe how the Offeror's proposed solution will support or enhance those current processes (to be).

5.7.6.2. The Business Process Analysis must have an initial delivery of input into the Design Phase and must be updated incrementally as needed, and the final delivery 90 days prior to the start of the Final Acceptance Period.

5.7.7. Interface Specification Document

5.7.7.1. The Contractor must provide a Microsoft Word document that provides both technical and functional details about how the proposed LIMS Solution will communicate with other County required systems, data to be transferred and logic for any selection, filtering, and processing for each interface.

5.7.7.2. The Interface Specification Document must have an initial delivery prior to the start of build-design specification needs to be approved and document maintained until final delivery signoff. This document must include test plan and expected results for the interface.

5.7.8. Deployment Plan

5.7.8.1. The Contractor must provide a Microsoft Project Document or Excel document that includes all activities and tasks that are included in the Go Live deployment and post Go Live of the LIMS solution, with decision point milestones to proceed or halt the implementation, and the failback recovery should the implementation be halted and fall back is triggered. The backout plan must be as detailed as the implementation plan to ensure the County is able to fall back completely with no service issues. This plan must include a detailed project schedule with all tasks, timelines, dependencies, and owners defined.

5.7.8.2. The Deployment Plan must have an initial delivery prior to the end of the Training/Test phase and must be updated incrementally as needed with the final version delivered prior to the start of the solution deployment.

5.7.9. Test Plan

5.7.9.1. The Contractor must provide a Test Plan. The Microsoft Word document must explain the test strategy, objectives, schedule, provides detailed test cases for the test resources to use, deadlines, and outlines the resources required to complete testing.

5.7.9.2. The Test Plan must have an initial delivery prior to the start of the Testing/Training phase and must be updated incrementally as needed with the final version delivered prior to the start of the solution deployment.

5.7.10. Test Cases and Test Summary Reports

5.7.10.1. The Contractor must provide a Microsoft Excel Sheet with all Test Cases, steps to execute, and expected outcomes. That allows for entry of pass/fail at each step and any step failed is considered a failure. This sheet calculates the pass/fail for each test case and has a summary sheet of all testing and test cases that is automatically updated as test cases are completed.

5.7.10.2. The initial delivery must be prior to the start of the Testing/Training phase. This document includes all business process testing and all interface testing and must be updated incrementally as needed. The final version must be delivered prior to the start of deployment to be used again as part of Go Live Ready Test Cycle.

5.7.11. Training Plan

5.7.11.1. The Contractor must submit a Training Plan. The Training Plan must detail the strategy that will be used to train the County on the Software and the System. It must include instructional analysis items, which take into consideration items such as needs/skills analysis, adoption, and development approach/materials. It must also include instructional methods and resources which take into consideration: training methodology, training environment needs, resource/facility needs, schedules, evaluation, and addressing any ongoing refresher training needs.

5.7.11.2. The Contractor will provide various levels of training agreed upon with the Project Manager of the County, but not limited to, Administrator level training for at least three individuals, Power User training for at least one individual within each discipline, Internal user training for all individuals using LIMS and finally an External user training for our customers such as officers and attorneys.

5.7.11.3. The Training Plan must have an initial delivery six (6) weeks prior to the start of training.

5.7.12. Training Manuals

5.7.12.1. The Contractor must provide one master set of training documentation in PDF (soft copies) and Microsoft Word to allow the County to print additional copies for staff and make edits to customize the documents at their discretion. The Training Manuals must account for all aspects of the System and all interfaces.

****NOTE: The Contractor must provide documentation for all infrastructure, software, license software and interfaces purchased by County in electronic format, (native format Word, Excel, PowerPoint, MS Project). ****