Attachment A

to

RFP 4383

ITS Project No. 46354

Technical Requirements

OIG/OC Case Management Solution

TABLE OF CONTENTS

TABLE OF CONTENTS

I. GENERAL

A. How to Respond

1. Beginning with Section C, Item 15 and through Section VII, Item 348 of this attachment, 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.
8. Where an outline point asks a question or requests information, the Vendor must respond with the specific answer or information requested.
9. In addition to the above, Vendor must provide explicit details as to the manner and degree to which the proposal meets or exceeds each specification.
10. 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 all mandatory requirements are subject to immediate disqualification.

B. General Overview and Background

11. The Mississippi Department of Human Services (MDHS), Office of the Inspector General (OIG) is responsible for investigating and collecting over-issued payments for various programmatic divisions including *Child Care*, *SNAP*, *Temporary Assistance for Needy Families* (TANF), *Low Income Home Energy Assistance Program* (*LIHEAP*), *Community Services Block Grant* (CSBG), *Weatherization*, and our subgrantees. Federal mandates and state statutes require MDHS to investigate, conduct hearings, and recoup any improper payments made to MDHS clients or subgrantees. These OIG functions are conducted through the Internal Audit Division, Investigations Division, Administrative Hearings Division, and Benefit Recovery Unit
12. The MDHS Office of Compliance (OC) is responsible for conducting fiscal and programmatic monitoring of MDHS subgrantees who receive funding through federal grants to administer specific programs, conducting quality control reviews

of MDHS programs, tracking, and resolving client and stakeholder complaints. The fiscal and programmatic monitoring functions are conducted by the Division of Monitoring. Such services include tracking, auditing, recovery of overpayments, reporting, hearing participation, and/or referral to OIG Benefit Recovery or Investigations Divisions. The federal programs include Child Care, SNAP E&T, TANF, LIHEAP, CSBG, Weatherization and Aging. The OC is also responsible for conducting quality control reviews of all programs to ensure eligibility and other requirements have been met. These programs include SNAP, Child Support, Child Care, Aging, Youth Services, LIHEAP, CSBG and TANF eligibility. These functions are conducted by the Programmatic QC and SNAP QC Divisions. The Division of External Affairs tracks and responds to client and stakeholder complaints.

13. Both the OIG and the OC rely on internal, manual processes for comprehensive case management activities including intake, audit, quality control, investigation, resolution, and compliance reporting. Manual case tracking processes are incapable of meeting current process management, tracking, and reporting needs. MDHS OIG and OC intend to select a single vendor who can provide a proven solution that is already being used effectively in environments of similar size and complexity for similar purposes. MDHS OIG and OC intend to select a vendor with a proven record of outstanding system design, customization, implementation, data migration, user training, customer support, and system maintenance.

14. MDHS OIG Divisions will conduct investigations and hearings, and initiate recoupment actions based on fraud tips received by MDHS OIG. MDHS OIG currently receives approximately 50 fraud tips daily with approximately 82% being related to the SNAP federal program. The current manual process for fraud tip intake and case initiation does not provide efficient workflows to prioritize tips and manage cases in a timely manner.

C. Procurement Goals and Objectives

15. MDHS OIG and OC seek to replace current case management processes with a commercial, full-featured, cloud-hosted solution that will eliminate manual in-house processes. MDHS OIG and OC seek current technologies, including browser neutrality and mobile access.

16. MDHS OIG and OC seek a single Vendor capable of implementing, hosting, supporting, and maintaining a case management solution that will meet the requirements of this RFP.

17. MDHS OIG and OC seek a single Vendor who can successfully transition from current manual case management processes to the awarded solution. Expectations include but are not limited to:

    a. Vendor must be capable of replicating and/or enhancing current MDHS OIG/OC workflows and case management processes so that OIG remains capable of fulfilling current program requirements. MDHS OIG/OC considers current program requirements and workflows to be typical to investigative audit, quality control reviews, and fund recovery cases.
    b. Vendor must maintain the integrity of the independent databases used by the MDHS OIG/OC.
    c. Vendor must successfully migrate all existing MDHS OIG/OC data to the awarded solution. Examples of existing data sources are Smartsheet, iManage, SharePoint, and OneDrive. Examples of data to be migrated are

case documents, case exhibits, and/or case attachments from Federal Fiscal Year 2018 to current.

18. At a minimum, MDHS OIG and OC case management expectations include but are not limited to:

    a. Proposed solution must allow authorized users to prioritize, track, and retain all relevant information regarding case initiation and general case management, audits and investigations, quality control reviews, overpayment recovery, and other associated activities;
    b. Proposed solution must accommodate case prioritization, task assignment/re-assignment, and customized workflows;
    c. Proposed solution must include extensive tracking and reporting on all MDHS-OIG/OC case management activities.

19. MDHS OIG and OC require a solution that will manage and track the case management process from the initiation of a case through its entire life cycle. MDHS OIG requires a solution that will offer a robust document management solution that will make it easy for all users to generate, access, and archive a variety of transactional documents required by the case management process.

20. MDHS OIG and OC require a solution that will offer robust reporting functions, including canned and ad hoc reports.

D. Statement of Understanding

21. MDHS OIG/OC staff will use the solution to analyze and investigate programmatic fraud, track, and analyze subgrantee monitoring reviews, track and analyze programmatic and SNAP quality control reviews, track and analyze client and stakeholder complaints, generate reports, monitor risk factors, as well as other case management duties inherent to the MSDH OIG/OC.

22. The terms MDHS, OIG/OC, and State may be used interchangeably.

23. Because of the limitations of the current manual case management system, the requirements of this RFP seek to address currently known case management and technological deficits. OIG and OC expect the COTS product proposed by the Vendor to represent the best practices and technologies currently available in case management solutions, whether or not a particular feature or function is specifically required by this RFP.

24. MSDH OIG and OC share many common case management needs, and each office may have distinct requirements, workflows, and business needs. Vendor's solution must be configurable to accommodate such needs and awarded Vendor agrees to take OIG and OC specific needs into account upon design and implementation.

25. The State will consider proposals for Vendor-hosted solutions, including government cloud service providers.

26. For vendor-hosted services, a sample software license and application service provider agreement is included in RFP No. 4383, Exhibit A.

E. Current Environment

27. OIG/OC case management information is housed in Smartsheet, iManage, Mississippi Application, Verification, Eligibility, Reporting, & Information Control (Known as MAVERICKS or MAVS), Client Application Registration System (CARS),

Mississippi Enforcement and Tracking of Support Systems (METSS)*, Virtual Roma**, Jobs Automated Work System (JAWS), MAGIC***, Child Care Payment System (CCPS) and any other database that is utilized by the MDHS Programmatic Divisions to administer the programs.

*METSS is an automated child support system utilized by the Division of Child Support Enforcement.

**Virtual Roma (VR2) is a data collection and client tracking system for the Division of Community Services. This system processes applications for Weatherization, Low Income Home Energy Assistance Program (LIHEAP), and Community Services Block Grants.

***MAGIC is the statewide accounting and procurement system of record (SAP Product).

28. Current OIG/OC case management information is comprised of a Smartsheet cloud solution, iManage, and data housed in databases that support specific DHS programs.

29. MDHS OIG/OC casework typically investigates criminal and administrative matters. OIG/OC case information is sensitive and confidential and is subject to controlled access as determined by OIG/OC.

30. Vendor must acknowledge the approximate quantitative reference information provided for sizing and costing in Table 1 below.

Table 1

Source	OIG	OC
	File Size	File Size
Worksite	24.5 GB	24.5 GB
Smartsheet	300 GB	300 GB*
*Represents historical data from approximately 40 users.		

F. Vendor Qualifications

31. **MANDATORY:** Vendor must be in the business of providing vendor hosted, cloud-based case management solutions of similar size and complexity. Preference will be given to vendors who have worked with public entities charged with the full spectrum of investigation and recovery of improperly used public funds. Vendor must have provided such cloud solutions within the last three years.

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

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

34. 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).

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

36. The Vendor must agree that under no circumstances shall any data or equipment associated with this project reside outside the continental United States. However,

a foreign company from outside of the state or outside of the United States can respond to this RFP as long as it has met all legal requirements to conduct business in Mississippi. With regard to the IRS 1075 language and the FTI, the foreign corporation would need to meet those requirements and MDHS would need to certify initially and annually that the Vendor understands policies for safeguarding FTI and how to handle the reporting of unauthorized disclosures and data breaches.

G. Vendor Implementation Team

37. 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 (include names and resumes) of who will be responsible for the execution of the various aspects of the project including but not limited to: Project Manager, Development Team, Business Analyst(s) and Technical Architect(s).
    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.

H. Regulatory Compliance

38. Vendor's solution must support compliance with monitoring, review and reporting applicable to federal and state requirements cited at 2 CFR200,7 CFR 210-299, 45 CFR 300-399, 45 CFR 96.

II. Hosting Requirements

A. Cloud Service Provider – FedRAMP Moderate Baseline Controls

39. **MANDATORY**: The solution must be hosted by a Cloud Service Provider (CSP) that is FedRAMP Moderate Impact Level compliant. The spreadsheet containing FedRAMP Moderate Baseline Controls can be found at the following hyperlink, which was active at the time this RFP was published. If the link is no longer active, Vendor is responsible for accessing and complying with the FedRAMP Moderate Impact Level Baseline Controls. See FedRAMP Moderate Baseline Controls at https://www.fedramp.gov/documents-templates/. Vendor must submit validation that the proposed CSP is FedRAMP Moderate Impact Level compliant.

40. The awarded Vendor must provide a valid third-party security assessment at NIST 800-53 Rev 5 Moderate Impact Level Controls prior to receiving any PII data from MDHS. Vendor must respond indicating if obtaining this assessment is attainable.

41. Vendor must agree that all data stored with the proposed solution must be subject to all data privacy laws including but not limited to NIST 800-53 Rev 5, USDA FNS Handbook 901 Section 9, OCSE IM-17-01, NIST Privacy Framework v1.0, State of

Mississippi Enterprise Cloud and Offsite Hosting Security Policy (included below), and NIST SP 800-122.

42. The solution provider must agree to a third-party audit of the provider's security practices and controls by MDHS on demand.

B. State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy

43. For hosted services, the proposed solution must be compliant with the State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy;

    a. For access to the State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy, send an email request to Bill Brinkley@its.ms.gov. Include a reference to this RFP requirement as justification for your request.

C. State of Mississippi - ITS Off-Site Hosting Requirements

44. The ITS off-site hosting requirements are presented below. Should a conflict exist between the State of Mississippi and the required FedRAMP requirements, Vendor shall adhere to the more restrictive requirements.

45. Data Ownership - The State shall own all right, title and interest in all data used by, resulting from, and collected using the services provided. The Vendor shall not access State User accounts, or State Data, except (i) in the course of data center operation related to this solution; (ii) response to service or technical issues; (iii) as required by the express terms of this service; or (iv) at State 's written request.

46. Data Protection - Protection of personal privacy and sensitive data shall be an integral part of the business activities of the Vendor to ensure that there is no inappropriate or unauthorized use of State information at any time. To this end, the Vendor shall safeguard the confidentiality, integrity, and availability of State information and comply with the following conditions:

    a. All information obtained by the Vendor under this contract shall become and remain property of the State.
    b. At no time shall any data or processes which either belong to or are intended for the use of State or its officers, agents, or employees be copied, disclosed, or retained by the Vendor or any party related to the Vendor for subsequent use in any transaction that does not include the State.

47. Data Location - The Vendor shall not store or transfer State data outside of the United States. This includes backup data and Disaster Recovery locations. The Vendor will permit its personnel and contractors to access State data remotely only as required to provide technical support.

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

49. 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.

50. Breach Notification and Recovery - Unauthorized access or disclosure of non-public data is considered to be a security breach. The Vendor will provide immediate notification and all communication shall be coordinated with the State. When the Vendor or their sub-contractors are liable for the loss, the Vendor shall bear all costs associated with the investigation, response and recovery from the breach including but not limited to credit monitoring services with a term of at least 3 years, mailing costs, website, and toll free telephone call center services. The State shall not agree to any limitation on liability that relieves a Vendor from its own negligence or to the extent that it creates an obligation on the part of the State to hold a Vendor harmless.

51. Notification of Legal Requests - The Vendor shall contact the State upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require access to the data of the State. The Vendor shall not respond to subpoenas, service of process, and other legal requests related to the State without first notifying the State unless prohibited by law from providing such notice.

52. Termination and Suspension of Service - In the event of termination of the contract, the Vendor shall implement an orderly return of State data in CSV or XML or another mutually agreeable format. The Vendor shall guarantee the subsequent secure disposal of State data.

53. 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.

54. 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 according to National Institute of Standards and Technology (NIST) approved methods. Within this 90-day timeframe, Vendor will continue to secure and back up State data covered under the contract.

55. 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.

56. 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.

57. Background Checks - The Vendor warrants that it will not utilize any staff members, including sub-contractors, to fulfill the obligations of the contract who have been convicted of any crime of dishonesty. The Vendor shall promote and maintain an awareness of the importance of securing the State's information among the Vendor's employees and agents.

58. Security Logs and Reports - The Vendor shall allow the State access to system security logs that affect this engagement, its data, and/or processes. This includes the ability to request a report of the activities that a specific user or administrator accessed over a specified period of time as well as the ability for an agency customer to request reports of activities of a specific user associated with that agency. These mechanisms should be defined up front and be available for the entire length of the agreement with the Vendor.

59. Contract Audit - The Vendor shall allow the State to audit conformance including contract terms, system security and data centers as appropriate. The State may perform this audit or contract with a third party at its discretion at the State's expense.

60. Sub-contractor Disclosure - The Vendor shall identify all of its strategic business partners related to services provided under this contract, including but not limited to, all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Vendor, who will be involved in any application development and/or operations.

61. Sub-contractor Compliance - The Vendor must ensure that any agent, including a Vendor or subcontractor, to whom the Vendor provides access agrees to the same restrictions and conditions that apply through this Agreement.

62. Processes and Procedures - The Vendor shall disclose its non-proprietary security processes and technical limitations to the State so that the State can determine if and how adequate protection and flexibility can be attained between the State and the Vendor. For example: virus checking and port sniffing — the State and the Vendor shall understand each other's roles and responsibilities.

63. Operational Metrics - The Vendor and the State shall reach agreement on operational metrics and document said metrics in the Service Level Agreement. At a minimum the SLA shall include:

    a. Advance notice and change control for major upgrades and system changes
    b. System availability/uptime guarantee/agreed-upon maintenance downtime
    c. Recovery Time Objective/Recovery Point Objective
    d. Security Vulnerability Scanning

D. Contingency Planning/Continuity of Operations/Disaster Recovery

64. Vendor must agree that prior to implementation, Vendor will provide a Continuity of Operations and Disaster Recovery Plan (COOP/DR) designed to meet the State's COOP/DR contingency planning requirements. The State will rely upon the NIST SP 800-53, Rev. 5 recommended contingency planning guidelines to set the minimum requirements of the plan. Proposing vendors may view the contingency planning excerpt from NIST SP 800-53, Rev 5 which is posted on the ITS website by name below the RFP No. 4383 documents. The excerpt is titled *CP Control Family NIST.SP.800-53r5.*

65. Vendor must acknowledge that the minimum components of the referenced NIST requirements include but are not limited to documentation of policies and procedures, contingency training/testing, alternate storge and processing sites, telecommunications services, system backup, recovery and reconstitution, and alternate communication protocols.

66. Vendor agrees to work with the State to define and document critical processes, recovery point objectives, recovery time objectives and other mission critical aspects related to continuity of operations and recovery of case management solution functionality and database content.

67. So that the State can evaluate Vendor's ability to provide COOP/DR services, Vendor must submit with the proposal, a preliminary Continuity of Operations/Disaster Recovery plan for review by the State. The plan can be a preliminary plan designed for OIG/OC or a sample plan used for an implementation of similar size and scope. Sample plans can be redacted for confidentiality.

68. The COOP/DR plan must be approved by the State prior to implementation and final acceptance.

E. Application Software Administration and Security

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

70. The solution must integrate with the MDHS Azure SSO and allow for the creation and administration of role-based access controls by MDHS.

71. Solution must provide controlled access to features and functions by configurable, role-based permissions as defined by MDHS OIG/OC.

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

73. Solution must prevent unauthorized access to the system.

74. Solution must accommodate administrator user rights to any and all workflows and tasks as determined by MDHS OIG/OC.

75. Authorized MDHS OIG/OC staff must be able to restrict specific user groups from being able to view or print certain types of documentation.

76. Solution must prevent users from permanently deleting records.

77. Authorized MDHS OIG/OC staff must be able to change a record status to inactive.

78. Authorized MDHS OIG/OC staff must be able to hide a record and/or related documentation from general view.

79. Authorized MDHS OIG/OC staff must be able to assign rules for data entry and validation rules for all entry points. Authorized MDHS OIG/OC staff must be able to add, edit, and delete rules.

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

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

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

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

84. Solution must accommodate two-factor authentication.

F. Product/Software Updates

85. 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 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
        3. All security updates comply with any applicable FedRAMP Moderate Impact Level Baseline Control requirements. https://www.fedramp.gov/documents-templates/

    b. System Maintenance;

    c. System Enhancements;

    d. Education and Training.

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

87. Once available, Vendor must provide at no additional cost 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.
88. Vendor agrees that maintenance services will also include maintaining compatibility of the solution software with any and all applicable contractor provided interfaces.
89. 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.
90. 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.
91. 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.
92. Enhancements and updates must be included with annual maintenance fees. Vendor must include the related cost in Section VIII, Cost Information Submission.

G. Backup Services

93. The Vendor must be able to configure, schedule, and manage backups of all the data including but not limited to files, folders, images, system state, databases, document management system, and enterprise applications.
94. The Vendor must maintain backup system security and application updates.
95. All backup services must comply with any applicable FedRAMP Moderate Impact Level Baseline Control requirements. https://www.fedramp.gov/documents-templates/
96. The Vendor must provide hosted backup options.
97. The Vendor must encrypt all backup files and data and must manage encryption keys. At a minimum, the backup options must encompass a strategy of daily incremental and weekly full backups. All instances must include options for snapshots and backups of snapshots.
98. The encrypted backup should be moved to another geographical region. Regardless of the method of backup, weekly full backups must include system information. OIG/OC minimum retention requirement for all backups is 30 days. Backup retrieval must be started within two hours of notification from OIG/OC. Vendor must monitor all disaster recovery instances, including replication and instance performances.
99. Solution must be capable of running backup reports on a weekly basis, or whatever sequence is required by OIG/OC. For example, report should reveal which jobs successfully completed, which jobs failed, and which jobs restarted, etc.

100. For backup reporting, solution must be capable of on-demand as well as auto-run reporting.

101. The Vendor must be willing to provide backups on demand related to database changes for development, production, or emergency situations.

102. Vendor must describe internal processes for periodic testing of backup services to ensure that they continue to work as required. Be specific about how backups are tested and proven to be successful. Describe vendor processes for reviewing and solving problems that occur during backups.

103. Vendor must provide an on-call technical person to consult with OIG/OC to review and approve any remedial measures to correct problems encountered during backup.

H. Patching

104. The Vendor must provide patching capabilities for all OIG/OC systems. Patching must cover all Microsoft and non-Microsoft vulnerabilities.

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

106. The Vendor must provide OIG/OC with a list of patches to be applied before each patching event.

107. From time to time, OIG/OC 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.

108. All patches must comply with any applicable FedRAMP Moderate Impact Level Baseline Control requirements. https://www.fedramp.gov/documents-templates/

I. System Monitoring

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

    a. Network connectivity within the confines of the provider (i.e., whether the network is up or down, and real-time bandwidth usage);
    b. Full stack application monitoring;
    c. Services running on the operating systems;
    d. Performance indicator;
    e. Network latency;
    f. Utilization (e.g., memory, disk usage);
    g. Trending (for minimum of one year);
    h. Sharing of the monitored data with OIG/OC through a portal;
    i. High Availability—provider must have capabilities to detect failover to another region or availability zone in the event OIG/OC workload and services failover; and
    j. Vendor must provide detailed examples of how it has integrated alerts that are triggered by monitoring technologies into their support processes

III. FUNCTIONAL/TECHNICAL REQUIREMENTS

A. General

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

111. Solution must provide administrative functions that identify user roles, user access, and the ability to set user role restrictions, etc. Must integrate with Azure AD for authentication.

112. Solution must include a calendar function for scheduling applicable workflow actions, such as deliverables, due dates, notifications, and should export to Office 365 calendar.

113. Solution must provide user access to in-progress cases to view records, attach required documentation, determine status, and satisfy pending requirements, etc.

114. Solution must provide sorting functionality to sort the list of open cases by several options including but not be limited to county, date assigned to investigator, date entered into system, investigator assigned for administrator access, and status of case for administrator access (e.g., claims, investigations, hearings, etc.)

115. Solution must be configurable to assign a unique identifier to every case, using OIG current numbering structure. An example of OIG case numbering structure is: FR 19 03 0400. FR represents Fraud, 19 represents year, 03 represents month, and 0400 is a sequential, system-assigned number.

116. Solution must be configurable to accommodate in-take processes as defined by OIG/OC. For instance, OIG/OC must be able to assign cases manually or automatically based on OIG/OC defined criteria. The solution must allow the assignment of multiple users per case.

117. Solution must be configurable to assign a unique identifier to case specific, Child Care, Child Support, LIHEAP, TANF eligibility.

118. Solution must auto-generate case numbers but must also accommodate manually assigned case numbers.

119. Solution must provide real-time information to all modules so that data is immediately available for use in all functions, including reports. Solution must provide ad-hoc report building to create flowcharts, line graphs, bar graphs, pie charts, heat maps, and other report types by dragging and dropping system fields into a report template.

120. Solution must allow comments or notes to be added to case records and attachments.

    a. Solution must ensure that notes or comments added to a record can only be edited or deleted by the originator or another authorized user.

    b. Solution must provide a method of managing and cataloging frequently used notes.

121. Case records must accept attachments from authorized users and/or OIG/OC staff. Document formats included but are not limited to all Microsoft Office Formats, .pdf, all photo formats, including JPEG, TIFF, .GIF, PNG, and all common audio/video formats.

122. Solution must provide data import and export capabilities. The formats should include CSV, JEG, JPG, PNG, Audio, Video, and files in any text format.

123. Solution must have tracking functionality for each case file containing the entire history of the investigation and a complete audit train of each case.

124. Solution must accommodate context sensitive messaging, error messaging, help, and instructions to OIG/OC staff. Solution must support typical Microsoft Office functions such as cut, copy, paste, etc.

125. Proposed solution must provide familiar keyboard shortcuts such as those common to Microsoft Windows applications.

126. Solution must allow the viewing of multiple projects and screens simultaneously, along with the ability to minimize and resize windows as needed. Solution must also provide Dashboard reports using maps, charts, and other graphics to display combinations of results for comparison and analysis.

127. Solution must be customizable for data elements applicable to OIG/OC case management submittal and management actions. Solution must be able to integrate current data bases and/or embedded links to other forms, documents, and websites to reduce duplication of case files. (Refer to Section IV.B. of this document).

128. Solution must allow for an unlimited number of data elements to be associated with cases, e.g., names, aliases, addresses, birth dates, driver license numbers, etc.

129. Data elements must be accessible through dropdown menus, checkboxes, date pickers, etc. to ensure standardization of OIG/OC processes and data collection formats.

130. Solution should have the ability to manage, verify, and apply digital signatures through DocuSign, which is currently used by OIG/OC.

131. Solution should include standard email templates, correspondence templates, and the ability to produce mailing labels based on user defined criteria. For example, OIG/OC must be able to send notifications through US mail, texts to mobile devices and emails through Microsoft 365. Vendor must describe proposed methodologies for providing these functionalities.

132. Solution must provide User Interfaces (UI) to build and manage email or correspondence templates across multiple devices.

133. Solution must allow authorized users to configure and maintain templates and components.

134. Solution must allow templates and components to be cloned and/or deleted by authorized users.

135. Solution must accommodate and accept the migration of current OIG/OC templates. Examples are Microsoft Word documents and generic fill-in Worksite forms in .pdf and excel formats.

136. All case related activities must be trackable and viewable by users for purposes of status and case management.

137. The solution must capture and maintain a chronological history of all relevant case events. Authorized OIG/OC staff must be able to flag cases for configurable reasons, such as inactivity, receipt of documents, and restitutions, etc.

138. Solution must generate task logs for all case management deliverables:
    a. Task logs must reveal daily assigned tasks, task details, task due dates, task status, and all other details pertinent to task management.
139. Solution must provide flexible, configurable time keeping capabilities.
    a. Solution must accommodate time keeping needs expressed by the OIG/OC including the ability to associate time entry statuses with specific workflow processes.
    b. Solution must include flexible output formats such as .pdf and .xls, or any other common format used by the OIG/OC;
    c. Solution must accommodate financial tracking of activities as defined by OIG/OC. Examples are restitutions, fines, fees, court costs, case time, and expenses.
140. Solution must support the management of all person-related activities, case – related activities and all other activities and parties involved in the case.
141. Within the OIG/OC case management database(s), solution must allow OIG/OC to create links between related cases for the purpose of aligning common case activities, common staffing, and common scheduling functions.
142. Within the database, solution must provide conflict checking to flag such conflict occurrences as defined by the OIG/OC.
143. At implementation, the proposed solution must accommodate at least 100 users.
144. OIG/OC must be able to define an unlimited number of additional case types without having to purchase additional modules or capacity. When OIG/OC case types are entered, only relevant codes and values (e.g., events, documents, and status) shall be displayed and available for entry by system users.
145. Solution must allow each OIG/OC defined case type to have distinct OIG/OC defined business rules.
146. Solution must allow for the use of OIG/OC mandatory, agency-specified, fields on all screens.
147. The proposed solution must be able to merge cases. For example, if we receive two separate tips against the same individual involving two separate programs, we need to be able to merge and manage the cases.
148. The solution must allow context sensitive flags to be set for participants.
149. The solution must be able to seal and password protect certain case documents.
150. Solution must allow unlimited number of case types to be configured.
151. Proposed solution must also be able to track overpayment recoveries and support accurate recovery reporting to meet MDHS Federal financial reporting requirements. Examples are FNS Form 366B and FNS Form 209, along with any other Federal reporting requirements.
152. Solution must have the ability to categorize a case with multiple case types such as investigations, fraud, and audit, etc.)

B. Access

153. The proposed solution must offer a public facing portal to grant access to OIG defined functions for fraud tip submission. The public facing portal for the solution must be intuitive and easy to navigate. Vendors can view the current fraud submission functionality on the MDHS website at the following link: https://www.mdhs.ms.gov/report-fraud/

154. Solution must be accessible to credentialed IOS and Android mobile devices.

155. Solution must include mobile access/functionality for IOS and Android platforms for use in the field by OIG/OC employees.

    a. Solution must be compatible with Microsoft tablet, Android tablet, IOS and related devices for the current and two immediately preceding versions.
    b. Solution must incorporate mobile case viewing for credentialed users.
    c. Solution must accommodate project management functions on mobile platforms.

156. Vendor must provide end to end data encryption known as *At Rest* or *In Motion Encryption* for case management data accessed by OIG/OC.

157. 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.

158. Solution must provide real-time data exchange with MDHS mobile devices having adequate access.

159. 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.

C. Workflow

160. Solution must accommodate configurable workflows and business rules that are common to best practice case management solutions, regardless of whether or not they are specified by this RFP.

161. OIG/OC case management processes follow prescribed steps, depending on the type of required action. The proposed solution must allow multiple, configurable workflows and processes in accordance with all OIG/OC data driven parameters and established procedures.

162. Solution must provide flexible workflow routing to accommodate OIG/OC processes involving multiple case types with differing workflows.

163. Solution must provide configurable triggers that will initiate event and/or data driven workflow actions that will result in automatic updates to cases.

164. Solution must provide configurable time standards that initiate, and route workflows based on multiple variables such as event aging and failure to comply with court actions. Such events and conditions will be defined by OIG/OC.

165. Solution must allow authorized users to redirect workflows in response to circumstances that require temporary or permanent changes

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

167. Solution must automatically calculate service deadlines; this feature must be configurable.

168. Workflow routing must accommodate, track, and report on due dates as defined by OIG/OC.

169. Solution must distribute case management information and/or tasks to relevant parties simultaneously.

170. Solution must display workflows in simple, graphic formats which are easily understood by system users.

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

172. Solution must allow workflows to be saved as templates to be reused for other types of case management actions.

173. Solution must provide the ability to create and modify workflows using built-in administrative tools.

174. Workflows must be capable of routing case management functional responsibilities to specific staff member work queues.

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

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

D. Document Manager

177. Solution must offer all document management features and functionality common to best practice case management solutions.

178. A vendor's proposal should include the document manager as a part of the solution. MDHS does not plan to implement or manage a 3rd party document manager solution.

179. Solution must offer a document management system (DMS) that accommodates importing, storing, retrieving, manipulating, and editing, scanned and electronic documents.

180. Proposed document manager must provide a robust, organized, and user-friendly document storage and retrieval structure for electronic files and digital evidence. Uploaded and stored electronic file types may include but are not limited to jpeg, pdf, and Microsoft Word, etc. Common forms of digital evidence are images, notes, emails, and audio/video interview recordings.

181. Proposed document manager must accept and upload large gigabyte documents.

182. Solution must accommodate printing and/or exporting of maintained and managed documents.

183. Solution must allow mobile users to upload and attach documents to targeted case management records.

184. Solution must allow permission-based review and editing of documents in the document manager.

185. Proposed document manager must accept the import of migrated documents and other digital assets presently used by OIG/OC for case management processes. Common OIG/OC document formats include but are not limited to all Microsoft Office formats, .pdf, all photo formats including JPEG, TIFF, GIF, PNG, and all common audio/video formats.

186. Based on workflow determined by OIG/OC, proposed solution must provide automatic document routing to appropriate work queues for users and/or automatic response.

    a. Proposed document manager must offer common features as described below. For each feature, indicate if it is supported by the proposed solution:
        1. Customizable case document types;
        2. Customizable flags and meta-data for document types;
        3. Attach multiple file types to case, including proprietary file types;
        4. Viewer for all allowed document file types;
        5. Docs can be searched by file name and metadata;
        6. Docs can be searched by content;
        7. Docs can be searched within a case and across cases;
        8. Docs can be attached to case and linked to events and participants;
        9. User-initiated and system-initiated OCR (optical character reader) of pdfs;
        10. Notification can be sent to users of new document attached to case;
        11. E-signature functionality;
        12. Customizable document retention policies - based on case type;
        13. Docs can be imported from repositories;
        14. Customizable document organization and display, using folders, tags, column sort, views;
        15. Documents can be scanned directly into CMS and OCR'd;
        16. Generated documents can be distributed to multiple people (and system captures/displays whom document was sent to;
        17. Docs can be redacted, and both original and redacted versions saved;
        18. Docs can be saved for cases that are not opened;
        19. Doc title/file name can be modified;
        20. Docs can have "draft" status, and drafts can be modified;
        21. Docs can have "final" status, and cannot be modified;
        22. External users can share docs for attachment to case;
        23. Multiple docs can be printed in a single batch job;
        24. Multiple documents can be attached/copied/printed with a single action, including by drag-and-drop;

25. Document-type pick list should be context-sensitive if need to be confidential in nature or by programmatic division case type for the nine divisions that are administered;
26. Users can bookmark documents;
27. Template-type approach to document;
28. Available and configurable version control;
29. Documents can be accessed offline, consistent with security requirements; and
30. Documents can be annotated within the OIG/OC;

b. For each feature described below, indicate whether or not proposed solution supports the feature:
   1. Attach docs directly from email;
   2. Approval workflow available for generated documents.

E. Search Functions

187. Solution must offer all search features and functionality common to best practice case management solutions, whether or not they are specified by this RFP.
188. 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.
189. Solution must be able to produce search results that represent the search term, as well as subtle variations of the search term.
190. Solution must offer pre-defined searches that would be common to OIG/OC activities.
191. Solution must have search functionality that allows keyword searches within case files as well as the full system data base.
192. Searches must be exportable or downloadable to common file formats such as Excel, .pdf, xml, and csv.
193. Users must be able to save frequently used searches for repeated use.
194. Users must be able to search for items opened or closed during specific time frames along with being able to search matters by case status, investigator assigned, outcomes, and by programmatic divisions.
195. Users must be able to search for upcoming events, deadlines, or other quantifiable parameters as determined by OIG/OC.

F. Reports and Dashboards

196. Solution must offer pre-designed, standard reports common to best practice OIG/OC case management activities, whether or not they are specified by this RFP.
197. Solution must provide all tracking and reporting functionality necessary to meet the mandated reporting requirements associated with OIG/OC activities. Such reports include but are not limited to OIG/OC monthly usage reports for each individual user, FNS-366b, FNS310, and FNS-209.
198. Solution must accommodate the creation and modification of standard reporting templates as defined by OIG/OC.

199. Solution must accommodate user defined reporting for the purpose of creating custom reports from any and all data elements for which OIG/OC requires tracking and/or reporting. User defined reporting tool must be intuitive and easy for the user to comprehend.
200. Solution must provide configurable reporting of all case-related, person-related, programmatic divisions, and event related activities as required by OIG/OC.
201. Solution must provide the ability to save user-generated reports under user profiles.
202. Solution must allow OIG/OC Staff to create and save customized reports and queries.
203. Solution must be capable of exporting reports into several file formats including but not limited to .pdf, MS Excel, MS Word, and common audio/video formats including, MP3/MP4.
204. Solution must be able to distribute reports through the workflow as email attachments.
205. Solution must provide configurable dashboards that can be customized to serve the needs of individual users.
206. Solution must provide configurable dashboards on throughput performance measures and system activities, such as: active users, action items, deliverables, etc.
207. Solution must provide configurable dashboards where all active cases can be viewed along with pertinent case information, such as: case number, outcome of case, recovery amounts, case history, summary, status, and comments. Solution must provide configurable dashboards for users to manage open tasks.
208. Solution must provide configurable executive dashboards.
209. Solution must be able to generate caseload and case status reports.
210. Solution queries must have capability to filter out repetitive results and cases that do not require action.
211. Solution must be able to automatically generate reports on a configurable schedule and distribute them to selected users.
212. For Vendor reference, a document providing examples of existing reports and dashboards that the solution must be able to produce is posted on the ITS website directly beneath the RFP No. 4383 documents. It is titled *Examples of Reports and Dashboards*. These examples are representative and are not all inclusive.

G. Ticklers

213. Solution must provide all tickler capabilities common to best practice case management 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. Ticklers can be viewed within a case and across cases;

e. Authorized users can configure tickler displays, including the ability to set an expiration date;
f. Solution provides a configurable display of a user's unsatisfied ticklers, within a case and across cases;
g. All case ticklers should remain permanently viewable in case view;
h. Satisfied ticklers can be filtered from display, but remain accessible;
i. Provides notification to users of unsatisfied overdue ticklers; and
j. Ticklers can be directed to multiple recipients.

214. If possible, solution should allow:

a. Tickler content to be saved as a case 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

H. Notifications

215. The Solution must provide notification capabilities common to best practice case management solutions, whether or not they are specified by this RFP.

216. Solution must offer configurable notifications and alerts.

217. Solution must auto-generate emails or notifications for OIG/OC for cases assigned to an investigator or analyst role that have not been acted upon by the investigator or analyst at designated configurable intervals from the date assigned. Solution must also auto-generate notification when a new assignment is initiated to an investigator/analyst.

218. Solution must provide email and/or correspondence templates for notification purposes.

219. Solution must notify staff that they have been assigned to a case.

I. Calendar Functions

220. Solution must offer full featured calendar functions that are common to all best practice case management solutions, whether or not they are specified by this RFP.

221. At a minimum, solution must offer calendar functions as described below:

a. Can generate calendars based on CMS data. Calendar event can be sent to Microsoft Office 365 Outlook. If event is updated, Outlook event is automatically updated;
b. Offers configurable meeting notification and event fields display;
c. Calendars can be shared with participating entities, as determined by OIG/OC;
d. Calendars are exportable and sharable (such as .ICS [iCalendar]);
e. Events can be display in calendar style;
f. Cancelled hearings can be excluded from calendar report;
g. Users can subscribe to calendar events; and
h. Can consume OIG/OC hearing dates and check against hearing date in CMS.

J. Audit Functions

222. The solution must offer common audit trail functions inherent to best practice case management 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 case type;
    c. Ability to set audit retention schedule based on data type or case type;
    d. Ability to audit user activity including but not limited to logins, logouts, and changes within a record, number of cases assigned, number of active cases, number of cases closed, number cases substantiated, and number of cases unsubstantiated.
    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.
223. For tracking and audit purposes, solution must assign unique identifiers to all users.
224. Solution must time stamp all actions taken by users and reflect the activity in the audit trail.
225. Solution must have capability to produce audit trail reports that capture case management user activities.

K. Charges, Dispositions, and Sentencing Information

226. Solution must capture the booking charges, prosecuted charges, and their related disposition (filed, declined, modified, etc.).
227. Solution must allow multiple defendants to be entered into one case and allow each defendant to be charged separately or in one indictment.
228. The solution must track the complete history of charges as amended throughout the case.
229. The solution must provide drop-downs for entry of statutory violations, descriptions, charging language, class or severity, possible sentences, and effective dates.
230. The solution must capture the charges upon which a defendant is sentenced and the disposition of each charge and of the case.
231. The solution must capture the parties to the disposition and sentence (attorneys, judge, other).
232. The solution must capture probation and probation conditions.
233. The solution must capture arrest/indictment information as well as sentencing information.

L. Evidence, Electronic Discovery, and Case Documents

234. The solution must accommodate, manage, track, and report on all evidentiary and discovery activities, documents, and outcomes common to best practice case management solutions, whether or not they are specified by this RFP.
235. The solution must allow the accumulation of large discovery documents, files, and images, etc. into a packet that can be date stamped and electronically and securely disclosed to others as determined by OIG.

236. The solution must allow discovery to be brought directly into the CMS from multiple repositories and stored within the system.

237. The solution must allow notes to be flagged as discoverable/not discoverable.

238. The solution must allow authorized users to organize and catalogue large volumes of documents used as evidence.

239. Solution must allow evidence and exhibits to be added to cases at any time, while maintaining a chain of custody by tracking locations, dates, times, and custodians in possession of such materials.

240. Solution must allow images of evidence to be attached as needed for use as proxies during hearings.

M. Pre-Trial Intervention/Diversion Programs

241. The system must be capable of tracking user defined pre-trial diversion programs such as defendant history and related cases.

242. The system must provide the ability to track fines and restitutions associated with these programs, both single payments and multiple payments over time, and capture a history of the date payments were made.

N. Archival

243. Solution must archive case management historical documents as determined by OIG/OC. For example, different OIG/OC programs may have differing archival requirements. Solution must be configurable to accommodate.

244. Solution must be configurable to comply with variable OIG/OC retention schedules, the longest of which is seven years.

245. Solution must alert staff when retention period is about to expire and when it has expired.

246. Authorized OIG/OC staff must have access to all archived records for viewing and/or printing.

IV. IMPLEMENTATION

A. Project Management Plan and Integrated Master Schedule

247. MSDH desires to implement the proposed solution as rapidly as possible after contract execution. So that MSDH can assess Vendor's ability to successfully implement the proposed solution, Vendor must submit a preliminary Project Management Plan (PMP) and timeline of not more than 12 months from execution of a contract, 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.

248. 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.

249. 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.

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

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

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

253. Vendor must identify any potential risks, roadblocks and challenges that have been encountered in similar implementations that could negatively affect a timely and successful completion of the project. Vendor must recommend a high-level strategy that to mitigate these risks.

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

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

B. Integrations and Interfaces

256. Some OIG/OC case management practices require interaction with data sources that are external to the case management solution. Such interactions are presently done through existing ESB and/or APIs. Proposing Vendor must be capable of replicating and/or providing these interactions. Vendor must describe proposed methodologies and provide examples of other implementations that prove Vendor's capabilities to interact with applications external to the case management solution.

    For example, proposed solution must interact with active MDHS legacy systems or Windows SQL databases such as MAVS, eFITS, Virtual Roma, CCPS, METSS, and any other external sources necessary to meet Federal/State compliance requirements.

257. Solution must be able to query SQL databases.

258. Solution's calendar function must interface with Microsoft Outlook 365.

259. Solution must offer configurable, flexible, and searchable calendar views for all case related activities and users.

260. Solution must be able integrate with existing case management databases and manual tools to eliminate having to manually recreate current and historical data elements in the awarded solution. If solution is not able to integrate with existing resources, then Vendor must convert and migrate as necessary to build the CMS, OIG and OC databases with current and historical data at no additional cost.

261. Costs for integrations and interfaces should be provided at no additional cost to the State.

C. Conversion and Migration

262. Vendor must successfully migrate all existing data housed by OIG/OC present case management tools as quantified in Table 1 of this document. A .pdf sample of Worksite document types and file sizes is posted by name on the ITS Website below the RFP documents. The document is named *Conversion and Migration of Data Usage for Worksite.*

263. Vendor must convert all existing customer system data from the resident CMS to the awarded solution including but not limited to assigned case number, investigator, persons involved, case status, case notes/narrative, and property involved. Supporting attachments must accompany converted records as appropriate.

    a. Vendor must sign a confidentiality agreement with the State prior to access to data.
    b. Vendor must present a detailed conversion plan for the State's approval prior to commencing conversion processes.
    c. Vendor must present a detailed data cleanup plan for the State's approval prior to commencing the process.
    d. Vendor must identify any required fields not currently populated by the resident system and a method to supply the same to the awarded solution.
    e. Vendor must provide verifiable, statistical information, such as record counts to prove the successful conversion of legacy data.

264. Vendor must acknowledge and agree that OIG/OC 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.

265. 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 OIG/OC.

266. 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.

267. 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.

D. Data Migration Plan

268. So that OIG/OC can assess Vendor's ability to migrate and map OIG/OC 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.

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

270. Vendor must be specific about the proposed methodology, tools, data, personnel and other resources required for the migration and mapping. Regarding personnel and other resources, Vendor should be specific about whether the resources are

supplied by the Vendor, OIG/OC, or other. Vendor should keep in mind that OIG/OC has limited available resources

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

272. Vendor must work with the OIG/OC project implementation team(s) to update and modify the preliminary data migration plan as appropriate.

273. Vendor must agree that final data migration and data migration testing plans are subject to approval by the OIG/OC.

274. Vendor will ensure 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.

275. Vendor agrees that before any actual code is written, the mapping specifications and supporting documentation will be clearly understood and approved by MDHS (OIG/OC) prior to migration of data.

276. 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 OIG/OC before any data migration occurs.

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

E. Developing and Test Environments

278. Vendor must agree to host and maintain a mutually agreed upon development and testing environment, including browser-based access, as required for collaboration between Vendor and OIG/OC for all related purposes.

279. Vendor must agree that all such test environments will comply with all State security requirements described in RFP 4383.

280. Vendor must submit a proposed acceptance testing plan (ATP) for review and approval by the State.

281. 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.

F. User Acceptance Testing

282. Once the State approves the written acceptance testing plan (ATP), Vendor agrees to conduct/support OIG 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.

283. So that OIG/OC can assess Vendor's ability to conduct UAT, Vendor must submit with this proposal a preliminary User Acceptance Testing Plan. OIG/OC will accept

a sample UAT Plan from a previous implementation of similar size and scope and Vendor may redact the plan if necessary.

284. At a minimum, the UAT Plan must incorporate the following minimum 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. UAT Test Report; and
    c. Training Materials;

285. At a minimum, the UAT Plan must:
    a. Include both scripts and normal operations to test end-to-end workflows, customizations, and integrations; all OIG/OC 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.
    c. In the user testing environment, all customizations, integrations, and interfaces must be tested and validated.

286. Upon award, Vendor agrees to finalize the preliminary UAT plan with input from the OIG/OC project team.
    a. Vendor agrees that the final UAT plan requires approval from OIG/OC.
    b. Vendor agrees that OIG/OC 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 OIG Final Acceptance Review (FAR).

287. Vendor must agree to regular status meetings with OIG/OC project management team to review progress on UAT.

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

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

G. Implementation and Final Acceptance

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

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

292. Following implementation, the Customer will conduct Final Acceptance of the System. 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 the Customer. 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.

H. User Training and Documentation

293. Awarded Vendor must provide complete user training documentation and keep it updated as appropriate. Web-accessible format is acceptable to OIG/OC for training documentation.

294. Awarded Vendor must provide thorough online tutorial/training geared toward OIG/OC users.

295. Prior to go-live, Vendor must agree to adequately train 25 to 40 OIG/OC 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 the Section VIII Cost Information Submission of RFP No. 4383.

296. Awarded Vendor must train OIG/OC staff users and administrators in the effective use of the document management system.

297. 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.

298. Solution must provide on-line training modules to address system customization that may be performed by OIG/OC authorized users.

299. Awarded Vendor must provide pre-implementation training.

300. 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. 4356, Cost Information Submission.

301. Vendor must be responsible for continual training and support of all system users deemed necessary by OIG/OC for the success of the case management operations and processes for the life of the Agreement.

I. Processes – Case Management Solution

302. The Vendor shall have mutually agreed upon processes and policies in place to support OIG/OC case management operations and processes.

303. Any modifications to the agreed upon policies and processes must receive prior approval from OIG/OC.

304. Such processes and policies must be thoroughly documented.

305. Such processes and policies must be reviewed by the Vendor and OIG/OC at least annually.

V. Warranty, Maintenance, and Support

A. Warranty

306. The warranty period is a one-year period during which the Vendor must warrant, at no cost to OIG/OC, all work performed as stated in RFP 4383 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.

307. 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 OIG/OC has accepted the phase or process as functioning properly and in coordination with any previously implemented phase(s) or process(es).

308. 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.

309. 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.

310. 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.

311. 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

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

313. Vendor must provide a toll-free telephone number for OIG/OC 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.

314. 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.

315. Vendor must keep the appropriate OIG/OC management and technical support staff updated on the status of trouble resolution.

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

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

318. 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 five years.

C. Issue Tracking

319. The Vendor shall use an industry standard tracking system to thoroughly document issues and requests for OIG/OC.

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

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

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

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

324. The Vendor shall provide a customer portal for OIG/OC to track help desk ticketing and incident resolution.

325. Details of OIG/OC environments must be readily available to any authorized support personnel of the provider, including but not limited to architecture diagrams, network connectivity diagrams, service level agreements (SLA), contacts, backups, and monitoring alerts.

326. The Vendor must provide a monthly issue tracking report as defined by OIG/OC. 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 OIG/OC.

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

D. Service Level Agreements

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

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

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

331. The provider shall follow the problem severity guidelines specified in Table 2 for assigning severity levels for incident creation.

Table 2 - Deficiency Priority Levels

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

E. Remedies for Failure to Meet Service Levels

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

333. 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.

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

335. 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 3, Service Credit Assessments.

336. Without limiting any other rights and remedies available to State, Vendor agrees to issue service credits in accordance with the measures prescribed by Table 3, Service Credit Assessments.

337. 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.

338. 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 the Table 3 will go into full force and effect.

339. 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.

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

Table 3 – 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

VI. OTHER

A. Additional Requirements

341. 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.

342. If any components necessary for the successful operation of the proposed solution are omitted from the Vendor's proposal, Vendor must be willing to provide the component(s) at no additional cost. This includes but is not limited to all components necessary for vendor hosting, secure web portals, web application servers, web services, mobile and non-mobile access, mobile and hybrid applications, database/servers, networking, technologies, and support and maintenance of the proposed solution.

B. Change Management and Control

343. Vendor must agree that upon award, Vendor will describe, justify, and submit all proposed changes to the agreed upon project deliverables to OIG/OC 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.

344. 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.

345. 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.

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

C. Cost Proposal

347. Vendor must present proposed costs in the form provided in Section VIII, Cost Information Submission in RFP No. 4383.

D. Change Order

348. After implementation and acceptance of the services procured by this RFP, OIG/OC 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. 4383.

VII. Table of Deliverables

349. Vendor must agree to provide the deliverables in Table 4 below so that the State can evaluate Vendor capabilities. Make preliminary deliverables as detailed as possible to show compliance with the specific RFP requirements. Post award, and prior to implementation, Vendor and OIG/OC will amend deliverables as appropriate. OIG/OC approval is required for all deliverables prior to implementation.

Table 4 - Deliverables

Deliverable/Title
1. Hosting Requirements – Section II
Continuity of Operations/Disaster Recovery Plan (COOP/DR) - Item D
2. Implementation Requirements - Section IV
Project Management Plan (PMP) – Item A
Data Migration IV (DMP) – Item D
Acceptance Testing Plan (ATP) – Item E
User Acceptance Testing Plan (UAT Plan) – Item F
User Training and Documentation – Item H
3. System manuals and project documentation - complete and all inclusive.