Attachment A

to

RFP No. 4635

Mississippi State Department
Of Health (MSDH)

Integrated Disease Surveillance
Platform

Functional and Technical Requirements

ITS Project No. 48420

TABLE OF CONTENTS

I. GENERAL

A. How to Respond

1. Beginning with Item 22 of this Attachment A, 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 to which they disagree.
3. The Vendor must respond with "WILL COMPLY" or "EXCEPTION" to each point in this section. In addition, many items in this RFP require detailed and specific responses to provide the requested information. Failure to provide the information requested will result in the Vendor receiving a lower score for that item, or, at the State's sole discretion, being subject to disqualification.
4. "WILL COMPLY" indicates that the vendor can and will adhere to the requirement. This response specifies that a vendor or vendor's proposed solution must comply with a specific item or must perform a certain task.
5. If the Vendor cannot respond with "WILL COMPLY", then the Vendor must respond with "EXCEPTION". (See RFP Section V, for additional instructions regarding Vendor exceptions.)
6. Where an outline point asks a question or requests information, Vendor must respond with the specific answer or information requested. NOTE: Vendor must be aware that parent verbiage of outlined requirements may or may not require a response.
7. In addition to the above, Vendor must provide explicit details as to the manner and degree to which the proposal meets or exceeds each specification.

B. Mandatory Provisions in Technical Requirements for this RFP

8. Certain items in the technical specifications of this RFP are MANDATORY. Vendors are specifically disallowed from taking exception to these mandatory requirements, and proposals that do not meet a mandatory requirement are subject to immediate disqualification.
9. Mandatory requirements are those features classified as "**MANDATORY**" in this Attachment A. Meeting a mandatory requirement means the Vendor meets the qualifications and experience required and/or requested functionality exists in the base solution.

C. General Overview and Background

10. The Mississippi State Department of Health (MSDH) and ITS are issuing this RFP to secure a qualified Vendor, through competitive procedures, to provide a Public Health communicable disease focused, integrated software solution and implementation services for a comprehensive, statewide, patient-centric Integrated Disease Surveillance Platform (IDSP). The Vendor will configure, implement, and maintain a Vendor-hosted web-based communicable disease reporting and surveillance system that provides MSDH with the required functionality to run and manage the Sexually Transmitted Diseases and Human Immunodeficiency Virus (STD/HIV), Tuberculosis (TB), and Epidemiology (EPI) programs by processing near real-time electronic laboratory results and electronic case records. In MSDH, EPI refers to the General Infectious Disease Epidemiology program. It will also meet all Centers for Disease Control and Prevention (CDC) reporting requirements, allow for manual web-based

reporting, and integrate associated, critical systems such as the MSDH electronic health record system (Epic), geographic information systems, and other mission critical systems (e.g., immunization registry) required for each MSDH program to efficiently manage disease surveillance and response.

11. MSDH considers integrated to mean the IDSP will support the following communicable disease programs in a patient centric, modernized infrastructure: Division of Epidemiology (EPI), Tuberculosis (TB), and Sexually Transmitted Diseases (STD/HIV). The current siloed surveillance systems utilized by the multiple MSDH program/office areas do not allow for a patient-centric approach that supports all public health events for a patient to be viewed from one central location. Functionality that currently exists in the multiple surveillance systems used by the various programs, including manual processes, will be integrated into a single, modernized IDSP infrastructure to support MSDH. A robust IDSP supporting STD/HIV, TB, and EPI will eliminate patient deduplication, decrease missed opportunities due to inaccessible data, increase efficiencies in case investigations, case reporting, outbreak management, contact tracing and reduce effort and cost for on-going maintenance and support.

12. An IDSP will help improve the agency's public health disease surveillance infrastructure to:

    - Increase MSDH disease surveillance efficiencies by facilitating state public health department collaboration, by providing the ability to view MSDH patients in a public health holistic context,
    - Increase MSDH's data analytical capabilities by providing an integrated data repository, which is a hub for infectious disease surveillance,
    - Increase the timeliness of data reporting by reducing the data entry burden on public health professionals,
    - Provide customizable tools such as easily configurable electronic disease data collection forms to quickly respond to emerging diseases,
    - Reduce MSDH manpower requirements by removing the need to support multiple, siloed systems,
    - Increase data availability by, connecting all MSDH disease surveillance programs to laboratories, healthcare providers, and national public health partners, utilizing existing standards,
    - Provide a system that combines technology, standards, and disease surveillance to be used to affect public health regulations and policy, and
    - Shift from paper to electronic data exchanges.

13. The Office of Communicable Diseases is responsible for statewide surveillance and investigation of reportable diseases and conditions. Activities include:

    - Investigation of individual cases and outbreaks of communicable diseases,
    - Collection, and analysis, to identify disease trends, including emerging infections,

- Dissemination of communicable disease information and education and training of public health and healthcare professionals on communicable disease prevention and control, and
- Planning epidemiological strategies/responses – to the occurrence of diseases of public health concern, outbreaks and public health emergencies involving communicable diseases

To support these functions, the IDSP will be used to track disease reports received from hospitals, laboratories, physicians, and other health care providers. The system must be capable of receiving manual key-entered and electronically transmitted disease and laboratory reports, assigning case investigations, tracking workflow, generating management and surveillance reports, and exporting data.

Rules and regulations governing reportable disease and conditions can be found here: MSDH Reportable Disease and Conditions Regulations

A list of notifiable conditions can be found here: Reportable Disease List

The MSDH programs directly impacted by this RFP in the Office of Communicable Diseases are Epidemiology, TB, and STD/HIV.

14. The following table identifies the number of MSDH cases identified and laboratory reports for each program area that the new solution will support and is not reflective of state-wide data. This table does not include COVID-19 data.

Table 1: MSDH Office of Communicable Diseases Cases and Lab Reports (Yearly Range for each year 2020 – 2023)

Program		
	Cases* Identified	**Lab Reports****
Epidemiology	3,500 – 6,000	15,000 – 18,000
TB	50 – 100	400 - 700
STD/HIV	35,000 – 45,000	275,000 – 350,000

*Cases identified are defined as how many cases are reported to MSDH.

**Lab reports are defined as electronic and manual lab reports provided to MSDH.

NOTE: Normal operations may result in exceeding the upper bound of the estimate.

Additional MSDH disease statistics and data can be found at: Home - Mississippi State Department of Health (ms.gov)

a. Epidemiology: The Office of Epidemiology is responsible for monitoring the occurrences and trends of reportable and communicable diseases, investigating outbreaks of diseases, monitoring disease trends and impact on at-risk populations to develop public health measures to interrupt outbreaks or disease occurrences, and reporting trends to the medical community and other target groups. This office also provides consultation to health care providers and the public on communicable diseases and disease outbreaks.

The Office of Epidemiology will benefit from the IDSP, as the integrated and efficient collection and tracking reportable conditions and associated data will ensure:

- Automatic case creation based on Electronic Laboratory Reporting (ELR)/ Electronic Care Reports (eCR), lab test type, and result.
- Prompt investigation of cases of selected reportable diseases to prevent further transmission.
- Analytical capabilities to assist in creation of epidemiological strategies and plans in response to public health emergencies and occurrence of diseases.
- Ability to look at risk factors and data across diseases for commonalities for individuals who have multiple diseases and to target educational and prevention efforts.
- Ensure that household or other close contacts of selected disease cases receive preventive treatment or appropriate evaluation, when indicated.
- Investigate disease outbreaks to identify and eliminate their sources.
- Receipt of HL7 files from participating labs and provide appropriate HL7 messages using CDC HL7 Message Mapping Guides for outbound delivery.
- Determine whether reported cases meet specific surveillance definitions for inclusion in disease statistics.
- Prepare statistical reports and data dashboards.

b. Tuberculosis: Surveillance of TB cases is a key activity for MSDH. The Office of Epidemiology, the TB program will benefit from:

- Automated creation of patient TB records using electronic lab reporting
- A seamless integrated contact tracing tool to link cases and contacts
- The ability to timely track contracts and symptom monitoring allowing quicker initiation of control and prevention measures thereby limiting the spread of the disease in a community
- The ability to know the HIV status of TB patients, and
- Communication with other MSDH Program areas (specifically STD/HIV) regarding patient history and proper treatment.

c. Sexually Transmitted Disease (STD)/Human Immunodeficiency Virus (HIV): The MSDH STD/HIV Program provides screening/testing, surveillance, education, treatment, and partner notification for reportable STDs (syphilis, chlamydia, and gonorrhea) and HIV in the state.

Further benefits of the IDSP to benefit the STD/HIV program is:

- The automation of completion of CDC and MSDH forms.
- The ability to know the TB status of HIV patients; and

- The flexibility of supporting future reporting and form changes as necessary.

15. Epidemic, Pandemic, or Natural/Man-made Public Health Disaster Surveillance and Reporting

    Epidemic, pandemic, or natural/man-made public health disaster surveillance allows MSDH the ability to monitor and track the event as well as educate and inform the public of the appropriate measures for prevention. The IDSP shall have the capability to scale for supporting epidemic, pandemic, or natural/man-made public health disaster surveillance and reporting such as the Coronavirus (COVID-19) pandemic.

    When COVID-19 first presented, MSDH used their existing system to identify and track cases identified throughout the state. However, as the numbers significantly increased over a short amount of time, it became apparent that another solution would need to be used for documenting and tracking the disease. In August 2020, all COVID-19 data began being tracked in the National Electronic Disease Surveillance System (NBS).

    In the event of epidemic, pandemic, or natural/man-made public health disaster, MSDH shall have the ability to use the IDSP for all surveillance purposes without the need for any other system or interruption in service.

    Table 2: COVID Cases and Lab Reports (Yearly Estimates 2020-2022)

Disease / Program		
	Cases Identified*	**Lab Reports**
COVID-19 / Epidemiology	~320,000	~2,800,000

    *Cases identified are defined as how many cases are reported to MSDH.

    Additional information and data reports regarding MSDH's COVID-19 program can be found at: Coronavirus COVID-19 - Mississippi State Department of Health (ms.gov)

16. Prior to the COVID-19 pandemic, there were approximately 500 internal and 250 external users. During the pandemic, there was an increase in the need for disease surveillance user accounts, both internally (approximately 1,200) and externally (approximately 2,800). The systems are available to input infectious disease reports on a 24/7/365 basis for disease control and disease surveillance purposes.

D. Statement of Understanding

17. Attendance at the Vendor Web Conference on Friday, March 14, 2025 at 10:00 a.m. Central Time is optional for any Vendor who intends to submit an RFP response.
    a. To access the Vendor Web Conference, Vendor must contact RFP@its.ms.gov no later than Thursday, March 13, 2025 at 12:00 p.m. Central Time to receive instructions on how to enter into the web conference.
18. Because Ernst and Young U.S., LLP, formerly Cambria Solutions, assisted in the preparation of this RFP Number 4635, they are disallowed from responding to this RFP.
19. Hourly Rates for Change Orders

a. The Vendor must provide fully loaded, onsite and remote, off-site hourly change order rates for each proposed role as well as a fully loaded blended rate. Blended rates shall be used in pricing of any subsequent change orders and will be based on milestones. Fully loaded rates include hourly rate plus travel, per diem, and lodging.

20. Additional Activities Proposed

    a. The Vendor is encouraged to recommend best practices or additional activities that would add value to the project in the RFP response. Any non-required activities which incur additional cost should be priced as an optional line item, separate from the required activities in the RFP response.

    b. MSDH reserves the right to use this procurement instrument to add additional and accompanying services that are in scope of this procurement, should they be needed.

21. Subsequent to Notice of Award and Contract Execution, contract deliverables will be reviewed by MSDH and shall require formal written approval from MSDH before acceptance of the deliverable. The Vendor shall allow for a minimum ten (10) business days following receipt, per deliverable, for MSDH to review each deliverable and document its findings, except as specified by MSDH. Based on the review findings, MSDH may accept the deliverable, reject portions of the deliverable, reject the complete deliverable, or require that revisions be made. The Vendor shall make all modifications directed by MSDH within ten (10) business days of receipt. MSDH reserves the right to make modifications to these timelines and, if needed, will do so in writing with the successful vendor.

E. Vendor Qualifications

22. The Vendor shall provide a detailed narrative describing the background of the corporation that includes:

    a. Date established

    b. Ownership (e.g., public company, partnership, subsidiary)

    c. Location of the principal place of business

    d. Number and location of other satellite offices

    e. Total number of employees

        1. Full-time

        2. Vendors/Subcontractors

        3. Within the United States

        4. Off-shore/Near-shore

23. **overv:** The Vendor shall demonstrate a minimum of one (1) year of prior experience and consistent use in at least one (1) jurisdiction with the proposed system with a local, state, or territorial public health jurisdiction located in the United States, including but not limited to (NOTE: consistent use defined as the jurisdiction is currently utilizing the proposed solution to support their EPI, STD/HIV, and TB programs. Partial usage does not meet the requirement (e.g. the jurisdiction uses the solution for EPI and STD/HIV – but not TB)):

a. Describe how the Vendor has a minimum of one (1) Public Health IDSP project with the proposed system in a State, local, or territorial U.S. public health jurisdiction of similar scope, and complexity, where the jurisdiction is currently using the solution to support all three programs (EPI, STD/HIV, TB) for at least one year.

b. Describe how the Vendor's proposed solution allows jurisdictional users to conduct Epidemiological management of statewide EPI, TB, and STD/HIV programs to include case investigations, contact tracing, outbreak management / response, treatment, required federal and state reporting, and post exposure prophylaxis documentation, etc.

c. Describe how the vendor supported CMS incentive program Public Health Promoting Interoperability supports reporting obligations for electronic laboratory results reporting and electronic case reports.

d. Describe how the vendor conducted the following efforts during the implementation of the Integrated Disease Surveillance Platform:

1. Development/Configuration
2. Legacy disease surveillance system data migration
3. Implementation
4. Ongoing operations
5. Support and maintenance

24. The Vendor shall describe their experience in meeting United States federal and state requirements (e.g. Message Mapping Guides (MMGs), HL7, etc.) that they identified and their timely incorporation into the system. Experience must include the project objectives, timelines, and public health domains (e.g., at a minimum EPI, Tuberculosis, STD/HIV programs). Experience should consider this RFP and provide a rational of why the Vendor has a proven record of success of implementing this RFP's requirements.

F. Staffing Requirements

25. Key Personnel (KP) designated as part of the proposed solution shall remain on the project team for the duration of the project unless a change in team is the result of a request or approval by MSDH in writing. If any key personnel leave the company, MSDH shall review resumes for any key personnel filling of vacancies.

26. The Vendor shall make provisions as needed for personnel to come on-site in Jackson, Mississippi and be available to state personnel at an MSDH facility as determined by MSDH and mutually agreed upon.

a. The Vendor shall provide all hardware, software, transportation, and lodging necessary for Vendor personnel to fulfill the RFP requirements. MSDH can provide minimal office space for on-site staff allowing collaboration between MSDH staff and Vendor staff. MSDH will provide adequate meeting space for the duration of the project.

b. The Vendor shall consider a full business day and make remote and/or on-site staff available during that time of 8:00 a.m. to 5:00 p.m. Central Time.

c. MSDH expects the Project Manager (PM) to adjust on-site schedules to provide elevated coverage at critical times relative to the solutions integration into the MSDH environment. MSDH expects periodic PM on-site presence during key phases of implementation. MSDH also expects a PM presence at steering committee meetings, key status meetings, and other key meetings, upon MSDH request, when provided with a minimum of a two (2) week notice.

d. MSDH expects the Vendor's technical architect be on-site during key phases of implementation. MSDH can request and expects the Vendor to accommodate on-site presence for key stakeholder meetings and other key meetings when provided with a minimum of a two (2) week notice.

e. MSDH expects the Vendor shall propose the on-site availability of the business analysts and public health / solution SMEs assigned to the Project. MSDH anticipates there are times, such as during functional requirements discovery, JADs and planning, and end user training where on-site presence will increase productivity and decrease project risk.

f. The Vendor shall describe in detail how it will collaborate with MSDH to ensure team member remote accessibility and team member on-site commitment.

27. The Vendor shall provide a narrative of relevant experience for all proposed key personnel identified in the proposal. If the proposed individual is not an employee, a letter of commitment to join the project upon award is required.

    a. The Vendor Experience Narrative document is incorporated in the RFP as Attachment B. It must be attached to the resumes describing specific experience with the type of service to be provided within this RFP. The Vendor will be required to describe specific experience with disease surveillance projects and include any professional credentials, licenses, and recent and relevant continuing education.

28. The Vendor shall provide a staffing contingency plan for all Key Personnel, which shall be updated annually, at a minimum.

29. The Vendor shall ensure Key Personnel maintain adequate subject matter expertise in all public health disciplines throughout the duration of the project. Subject matter expertise is defined as personnel with significant experience and knowledge in state, local, and jurisdictional public health systems that impact this project.

30. (KP) Project Executive: For the duration of the entire project, the Vendor shall provide an overall Project Executive once per month for the MSDH monthly Steering Group meetings.

31. (KP) Project Manager (PM) for the proposed IDSP instance(s). The PM shall have the following experience and skill set:

    a. Minimum of three (3) years of experience with a State, local, or territorial United States public health jurisdiction.

    b. Minimum of three (3) years of experience participating in a project related to a public health integrated disease surveillance system, with a State, local, or territorial public health jurisdiction, project as a Business Analyst, Subject Matter Expert, Project Lead, Technical, or other similar role. Other roles proposed to meet this experience requirement will be approved at the sole discretion of MSDH. Vendor must describe how they will meet this requirement.

c. Shall have at least one (1) year verifiable experience leading at least one (1) successful implementation of a public health integrated disease surveillance system, with a larger state, local, or territorial public health jurisdiction, and/or project of similar size, scope, and complexity (multiple entities, systems, data sources, and/or modules) to this multifaceted project. Vendor must describe how they will meet this requirement.

d. Project Management Professional (PMP) Certification

e. Demonstrable knowledge of PMBOK project management theories and practices applicable to highly complex projects.

f. Experience making presentations to high-level executives and stakeholders.

g. Experience providing functional supervision and direction to high-level executives.

h. Experience in providing leadership to staff.

i. Experience in performing complex advanced level research.

j. Experience in identifying project risks, gaps, and providing solutions to complex high-level projects.

k. Proven negotiation and facilitation experience.

l. Experience implementing and using new technology and work processes to enhance decision-making.

m. Experience organizing and presenting information effectively, both orally and in writing.

n. Experience applying independent judgment in making critical decisions.

o. Experience leading and working cooperatively in a team environment.

p. The PM will be responsible for the following:

1. Performing overall project planning (including a detailed project plan in MS Project), project reporting, project management, quality assurance, and documentation as needed or required by MSDH.
2. Managing the overall project in accordance with the project plan.
3. Creating monthly overall status report.
4. Managing team members including the Technical Architect, Business Analysts, Testers, and any support staff.
5. Creating and maintaining Risk and Issue Registers.
6. Supporting the work of any oversight or IV&V Vendor testing, including UAT and validating performance, stress testing and other testing and validation as deemed necessary.
7. Reporting to the MSDH Project Manager and serving as liaison to any Independent Verification and Validation Vendor (IV&V) or Systems Integrator MSDH is using on a project.
8. Attending monthly Steering Group meeting and presenting overall status, issues, and risks to participants.

32. (KP) Technical Architect: One (1) Technical Architect to support the IDSP instance(s), as well as the integration of the solution into the MSDH technical and operational

environment. Experience must clearly demonstrate prior experience such that focus is on MSDH integration, not on the job training.

a. Technical Architect shall have experience in the key areas listed below. An explanation must be provided describing the candidate's specific experience in each key area and supported by the provided resume

    1. Minimum of three (3) years of experience as a technical architect or equivalent role, supporting the proposed system by integrating disease surveillance information technology into an existing public health infrastructure. Vendor must describe how they will meet this requirement.
    2. Minimum of two (2) years of experience with healthcare interoperability. Experience must demonstrate expertise and a working knowledge with SOA, HL7, FHIR, and EHR portability standards and other common healthcare interoperability technologies.
    3. Experience collaborating with both public health and private sector technical teams in defining architectural roadmaps to meet business goals.
    4. Minimum of two (2) years of experience in end-to-end Cloud-based solution design and development.
    5. Experience in systems, hardware, and network design and developments.
    6. Strong, articulate communication skills, including ability to convey the right level of technical detail for multiple audiences (executives, IT staff, policy staff, program support staff, etc.).

b. Technical Architect will be responsible for the following:

    1. Providing technical planning and design of the proposed solution for MSDH programs included in this RFP.
    2. Providing overall technical subject matter expertise.
    3. Providing on-site support during key phases of implementation and
    4. Developing a "big picture" view driven from technical details and identifying "ripple effects" from any organizational technical decisions.
    5. Proficient with public health system interface implementation and interoperability using standard based solutions and protocols such as but not limited to HL7.
    6. Possess expert level knowledge of HL7 and additional interfaces to adequately support the Vendor product and meet all CDC reporting requirements.

33. Business Analyst: One (1) primary or lead business analyst is required.

a. Business Analyst shall have the following experience and skill set:

    1. Minimum of five (5) years of experience with a State, local or territorial public health jurisdiction information technology projects.
    2. Verifiable experience with a State, local or territorial public health jurisdiction integrated disease surveillance system implementation(s) as an Implementation Consultant or a Business Analyst.
    3. Expert level experience with proposed solution as a Business Analyst.
    4. Experience in the development, review, distribution, and presentation of project status reports.
    5. Experience in developing, reviewing, and/or discussing project related deliverables.

6. Experience in documenting and escalating project action items, issues, risks, and/or decisions in timely manner to the client, and other project stakeholders as is necessary.

b. Business Analyst / Public Health SMEs will be responsible for the following:

1. Participate in staff/team meetings and trainings:
2. Provide frequent, clear, and consistent communication to the client, team members, Vendor, and direct reports.
3. Analyze, review, and maintain Vendor and/or client-supplied documentation.
4. Assist in documentation review facilitation, tracking, and maintenance.
5. Perform assigned tasks efficiently and effectively, asking questions when instructions are unclear.
6. Perform responsibilities on-site at the Vendor provided office facility in support of functional requirements discovery, JADs and planning, and end user training (unless otherwise given written approval from MSDH) from Project Initiation until completion of Project Go-Live.
7. Assist the MSDH teams with User Acceptance Testing (UAT) as well as with any changes, updates, patches or fixes as necessary and requested by MSDH relative to meeting requirements.
8. Provide ongoing support to MSDH after Go-Live by monitoring the effectiveness of the product in the MSDH environment.

34. Technical training staff responsibilities:

a. The Vendor shall provide trainers with relevant and appropriate experience dependent on the type of training being conducted.

b. The Vendor shall provide training that will use a combination of on-site in person, as well as web-based training that will provide technical training MSDH on the approach to integration development, functions of the proposed solution, workflows, procedures of proper operation, and reporting and audit logs.

c. The Vendor shall provide detailed training documentation and system documentation for the entire technical solution. All documentation shall be updated on a regular basis, with updates occurring minimally every six (6) months.

d. The training shall be phased over time and location

e. The technical training attendees shall be composed of selected MSDH program staff selected by the MSDH IDSP Steering Committee.

35. The Vendor must provide the appropriate quality and quantity of staff to successfully perform the services described in this RFP. The Vendor shall submit a Staffing Plan to MSDH with their response to the RFP.

a. The plan shall include a team organization chart that clearly defines reporting relationships. The Vendor must provide a descriptive narrative indicating the key staff status, title, roles, and responsibilities of each resource or entity identified. All positions identified on the team organization chart that are not fulfilled by project Key Personnel must include a representative profile that includes qualifications, experience, and education.

b. The plan shall indicate the Subject Matter Expert(s) (SME) assigned to the project and the specific knowledge areas matching the public health areas targeted by this RFP. Each SMEs qualifications, education, and/or training relevant to this project is required. MSDH minimally expects credentialed SMEs in epidemiology, tuberculosis, and STD/HIV to support integration activities into those program areas.

c. The plan shall include a statement and chart that clearly indicates the time commitment of each of the proposed project personnel for each phase. The Vendor will be required to include a statement indicating to what extent, if any, the key project personnel may work on other projects during the term of the contract. MSDH may reject any proposal that commits the proposed key personnel to other projects during the term of the contract if MSDH believes that such commitment may be detrimental to the Vendor's performance or proposed project schedule.

d. The Vendor shall provide an emergency contact list with full contact information for all relevant participants including any commercial partners or Vendors upon whose products or services operations are dependent.

e. The Vendor will have limited office space at the MSDH facilities in Mississippi. Equipment and lifecycle management tools (such as a secure document repository, project software, etc.) as approved by MSDH shall be provided by the Vendor. MSDH is standardized on Microsoft Office, and other Microsoft project software.

f. The Staffing Plan shall include how the Vendor plans to address staffing requirements, project roles and responsibilities with Key Personnel clearly identified, partners, subcontractors, and how changes in staff will be handled through all phases of the project.

36. The Vendor is encouraged to enhance the essential staff with additional personnel in the proposal as they see fit.

37. The Vendor shall provide aid and support to the MSDH Office of Health Information Technology (OHIT) and communicable disease program staff during the transition to the new system. Support shall include availability to answer questions, recommendations for approaches to move from as-is processes into solution processes, technical staff support, and if necessary, refresher or knowledge transfer on areas MSDH staff requires additional guidance.

38. The Vendor shall describe with real company experience, how it adapted and changed in reaction to evolving COVID-19 reporting requirements, reporting volume, system utilization increases, and rapidly changing policy. Include how the company, based on the experience, has changed to better deal with future epidemic, pandemic, or natural/man-made public health disaster.

II. IDSP Functional Requirements

G. User Interface

Data Entry and Searches

39. The Vendor shall provide a solution that supports a user interface that allows users to interact with elements of the system so that MSDH has visibility into the process being used to identify the single best record and its originating source.

40. The proposed solution screens shall be browser based and conform to project approved usability guidelines and is ADA compliant: https://www.ada.gov/resources/web-guidance/

41. The proposed solution shall provide a password secured browser-based user interface with multifactor authentication and capable of supporting SSO with Microsoft Authenticator.

42. **MANDATORY**: Patient Search capabilities.

43. The solution shall provide patient searches capable of finding information.

a. The solution shall allow users to save ad hoc searches as named searches and copy and/or edit existing named searches.

b. The solution shall support ad hoc searches as well as named searches that are available by selection to all users, limited to user groups or individuals/creators.

c. The Vendor shall provide a solution that supports flexible search criteria during the person identification process, for example: partial name, common pseudonyms, Soundex, Social Security Number (SSN), medical record number, encounter number, date of birth, sex, or combinations of data searching and matching on persons stored in the proposed solution.

d. The proposed solution shall provide multiple methods to identify its persons when provided with partial person information, enabling exact and fuzzy match logic.

e. The proposed solution shall have logic that can score returned results ranked by potential matches when a failure to find an exact person occurs.

f. The proposed solution shall support limiting the number of returned matches to avoid excessive number of returned rows based on criteria or rules.

g. The proposed solution shall allow users to provide demographic, diagnostic factors, and identification (IDs) (at a minimum: RVCT Number, Correctional ID (incarcerated patients), Medical Record Number (MRN), lab ID, patient ID, investigation ID, age, race, gender, ethnicity, name, dob, disease name(s), county, case classification, case status, diagnosis date, onset date) that limit results.

44. Search results.

a. The solution shall display search results in a screen (Case Listing Screen) with enhanced functionality.

b. The solution shall, using the Case Listing Screen, provide the ability to directly assign individual or bulk cases to specific case managers.

c. The solution shall, using the Case Listing Screen, provide the ability to directly assign individual or bulk cases to an existing Outbreak.

d. The solution shall, using the Case Listing Screen, provide the ability to change investigation status for individual or bulk cases (e.g. new, active, reviewed, etc.).

e. The solution shall, using the Case Listing Screen, provide the ability to export selected case records into a standard format (CSV, etc.)

f. Searches can be created from the Case Listing Screen and saved by users with appropriate access and can include but not limited to the following elements: specific disease, case manager, case classification (Class 1, etc.), geographic elements (district, county, etc.), and other Core Fields.

g. Saved searches can be accessed and utilized via a dropdown menu.

h. The Case Listing Screen shall have a rapid search capability for individual or multiple patients using patient identifiers, condition name, date of birth,

i. The results list shall support column order changing, re-sorting, hiding columns, showing columns, showing more results, and filtering within the results.

j. Search results shall respect security regarding user role-based record segregation and shall not display record results users would not otherwise have access to.

k. Search results will be sorted and in a paginated tabular list form.

l. Discovery and JAD session will be required. Results will be included in the SOP/Configuration Guide.

45. Data validation on search results.

a. The solution shall have the ability to conduct data validation on search results.

b. The solution shall provide the ability to create, edit, delete, save, and share data validation rules that can be applied to multiple search results.

1. The data validation rules shall identify missing, incomplete, or specific data fields within the search results displaying warning flags or errors for records that are missing or incomplete.

2. The data validation rules shall identify records in the search results that fall outside defined date ranges (e.g. date of initiation vs date of completion), chronological date validation (ensuring proper date sequencing), etc.

c. From the Case Listing Screen, the data validation rules can be applied to search results.

1. Results from applying the data validation rules will be displayed such that records can be directly edited, or data can be updated to resolve the error or warning.

2. Adjudicated records will be removed from the Case Listing Screen.

d. Vendor shall describe any natural language processing or AI supported searching / data validation available with the proposed solution. Any additional costs must be included in the Cost Information Submission as an optional item.

e. Discovery and JAD sessions will be required. Results will be included in the SOP/Configuration Guide.

46. The solution shall allow users to drill-down or open detailed information from the search results.

47. The solution shall have the capability for the user to return or resume a search from the place where the user was prior to navigating into additional or detailed

information. A new search shall not be required, nor shall it be difficult for the user to find the summary row in search results.

48. Uploading documents and images.

    a. The solution shall allow uploading documents and images.

    b. The solution shall support uploaded documents to be found in the context where they were uploaded and will be available for viewing with an appropriate external viewer.

    c. The solution shall associate uploaded documents and images with a patient or a patient disease event or case.

    d. The solution shall support querying of uploaded data.

    e. The solution shall allow users to manage documents, where allowed by roles, during and after upload. This includes assigning types such as a medical record or radiology results, correcting mistakes, removing, reassigning when linked to the wrong record, moving from lower to higher folders within the record, and other typical activities that support document upload, document labeling, and quality control.

    f. The solution shall be capable of managing document upload size, where possible, to balance network capacity, storage limits, and document quality.

    g. Uploaded documents are limited to MSDH viewable formats such as Microsoft formats (e.g., Word, Excel, etc.), PDF documents, and JPEG images.

49. The solution shall allow the end-user to update the patient case, such as, but not limited to, the status of the case from suspected to confirmed.

50. The solution shall allow the end-user to search for and edit a completed (closed) case.

51. The solution shall support user roles such that authorized users can assign/reassign cases to users with appropriate access.

52. Managing districts.

    a. The solution shall define, edit, and manage districts using identifiable geographical boundaries (e.g. counties), to be determined by MSDH.

    b. The solution shall store region definitions that support the manual assignment of cases to workers in districts.

    c. The solution shall determine county using address information and automatically assign disease reports to a district and worker. Automatic assignments can be adjusted and changed by authorized personnel.

53. The solution shall provide the ability for MSDH to define Core Data Fields. (Core Data Fields are defined as common data elements that are collected / used system wide e.g. name, DOB, address, zip code, disease, etc.)

54. Hyperlinks.

    a. The solution shall support adding hyperlinks.

b. The solution shall support linking external systems allowing workers to quickly jump to external systems providing additional or context specific information.

c. Hyperlinks can be functional links such as email links which open the default email application.

55. The solution shall provide MSDH the ability to define drop-down or pick-list defaults.

56. System lists enhanced functionality.

a. The solution shall provide enhanced functionality for all system lists that will be used in the MSDH workflows.

b. The Vendor shall ensure every list supports a default format and configurable default choice.

c. The solution shall support lists with more than one column that are exportable, searchable, filterable, and sortable.

d. The solution shall support lists displaying detailed information about entity data such as person, lab or clinical information to allow direct linking to the entity data.

e. The solution shall allow authorized MSDH program administrative staff to add, edit, and manage disease names available for selection in a patient's case investigation record.

f. Authorized administrative staff can limit which diseases are available to external users.

Surveys

57. Integrated survey capabilities.

a. The solution shall provide integrated public facing online survey capabilities.

58. The solution's survey capabilities shall support seamless integration of surveys with case investigation and outbreak forms (e.g. a survey result can populate an existing case record or create a new case record with minimal manual intervention). Describe how the survey system integrates with the proposed solution.

a. The solution shall support the capability for online survey submission.

1. When the online survey submission is completed, an email notification shall be sent by the system to the person who submitted the response.

b. The solution shall accept multiple email or SMS addresses for bulk sending of survey requests.

59. Survey responses / results.

a. The solution shall support the automated receipt of survey responses.

b. The solution shall have the ability to notify MSDH staff when forms/surveys have been submitted into the solution.

c. The solution shall support a customizable export e.g. allowing MSDH staff to choose specific fields from the survey to export.

d. The solution surveys must support linking surveys / survey results with ongoing epidemiology investigations related to an outbreak or an existing case.

e. The solution shall have the ability for authorized users to create cases from outbreak survey results and populate relevant case data into the case investigation form.

f. The solution shall have the ability to export survey responses in a standard format (e.g. CSV).

60. Survey generation.

a. The solution shall provide a survey generation system allowing MSDH staff to generate a custom survey.

b. The solution shall have availability of common survey capabilities such as multiple questions and varied answer modes such as fill in the blank, selection from a list, radio buttons, checkboxes, single choice, multiple choice, etc.

c. The solution shall have the ability to select and add core data fields as questions on the outbreak surveys.

d. The solution shall have the ability to insert logic. Based on responses to questions, the solution will enable/disable additional questions and can sum values in tables.

e. The solution shall have the ability to perform simple mathematical operations (e.g., addition, subtraction, etc.) in the surveys.

f. The solution shall have the ability to perform calculations in the surveys (e.g., enter the date of birth and the solution calculates the person's age, etc.).

g. The solution shall have the ability to allow authorized users to set time-sensitive parameters (e.g., start/end dates) for completion of a survey

h. The solution shall support surveys that can be saved and can be accessed by external individuals through the public facing web portal.

i. The solution shall have the ability to edit and add new fields to surveys.

j. The solution shall have the ability to perform HTML formatting for field names, labels, read-only text, etc.

k. The solution shall have the ability to allow the user to set fields in a survey as "required".

l. The solution shall provide a means for MSDH staff to send a survey link to individual or multiple / bulk email addresses or SMS device.

m. The solution shall have the ability to allow a survey recipient to utilize one survey link to submit multiple surveys to the solution (e.g., a mother provides her email address and needs to submit three outbreak responses utilizing the one link in her email).

n. The solution shall have the ability to notify MSDH staff when surveys have been submitted into the solution.

o. The solution shall support maintaining a record of when the survey was sent, who the survey was sent to, and the submitted responses for a minimum of seven (7) years.

61. Entering survey data for recipients.
    a. The solution shall allow MSDH staff to enter a survey on behalf of a recipient.
    b. The solution shall allow MSDH staff to gather any information through other means necessary to complete the survey but record the results as if the link recipient filled out the survey.
    c. Survey results shall be maintained as if the recipient filled out the survey but also track as if the MSDH worker entered it.

Forms

62. The solution shall be capable of processing current CDC created case report forms and remain flexible to support future changes and future new forms published or recommended by the CDC at no additional cost to MSDH.
    a. CDC forms shall be protected and can be replaced by newly published CDC forms or altered by authorized staff based on CDC guidelines.
63. The solution shall have the ability for users to search for forms and choose between view, edit, and delete.
64. The solution shall have the ability to manage versioning of forms.
65. The solution shall have the ability to perform HTML formatting for field names, labels, read-only text, etc.
66. MSDH shall have the ability to restrict user ability to edit and delete forms based on form type and user role.
67. The system shall be able to import previously created forms in file types as identified by the agency.
68. Form Templates.
    a. Form templates may be used to create new forms or append to existing forms.
    b. The solution shall allow authorized MSDH program users the ability to create different types of custom forms (e.g., supplemental form, outbreak event forms, and outbreak summary forms).
    c. The solution shall have the ability to allow the user to set fields in a form as “required”.
    d. The solution shall have the ability to add elements in various form types (e.g., Free Text, Dropdown, Multiselect, Check Box, Core Data Question, Field Sets, Table, Label and Read Only).
    e. The solution shall have the ability to set default values for fields as determined by MSDH authorized users.
    f. The solution shall have the ability to enter dates, zip codes, email addresses, time, numbers (with and without decimals), phone numbers.
69. The solution shall have the ability to notify MSDH staff when select disease case report forms have been submitted into the solution.
70. The forms creation screen shall be customizable and user friendly, with the ability to create various sections of a form.

71. The solution shall include common validation and advanced properties in forms creation. (e.g., required fields, cell spanning, label location, format (plain text), and max number of characters.)

72. The solution shall have the ability to insert logic. Based on response to question, the solution will enable/disable additional questions and can sum values in tables.

73. The solution shall have the ability for program system administrators to see change history and revert changes.

74. The solution shall have the ability to promote the form to production and give alerts to the user if the promotion was successful or not.

75. The solution shall have the ability to link certain form types to a specific outbreak.

76. The solution shall have the ability for the user to clear the information entered in the form and revert all populated fields to original state.

77. The solution shall have the ability to utilize predictive text in drop down and/or multiselect fields (e.g., Facility Name would be preloaded into the solution)

78. The solution shall have the ability for the forms data to be exported (e.g. to a CSV file).

79. The solution shall have the ability for a system user to filter the columns being viewed on the outbreak event line listing screen.

Alerts

80. **MANDATORY**: The solution will provide alerts based on programmatic or analytical rules (e.g., clusters of specific diseases in a small geographical area, co-morbidity across multiple data sets). Describe how programmatic or analytical rules are configured, managed, and utilized. JAD sessions will be used to determine programmatic and administrative alerts.

81. Informative alerts.

    a. The solution shall provide informative alerts supporting MSDH's workflow.

    b. The solution shall support alerts for both normal and abnormal events that require MSDH programmatic or administrative action or review to continue a normal automatic workflow.

    c. The solution shall allow users with appropriate access, to define what data elements and thresholds will trigger an alert for certain diseases (e.g. HIV), such as patient name, data change for specific patient, etc.

    d. The solution shall allow users with appropriate access to define alerts related to geographical data elements (such as zip code, county, etc.).

82. Administrative alerts.

    a. The solution will provide administrative alerts based on abnormal ELR and eCR activity.

    b. The solution will provide an alert if ELR messages from any production interface are not received within a defined period.

c. The solution will provide an alert if there is a system-wide ELR failure (e.g., no ELR / eCR messages are received or if they are received but unable to be processed or available to the end user).

d. Describe how the system identifies abnormal ELR and eCR activity and categorize the type of data quality issues the proposed system can provide alerts for.

83. The solution shall provide alerts (e.g., co-infections) for patients in all systems (TB, HIV/STD, and EPI). Alerts (and who will receive them) will be configurable by authorized Communicable Disease users.

84. Solution shall only include enough secure information in Alerts sent outside of the system such that the user can understand what triggered the alert and the case ID.

Dashboards

85. Customizable dashboards.

a. The solution shall provide a user customizable dashboard to MSDH staff upon login.

b. The customizable dashboard will have the ability to display operational and analytical information to the users with drill-down capability.

c. MSDH staff dashboards shall have the ability for program administrators to set dashboard parameters and content by user role.

1. Display results of Case Listing queries with the ability to individually assign a case from the dashboard to a user with appropriate access.

2. Display results of Case Listing queries with the ability to bulk assign cases from the dashboard to a user with appropriate access.

3. Display ELR /eCR activity and trends in a graphical, drill down manner

d. MSDH staff dashboards shall be customizable by user to present surveillance information, ability to monitor and identify trends / clusters, case workload, and alerts.

1. Display workload information to include totals of open and closed cases using date ranges as constraints, by disease, by worker, by district, etc.

e. MSDH staff dashboards shall allow for the user to view alerts in the system and set preference on types of alerts sent via email or text.

f. Describe in detail the dashboard functionality in the proposed solution and how the vendor will meet dashboard requirements.

86. **MANDATORY:** Discovery and JAD sessions will be required to fully identify how the proposed systems dashboard functionality will be deployed. Results will be included in the SOP/Configuration Guide.

Online Reporting

87. Online, web-based public facing reporting system.

a. **MANDATORY:** The solution shall provide an online, web-based public facing disease reporting system.

b. **MANDATORY:** The online reporting system shall allow authenticated users to use the online reporting system public facing system to enter patient demographics, lab reports, and medical case information, as required by MSDH.

1. The online reporting system will have the capability for users to upload documents related to the disease event

2. The online reporting system shall be capable of managing document upload size, where possible, to balance network capacity, storage limits, and document quality.

c. The online reporting system shall automatically ingest and incorporate all information into normal MSDH workflows.

d. **MANDATORY**: The online reporting system shall have automatic processing similar to the automatic Electronic Laboratory Reporting (ELR/eCR) processing with as minimal as possible additional manual worker intervention (e.g., cases are automatically created).

e. **MANDATORY**: The online reporting system shall have automatic duplicate detection and manage the duplicate such that duplicate reports are tracked, managed, and incorporated and not misreported as separate events.

f. The online reporting system shall provide the capability for authorized users to report aggregate Influenza-like Illness (ILI) data. The collected data will be available to MSDH to run reports and export the data in a common format e.g. a CSV formatted file.

g. The online reporting system shall allow MSDH Communicable Disease administrative staff to determine necessary and required fields, labels, help text, required fields, data entry method, valid formats, and valid value lists.

h. The online reporting system shall allow all changes to the online reporting system public facing system to be applied as an administration task by authorized Communicable Diseases staff.

88. Online reporting tool prefill capability.

a. The online reporting system shall prefill as much data as is known at each facility when web users create reports using the public facing system.

b. Prefill shall apply to any information that can be anticipated to increase data entry accuracy or data entry volume such as facility name, ordering provider, test type and similar information that can be anticipated.

c. The online reporting system shall support batch entry. For example, the system might implement uploading a pre-defined spreadsheet template containing patient demographics, filled in by a web user, and uploaded to the IDSP for processing. The Vendor shall propose the solution, the methodology, and any MSDH required data formats offered by the solution.

d. The online reporting system shall allow prefilled data to be achieved using patient information search or other similar means but shall be strictly limited by the user login rule.

GIS Capabilities

89. All incoming lab or case reports via ELR, eCR, on-line provider reporting, or manual entry will be automatically geocoded via Lat, Long / UTM / Street Address or other data point with a PDOP of ¼ mile or less.

90. The solution will provide the end user the option to map individual disease events and/or multiple related disease events.

91. Authorized end users will be able to create, view, download and export a map of individual disease events and/or multiple related disease events based on parameters entered by the end user (e.g., by district, disease, age/age group, date of event, etc.).

H. Case Investigation Functionality

Tuberculosis

Background: The MSDH TB program is responsible for the care and management of all active case TB in the state of MS as well as most latent Tuberculosis Infections. Because of this, all clinical visits and medicine administration documentation are documented in the current TB surveillance system. Clinical documentation can be entered into both the TB surveillance system or EPIC depending on CDC/ TB program reporting requirements. The vendor's response to requirements in this section must provide for clinical documentation to be entered into both the proposed solution and MSDH's EHR using appropriate integration between the two systems. Discovery and JAD sessions will be required to determine the specific details of the integration solution. Results will be included in the Integration and Interoperability Plan.

92. Clinical Documentation

    MANDATORY: The solution shall provide the ability to automatically complete a standard The Report of Verified Case of TB (RVCT) form to meet CDC reporting.

93. **MANDATORY:** The solution shall maintain the RVCT and ensure all data fields are up to date at no additional cost to MSDH.

94. **MANDATORY:** TB Functionality.

    a. The solution shall have specific TB functionality that, at a minimum, meets the following requirements. Vendor must describe in detail how the proposed solution meets the following requirements.

        1. Shall have the ability to document medication administration and track every TB Patient Medication visit.
        2. Shall have the ability to collect and store physician orders.
        3. Shall have the ability to collect and store patient notes.
        4. Shall have the ability to store clinical and surveillance information related to on-going management of TB cases.
        5. Shall have the ability to back-schedule single and multiple visits
        6. The solution shall have ability to automatically add / schedule the next Direct Observational Treatment (DOT) dose after entering a dose.
        7. The solution shall perform automatic medication count tracking per regimen.

95. The solution shall have ability to collect and store all medications administered by MSDH or external providers (with start and stop dates, and reason stopped, and ability to continually add new).

96. The solution shall have the ability to upload and label TB related documents such as: Death Certificate, Interstate Notice, Nursing Home Letter, Legal Orders, Discharge Summary, History and Physical, and Radiology.

97. The solution shall have the ability to collect and manage medications.

98. TB clinical laboratory results.

    a. The solution shall have the ability to collect and store Bacteriology (e.g. sputum Acid Fast Bacilli, sputum cultures)

        1. Must show Drug Sensitivity Testing results to coincide with specific specimen.

    b. The solution shall have the ability collect and store IGRA testing results.

    c. The solution shall have the ability to collect and store Supplemental laboratory results such as chemistry panels, liver function tests, CBCs, etc.

99. The solution shall provide the ability to collect historical information related to TB infection to include at a minimum BCG vaccination history and TB/LTBI treatment history.

100. The solution shall provide easy access to view current classification and episode status for TB patients.

101. The solution shall provide assignable rights to close cases.

102. The solution shall provide the ability to capture and store “Location at Time of Diagnosis” using dropdown choices defined by MSDH.

103. The system shall collect Housing Status at Diagnosis and Housing History as required fields

104. The solution shall provide the ability to collect immigration information, to include at a minimum: country of birth, country of usual residence, preferred language, date of immigration to US, information re: TB screening prior to immigration (e.g. laboratory reports, radiology reports, vaccination history, prior TB history).

105. The solution shall provide the ability to make “Allergies” required for TB cases.

106. The solution shall provide the ability to assign disease-specific tasks to other users with drop downs specific to each disease.

107. The solution shall have the ability to upload an x-ray image to the patient record.

STD / HIV

108. The solution shall have the ability for field staff to add SOGI (the sexual orientation, self-reported gender identity, and ethnicity) to a patient’s record.

109. The solution shall have the ability to view and/or document the patient’s eHARS number in the patient record for newly or previously HIV infected patient.

110. The solution shall have the ability to document allergies and chronic infections in the patient record

111. The solution shall have the ability to document the responses to the required CDC questions regarding the clinical manifestations (optic, ocular, neurologic, etc.) of syphilis for new syphilis cases.
112. The solution shall have the ability to document treatment for positive syphilis cases
113. The solution shall have the ability to use an MSDH defined drop down box to add standard and non-standard treatment of syphilis or any STI infection and allow for additional choices to the drop-down box.
114. The solution shall have the ability to add/update PrEP questions.
115. The solution shall have the ability for an authorized user to add a linkage to care for newly/previously diagnosed patients.
116. The solution shall have the ability to allow a user to manage all linkage to care entries.
117. The solution shall have the ability for an authorized user to change or update case status for a case investigation for syphilis/HIV.
118. The solution shall have the ability to use a drop down to choose a disposition type and allow a user to add new disposition types.
119. The solution shall have the ability to collect interview information such as detection methods, referral source, HIV self-reported status, and HIV posttest counseling.
120. The solution shall have the ability to document if an HIV test was done at the time of testing positive for syphilis.
121. The solution shall have the ability to view all previous cases for syphilis or HIV for a patient once a new case is entered for that patient.
122. The solution shall have the ability to document HIV case reports (such as case report dates, source of reports, previous history of HIV tests) in a patient's record.
123. The solution shall have the ability to document risk factors required by CDC standards for each case interviewed.

Epidemiology

124. The solution shall have the ability to collect documentation of multiple travel destinations / trips, to include at a minimum: destination, country, departure and return dates.
125. The solution shall have the ability to print populated and blank individual case report forms in a PDF format.
126. The solution shall have the ability to print populated and blank individual case investigation forms in a PDF format.
127. The solution shall have the ability to display a message or brief update to either all internal or external users or both registered in the solution in an ad hoc manner.
128. The solution shall have the ability to generate a form letter for contacting parents or guardians of cases under the age of 18.
129. The solution shall have the ability to conduct searches using date range fields to include at a minimum: Event Date, Onset Date, Diagnosis Date, Referral Date,

Specimen Collection Date, MMWR Year / Week, First CDC Report Date, Last CDC Report Date, and Lab Report Date.

130. The solution shall have the ability, while in a patient record, to view multiple screens simultaneously (e.g. while in the patient's case report form, open another window to view the same patient's lab report detail).

131. The solution shall have the ability to automatically calculate the age once a date of birth is entered.

132. The solution shall have the ability for the state to configure a default for each drop down if no data is reported (e.g. For race, if not reported the state can choose a default of Unknown but for other fields the state can choose another default).

133. The solution shall have the ability to document that a case was imported from another country and the countries must be listed in a drop down with predictive text.

134. The solution shall have the ability to document historical home addresses with date ranges.

135. The solution shall have the ability to restrict queue entries by using access rights by disease / program (E.g. someone with only EPI access should not be able to see STD labs in the queue).

Outbreak Management

136. The solution shall have the ability to create an Outbreak Event to include the following fields at a minimum:

- Unique system generated Identifier
- Outbreak Name (Mississippi standard (free text, alpha numeric)
- Outbreak Number (Mississippi standard (free text, alpha numeric))
- Link to Supplemental Form(s)
- Link to Outbreak Event Form
- Link to Outbreak Summary
- Active / Inactive Field

137. The solution shall have the ability to associate multiple Supplemental Forms, an Outbreak Event Form, and an Outbreak Summary Form to the Outbreak Event via dropdown menus.

138. The solution shall have the ability to edit all fields in the Outbreak Event record.

139. The solution shall have the ability to make fields associating a patient with an Outbreak as Core Data Fields (e.g. Outbreak – Yes/No; Outbreak Name, Outbreak ID (auto-populated once Outbreak Name is chosen)).

140. The solution shall have the ability to link a patient to an existing Outbreak Event using a predictive text dropdown listing of all open Outbreak Events.

141. The solution shall have the ability for an authorized user to manually close an Outbreak Event.

142. The solution shall have the ability to use populated Core Data Fields to automatically populate forms.

Contact Tracing

143. The solution shall have the ability to document contacts and link the contact to the original case.

144. Contact data sharing across programs.

   a. The solution shall have the ability to collect contact information that will support all OCD programs (EPI, TB, and STD/HIV).

   b. The solution shall have the ability to collect specific details regarding the exposure: where did the exposure occur (e.g. home, office, outdoors, school, club, etc.), duration of exposure (minute, hours, etc.), frequency of the exposure (daily, weekly, on-time, etc.); ventilation (e.g. outdoors, car, central air, etc.); first exposure date; last exposure date; type of exposure (oral, anal, etc. (STI); raspatory (TB)); relationship to case (family member, significant other, friend, etc); priority; contact attempts.

   c. The solution shall have the ability to document exposure and treatment history for reportable diseases and details of treatment / completion.

   d. The solution shall document risk factors i.e. homelessness, underlying medical conditions, high risk sexual activity, alcohol / substance abuse, incarceration history, etc.

   e. The solution shall have the ability to create specific forms used by each program to collect all contact.

145. Documenting contact laboratory results.

   a. The solution shall have the ability to document laboratory testing for the contact.

   b. The solution shall have the ability to manually add laboratory results.

   c. The solution shall have the ability to document initial testing such as gonorrhea, chlamydia, HIV, QuantiFERON, IGRA, TST, etc.

   d. The solution shall have the ability to document supportive testing such as chest x-rays (including image), CBC, LFTs, viral loads, renal panel, etc.

146. The solution shall allow authorized users to manually change the contact status based on the results of laboratory testing, x-rays, and signs/symptoms.

147. The solution shall have the ability to set alerts / reminders for follow-up testing or treatment for contacts.

148. The solution shall have the ability for users to assign tasks to other users.

149. The solution shall have the ability to document treatment for the contact either manually or be populated within the Epic interface (may be one-time treatment or on-going treatment).

150. The solution shall have the ability to collect treatment start date and end date and calculate the number of doses received.

151. The solution shall have the ability to document post treatment follow-up for contacts.

152. The solution shall allow users to view all linked contact records to a case of a reportable disease.

153. The solution shall allow exports of contact details related to a certain disease type.

154. The solution shall allow the generation of summary report of contact details related to a certain case or disease type.

155. The solution shall have the ability to calculate partner and cluster index summary report by geographical area, by user, etc.

I. Federal Reporting Requirements

156. **MANDATORY:** The solution shall support reporting to the CDC, Health Resources and Services Administration (HRSA), and any other Federal Partners per all state and federal requirements. Vendor must provide a detailed description of previous reports provided.

157. **MANDATORY:** The solution shall have the ability to send weekly reports of non-MMG diseases to Security Access Management System (SAMS) in the CDC required (NETSS.dat) format.

158. **MANDATORY:** The solution shall automatically create and send a weekly CSV file to the CDC with required Report of Verified Case of Tuberculosis (RVCT) data.

159. **MANDATORY:** The solution shall automatically send any updates to diseases that have corresponding MMGs to the CDC via HL7.

160. **MANDATORY:** The solution shall create reports using required formats as directed by MSDH.

161. **MANDATORY:** The solution shall automate TB case reporting in the Web-based CDC program National Tuberculosis Surveillance System Case Reporting (NTSSCR).

162. **MANDATORY:** The solution shall automate all CDC reporting where applicable (e.g., if the CDC supports automatically reporting for that data, the solution shall automate reporting that data).

163. **MANDATORY:** The solution shall support additional required federal reporting as required by MSDH.

164. **MANDATORY:** All MMG development and reporting shall be in accordance with CDC standards and remain current with all CDC required updates. All current MMGs shall be identified and implemented and deployed at Go-Live.

165. **MANDATORY:** The solution shall support implementation of additional MMGs as required by the CDC and other Federal Partners requiring MMGs for MSDH reporting at no additional cost to MSDH.

ELR/eCR Processing

166. **MANDATORY:** As part of implementation, the vendor shall provide human resources to migrate all existing production ELR and AIMS interfaces to the proposed system, ensuring adherence to current HL7 standards. Duties include onboarding / registering the trading partners within the system and establishing

connections with existing production interface system(s). The vendor will also monitor all production interfaces, duties include: monitoring incoming messages for data quality, interface performance, alerting / communicating if needed with MSDH on identified interface and data quality issues and resolving those issues as directed by MSDH. All costs to meet this requirement shall be included in the Implementation costs in the Cost Information Submission.

167. **MANDATORY:** After implementation (during M&O), the vendor shall provide human resources for onboarding new (post implementation) trading partners for ELR and eCRs with other duties to include onboarding / registering the trading partners within the system, establishing connections to new trading partner system(s). Also includes providing interface data quality monitoring resources that monitor all ELR interfaces whose duties include: monitoring incoming messages for data quality, interface performance, alerting / communicating if needed with MSDH on identified interface and data quality issues and working with trading partners directly to resolve those issues as directed by MSDH. The vendor must include all costs to meet this requirement as a separate line item in the Cost Information Submission.

168. **MANDATORY:** ELR processing.

    a. The solution shall support receiving ELR information from sources utilizing standardized, current Promoting Interoperability HL7 interface specifications.

    b. The solution shall create a new patient record for an incoming ELR or append to an existing patient record if the patient exists in the system.

    c. All historical lab results attached to patient's records will be accessible by MSDH users.

    d. The solution shall support receiving and processing as an HL7 ELR message, CSV formatted files.

169. The solution shall incorporate robust HL7 acknowledgements that shall be utilized in service responses to address quality issues.

170. **MANDATORY:** The solution shall support current ELR/eCR interoperability standards and remain current with industry standards, MSDH trading partners, and federal communicable disease requirements at no additional cost to the agency.

171. **MANDATORY:** The solution shall detect and properly organize or flag ingested ELR/eCR, and other reports, automatic and manual, that are duplicates. Duplicate detection shall be rules based, and the system shall allow adjusting the rules to improve data quality (e.g., a report for the same disease on the same patient is received from two sources within a week could be flagged as a duplicate). Describe the solutions approach.

172. **MANDATORY:** The solution shall allow duplicate patient records to be manually merged. Merged patient records are flagged for end user identification that a merge occurred.

173. **MANDATORY**: The solution shall provide the ability to unmerge patient records that have been manually or systematically merged. Unmerged lab reports must maintain original record integrity.

174. **MANDATORY**: The solution shall consider merging patient records as inclusive of merging entire patients, eCRs, ELRs, and other discrete patient record parts supported by the solution.

175. **MANDATORY:** The solution shall be capable of automatically processing and storing ELR/eCR based on mapping rules with minimal queues or manual intervention (e.g., negative results are processed and stored automatically but do not generate worker alerts unless otherwise requested by MSDH).

176. Data processing queues.

    a. The solution shall maintain a queue(s) or list of all ingested information that cannot be automatically integrated into existing patient records or are used as typical processing (e.g. queues used for duplicate patients or lab results). This applies to all ingested information from any source or from the on-line reporting tool.

    b. Describe in detail how queues are used in all workflows in which data are processed. Include in the description the number / name of queues that MSDH staff will be required to manage.

    c. The solution shall have the ability for multiple workers to simultaneously process individual records in the queue, access to the underlying message, message source, detected errors, and perform relevant lookups to disambiguate the record and complete processing.

    d. The solution supports allowing multiple users to work in the same record or queue at the same time, are alerted of other users, and are protected to ensure one user is not allowed to inadvertently overwrite another user's update.

    e. The solution shall support automatic disambiguation for all types of ingested information where possible.

    f. Disambiguation support covers enhanced patient identity matching, automatic error detection and correction, and other solution specific processes that can work with partial or ambiguous information and resolve it such that it can be properly associated and stored.

    g. All automatic and manual disambiguation is tracked and can be audited with the solution.

177. The solution shall auto process manually entered or loaded lab reports and case records based on the same mapping rules and quality control goals as used for electronic automatic processing.

178. **MANDATORY:** The vendor shall provide mapping rule authoring support allowing MSDH personnel to create new mapping rules, edit mapping rules, assign mapping rules to be used in appropriate workflows, and assign mapping rules to be used ad hoc to clear issues related to manually entered or electronic queue entries that must be processed with special circumstances.

179. The solution shall allow communicable disease administrative staff to add, edit, and manage the list of new diseases and existing disease names available for mapping.

180. The solution shall support uploading whole genome sequencing (WGS) and other disease sub types using HL7 or other standard formats. Discovery (JAD sessions) will be required to determine specific requirements.

J. IDSP Integration / Interoperability and Data Requirements

Integration and Interoperability

181. The Vendor shall provide an Integration / Interoperability Plan in their proposal based on the RFP requirements, verifying the Vendor's understanding of the IDSP Integration / Interoperability needs and requirements. The plan should include initial strategies, solutions, past experiences with the proposed solutions, and the use of JAD sessions. If awarded, the Vendor will develop a final version to be approved by MSDH after JADs / Discovery and before implementation can begin. This will require the Vendor to perform additional program workflow and IT discovery and technical specification analysis (possibly to the specific field level) to include at a minimum: documented program work/data flow related to the integration with the IDSP, transport protocol, modality (solicited, unsolicited, uni / bi-directional), technical approach, roles and responsibilities, risks, assumptions, and constraints with MSDH technical personnel, MSDH programmatic personnel. and possibly other third-party Vendors.

182. *Background: MSDH's instance of Epic, or the current EHR for MSDH, is to remain the system of record for MSDH's patient health records (clinical documentation). MSDH uses Epic in all county health departments to collect clinical data for its patients. The Vendor's proposed solution will be the system of record for all surveillance data and perform all federal reporting.*

MANDATORY: The solution will appropriately integrate with MSDH's electronic health record (Epic) such that clinical data entered in Epic that is needed to fulfill federal and state reporting and program case investigations / management requirements must be included in the integration/interoperability with the Vendor's solution appropriately. Discovery/JADs will be needed to define the final integration solution (to the data element) with the results included in the final Integration / Interoperability Plan.

183. **MANDATORY:** The solution shall provide a standards-based, near real-time patient level Vaccine Preventable Disease (VPD) query from the IDSP while the patient is in context, with the state's Immunization Registry (MIIX) adhering to the MIIX HL7 Implementation Guide (https://msdh.ms.gov/msdhsite/_static/resources/4567.pdf). Results will be available for the end user to import into the patient's case report to be viewed by all users appropriately. Discovery/JADs will be needed to identify the final integration solution (to the data element) with the results included in the final Integration/Interoperability Plan.

184. **MANDATORY:** The solution will integrate/interoperate with internal and external systems required to ensure:

a. The HIV status is appropriately viewable by other IDSP programs when required for their investigations.

b. The TB RVCT is appropriately completed, and all federal reporting can be done through the Vendor's solution.

c. Discovery/JADs will be needed to identify all systems and data elements needed to be integrated/interoperated with the results included in the final Integration/Interoperability Plan.

185. **MANDATORY:** The solution shall integrate with the MSDH's instance of CDC's eHARs such that:

a. Laboratory tests including initial HIV testing and confirmation as well as all viral load testing are exchanged appropriately.

b. Required risk factors associated with HIV are exchanged appropriately.

c. Required HIV confidentiality forms are exchanged appropriately.

d. Discovery/JADs will be needed to identify the final integration solution (to the data element) with the results included in the final Integration/Interoperability Plan.

186. The solution shall integrate/interoperate with MSDH's Vital Records/Statistics system to integrate birth data and mortality data into the system appropriately. Examples include, at a minimum, the STD/HIV program needs birth information regarding children of mothers diagnosed with certain STDs and EPI needs mortality information of patients diagnosed with certain infectious diseases. Discovery/JADs will be needed to further define the integration with the results included in the final Integration/Interoperability Plan.

187. Non-laboratory Trading Partners.

a. **MANDATORY:** The solution shall integrate with national data hubs such as the APHL Informatics Messaging Service (AIMS) platform.

b. The solution shall integrate with other State Departments of Health reporting ELR to and receiving ELR from MSDH.

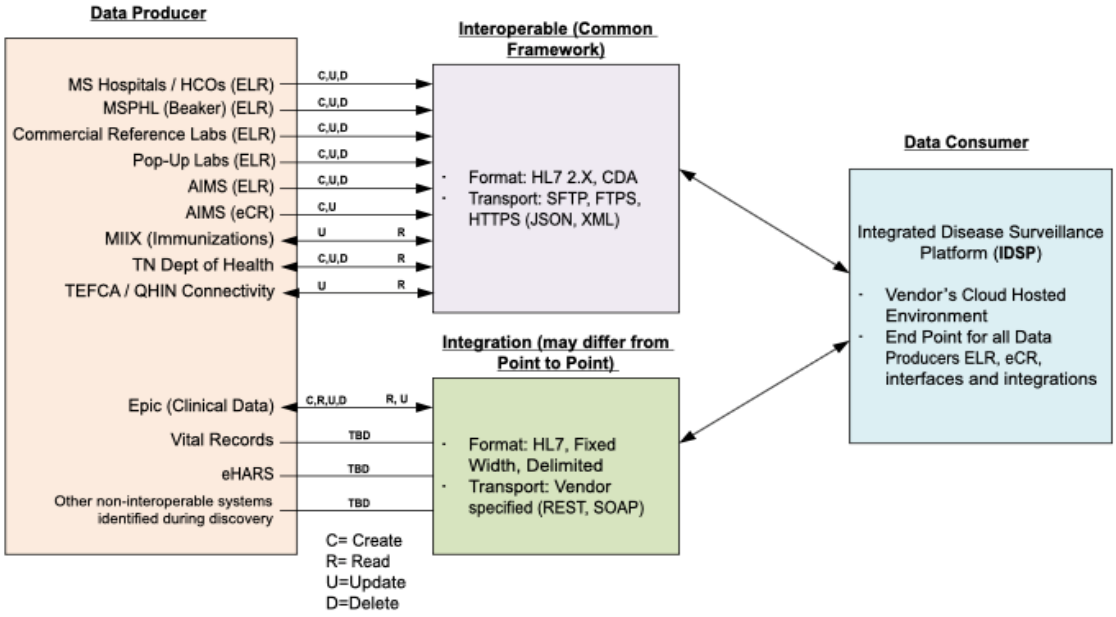
c. **MANDATORY:** Discovery / JADs will be needed to 'identify all ELR /eCR reporting integrations with the results included in the final Integration / Interoperability Plan.

188. The Vendor shall connect the proposed solution to a Qualified Health Information Network (QHIN) and the proposed solution shall have the capability to support all TEFCA public health use cases (e.g. query for supplemental data). The Vendor shall conduct discovery to determine options for QHIN connectivity and how the TEFCA use cases will be satisfied using the proposed solution. The results of the discovery will be included in the final Integration / Interoperability Plan. All costs to meet this requirement must be listed in the Cost Information Submission as a separate line item.

189. The final plan shall consider all types of laboratories that will be sending (national and state commercial reference labs, hospital and ambulatory labs, public health emergency pop-up labs, and MS Public Health Lab).

190. The initial plan submitted with the proposal shall address all integration described in this section and be based on the Diagrams below. All interfaces and integrations will terminate directly with the Vendor's solution. The final plan may identify additional systems and integrations required to satisfy federal reporting requirements.

Diagram 1 – IDSP Integration / Interface Implementation



191. The Vendor shall define and implement all identified integrations and interoperability efforts as defined in the Integration/Interoperability Plan at no additional cost to the state.

192. The solution shall support and remain current with the complete HL7 interoperability standards, FHIR standards, as well as MSDH trading partners and federal EHR reporting requirements at no additional cost to MSDH.

193. **MANDATORY:** The solution shall be capable of securely interfacing with IDSP trading partners and internal MSDH systems using Simple Object Access Protocol (SOAP), Secure File Transfer (SFTP), and representational state transfer (REST) API services.

194. The system shall have the ability to provide role-based access to raw HL7 and FHIR messages for MSDH to assist trading partners with identifying message errors.

195. The solution shall have access to the state network via the internet/FIPS-rated encrypted connection. The encrypted connection must meet ITS Cloud and Security policy.

Data Input / Export and Extraction

196. The solution shall allow the creation of custom defined input and export file formats.

197. The solution shall support export formats that generate files that can be automatically uploaded to the reporting agency or manually downloaded by a user.

198. The solution shall allow exporting of all data to formats such as CSV, paginated PDF, Tableau, and Power BI.

199. Saving Report Searches

   a. The solution shall provide the capability of creating and saving Report Searches capable of finding information.

   b. Report Searches shall be created using all Core Fields e.g. disease name, case classifications, investigation status, all date fields (e.g. Event Date, Onset Date, etc.), address information (county, district, etc.), facility name, performing laboratory, case creation method (ELR, manual entry, etc.), gender, race, ethnicity, date of birth, etc.

   c. The solution shall have the ability to export search results and patient and/or case records.

   d. Saved Report Searches will be available for other authorized users to execute.

200. The solution shall provide the ability to view a summarized listing of export results that meet the Report Search criteria.

   a. The solution shall provide the ability for users to customize the summarized listing.

201. The solution shall support limiting export results by allowing the user to select specific fields to be included in the CSV.

Data Migration / Conversion and Retention

202. Data Migration Plan

   a. The Vendor shall submit a Data Migration Plan with the initial proposal that describes the Vendor's data migration approach and details regarding importing required data from multiple legacy systems into the solution from past disease surveillance patients. If awarded, the Vendor will develop a final version to be approved by MSDH after JADs/Discovery and before implementation can begin. The Vendor's data migration and conversion fees must be included in the Cost Information Submission, Section VII of the RFP.

   b. The Vendor shall include in the Data Migration Plan the approach to also migrate user configurations/accounts and other relevant data from existing systems replaced by the IDSP.

   c. The Vendor shall review MSDH data infrastructure and systems being replaced and work with MSDH to define the data imports that are necessary for the solution and to support MSDH business processes moving forward.

   d. The Vendor shall be responsible for extracting data from the legacy system from the following systems:

      1. Epi-Tracks (used to support the Epidemiology Program)

      2. CDC-IS (used to support the Tuberculosis Program)

      3. PRISM (used to support the STD Program)

203. The data import shall convert the legacy data into a homogenous, error checked extract that can be imported into the solution.

204. MSDH anticipates providing technical assistance and guidance to Vendor data exports.

205. The Vendor shall work with MSDH to satisfactorily resolve incompatibilities where data is missing, duplicate, bad, or incompatible.

Data Retention

206. The Vendor shall retain records in compliance with state, federal, and MSDH program data retention policies. It is the Vendor's responsibility and due diligence to identify and categorize data to remain within retention policy, which currently has most data retained for seven (7) years.

207. The Vendor shall inform MSDH when it discovers or is required to change or adjust data retention rules.

Auditing and Security

208. External user management system and Auditing

a. The solution shall provide an external facing, facility federated user management system.

b. External facilities shall have the ability to register with the agency and independently manage users within their facility that can utilize online reporting.

1. The external user management system shall follow MSDH user account and password management standards, including multifactor authentication.

2. Additional security features are optional and can be enumerated.

c. Audit/Log: The Vendor shall provide a solution that is capable of auditing and logging events. Auditing and logging are integrated such that the system cannot take actions and avoid auditing and logging. Solution logging is available for review through various methods such as screens, reports, and Application Programming Interfaces (API)/messaging services.

1. The proposed solution shall support the ability to audit all solution and component activities, meet federal and state regulations for privacy and, by user or process such as but not limited to:

1. Additions/Deletions/Edits;
2. Merges/Unmerges;
3. Rejected merges;
4. Logins;
5. Errors;
6. Searches;
7. Exported data / Imported data;
8. User actions;
9. Reports run; and
10. Messages received/sent.

c. The solution shall provide access to system audit data.

i. Audit data shall be the data that tracks all solution activities and can be used to report on success, warnings, and errors/failures.

ii. Audit data shall include message warnings and errors, user activity, system events, and the typical logging of successful activities.

iii. The solutions shall support users with appropriate program level access. the ability to search, view, filter, and export the logs.
iv. Log search criteria shall at a minimum support time, event type, and user. Log exporting supports CSV.

d. **MANDATORY:** The solution's user interface shall provide a Single Sign-On (SSO) experience for MSDH personnel managed by the Department's Azure Active Directory. Azure Active Directory shall be used to manage user authentication and roles establishing user access rights within the solution. The SSO experience also fully supports multi factor authentication (MFA). MSDH personnel will utilize the MSDH provided MFA. The vendor will provide an MFA solution for non-MSDH personnel.

K. Operational Requirements

Hosting Requirements

209. The Vendor shall deliver, host, implement, maintain, and support the infrastructure and the software for the proposed solution in a Software as a Service (SaaS) offering for the life of the contract.

210. The Vendor shall follow Industry Standards and Best Practices for hosting and security per the SaaS Product Development Life Cycle procedures.

211. MSDH seeks a single host setting for all IDSP instances provided by the vendor. Potential host settings to be considered are any cloud-based HIPAA-certified facility that complies with Federal, State and local laws.

212. **MANDATORY:** The Vendor shall be aware that under no circumstances shall any data, or equipment associated with this project reside outside the continental United States, nor shall any data, or equipment associated with this project be accessible to people outside the continental United States. All operational resources including help desk must be in the continental USA. Under no circumstances will PHI be moved offshore either for testing purposes or in production (the use of offshore and near-shore resources may be permitted for development efforts only). Vendor must describe how this requirement will be met.

213. The Vendor shall provide a disaster recovery (DR) data center location in the continental United States that is at least two hundred and fifty (250) miles from the primary facility. The Vendor's proposal shall describe how the DR data center location minimizes risk in the event of a disaster, including service levels for recovery and minimizing data loss (RPO and RTO).

214. The Vendor shall host all instances in a certified, Tier 2+data center, with the following:

a. All equipment required to provision, maintain, monitor, and manage the circuit to the hosting and DR facilities;

b. Network protection on any servers with MSDH data or applications and cloud servers to prevent attacks and to ensure MSDH data, information, software, and networks are secured from unauthorized access. This protection shall comply with the transmission security provisions of HIPAA, as well as all relevant federal, state, and local laws and MSDH IT Security Policy;

c. Intrusion detection and abnormal data retrieval detection and alerts (for example, mass downloads of PHI);

d. Perform recording and reporting on security incidents and breaches (both immediate reporting and summary reporting);

e. Current Operating System security patches;

f. Current antivirus software;

g. Two factor authentications to access PHI by Vendor staff;

h. Encryption in transit and at rest; and

i. Encryption for each website.

215. Vendor must provide wide area network (WAN) encrypted tunnel or virtual private network (VPN) tunnel support to MSDH from both the primary and the DR site.

216. The Vendor shall ensure the facility is compliant with SSAE 16 (i.e., SOC 1) and HIPAA standards.

217. The Vendor shall provide dedicated services with no intermingling of data or resources with other clients other than MSDH. This includes all internet connectivity.

218. The Vendor shall provide the data center and hosting capacity sufficient to handle the bi-directional transactions discussed in this RFP and be capable of increasing and decreasing the hosting capacity and associated cost in a structured way based on current system capacity needs.

219. The Vendor must demonstrate in the proposal its ability to increase the size of the circuit in incremental increases of 100 Mbps and one Gbps should MSDH require an increase in the future. Pricing must be presented in RFP No. 4635 Section VIII, Cost Information Submission as an optional cost.

220. The Vendor shall provide system and data reliability through off-site system and data backup in accordance with Table 3: SLA Matrix provided by MSDH.

221. The Vendor's Security service shall provide monitoring for timely reporting of threats and intrusions.

222. The Vendor's Security services shall include a security agent to control all traffic between the primary and disaster recovery center and the outside world and protect against unauthorized access or intrusions.

223. The Vendor's Security services shall allow reporting for firewall and other statistics from any Internet browser with monthly analysis and recommendations to improve security and throughout.

224. The Vendor shall submit a Cloud Architecture Diagram and SOP at the initiation of the project. The Vendor shall follow the approved plan and maintain the plan such that it remains current and accurate to the procedures established for the technical environment. The plan shall be made available to MSDH staff and designated auditors upon request

225. The Vendor shall provide the projected cost analysis over a five (5)-year period for maintenance, enhancements, upgrades, and any associated licensing or data storage fees.

226. **MANDATORY:** The proposed solution shall remain current and compliant with HIPAA and NIST 800 standards for data privacy and data security.

227. The Vendor shall be responsible for System Security Plan (SSP) requirements associated with an IDSP.

    a. The SSP shall remain based on the current with NIST 800 updates, compliance from all third-party affiliated systems and updates to the SSP for the system and affiliated systems.

    b. The Vendor shall follow the standards and best practices documented in the approved SSP to ensure security for all data and messages.

    c. Describe the testing the Vendor will do to quality check the SSP, prepare for audits, and respond to issues detected during audits such as vulnerability tests, penetration tests, and other internal audits

    d. The Vendor will complete vulnerability tests, penetration tests, and other appropriate audits yearly or upon request.

        i. The Vendor shall provide test and audit report results upon completion or provide the most recent report upon request.

    e. Provide a sample or clearly identify the reporting methodology and content used to convey SSP execution results, both successes and failures, the period of reporting, and the reporting showing security issue resolution plans, root cause analysis and successful resolution; and

    f. Describe security for the system, contractors, third party products, and affiliated systems;

    g. Describe the schedule, triggers, and responsibilities that ensure the SSP remains current and accurate at all times;

    h. MSDH will be responsible for all user account management during normal operations (normal operations defined as operating not under surge conditions). Discuss user security and user management for internal and external users as well as a comprehensive discussion on user account management through Azure Active Directory and the Vendor managed external user management system. This section also includes a description of the two-factor authentication process.

228. The Vendor shall be required to participate in the MSDH Vendor Risk Management Policy program.

229. The Vendor shall use Transport Layer Security (TLS) 1.2 or higher if available as a standard and shall upgrade as the standard evolves, at no cost to MSDH.

230. The proposed solution must include the following access control requirements:

    a. Each instance must be equipped to establish role-based security levels based on user profiles;

    b. Each instance shall limit access to PHI and sensitive information based on the role of the user;

    c. Roles will be defined and provisioned to support MSDH workflows for staff, contractors, and other authorized persons, read-only roles, and one or more administrative roles;

    d. All access to PHI must be recorded and made available for reporting to include Timestamp, content accessed, person accessing, physical location of access

with IP address, reason for access and method of access. Demographic data is PHI;

e. Data shall be available to MSDH staff, auditors, and HIPAA reporting/auditing upon request;

f. Data present in all test system/instances is synthetic or simulated using security and privacy best practices unless just cause is provided and approved by MSDH;

g. The solution shall support security administration for user roles and shall have the ability to hide menu items and screens within the system, can limit data entry fields making them view only by role, and can limit data visibility and editability using record data such as assigned worker or record owner.

h. Each instance must prohibit unauthorized users from accessing PHI and other sensitive information according to state and federal confidentiality rules; and

i. Vendor staff including development and support staff shall use two-factor authentications when accessing any aspect of the production application or its data.

j. The proposed solution shall include the following System Support Requirements:

    1. The Vendor shall be responsible for the operational aspects of the proposed solution;

    2. **MANDATORY**: The Vendor shall be responsible for providing Tier 1 and Tier 2 Help Desk support during Implementation. Tier 1 tech support is the first line of technical support responsible for basic customer issues for all users (internal, external, and trading partners). It is synonymous with first-line support or level 1 or L1 support resolving basic technical or semi-technical issues. Tier 2 tech support is more in-depth technical support. It is synonymous with support level 2 or L2 support, support requiring more experienced support staff that are knowledgeable of the proposed solution and capabilities. After, Implementation (during M&O) the vendor will only be responsible for providing Tier 2 Help Desk Support. Help desk support shall not preclude creation and delivery of report requests, in an ad hoc fashion or for audit purposes; all costs required to meet this requirement must be included in the Cost Information Table as a separate line item.

    3. The Vendor shall provide a toll-free support line for contacting the help desk.

    4. The help desk shall be available during MSDH working hours (typically 7:00 a.m. to 7:00 p.m. Central Time Monday through Friday).

    5. The Vendor shall keep current all user documentation, support, and train MSDH staff on the vendor supplied help desk process and procedures and provide periodic refresher training. Acceptable training approaches are in-person training, computer-based training, (interactive solutions, webinars, etc.), and/or training videos.

    6. The Vendor shall provide a secure, Web-based MSDH user support center, including the ability for MSDH staff to report a problem and monitor its status.

7. The Vendor shall provide reporting of SLA metrics in accordance with Table 3: SLA Matrix.
8. The Vendor shall keep the information in the SOP/Configuration Guide current and accurate for the life of the contract.
9. The Vendor shall keep the information in the System Security Plan (SSP) current and accurate for the life of the contract.
10. The Vendor shall keep the information in the System Turnover Plan current and accurate for the life of the contract.

k. The Vendor shall develop a SaaS Product Development Plan outlining the approach. The plan shall include the following:
   1. The Vendor shall implement and maintain change and release management best practices so that releases can be rolled back;
   2. The Vendor shall develop a method for deploying the current code into selected pre-production environment(s) and validating that the code is ready for deployment into the production environment; and
   3. The Vendor shall use version control when upgrades are made to any instance.

l. The Vendor shall develop a SaaS Data Turnover Plan that describes the methodology, schedule, and process for contract termination, detailing how the following specifications will be met:
   1. The Vendor shall cooperate with the successor Vendor while providing all required turnover services at no additional costs to MSDH. This shall include meeting with the successor and devising work schedules that are agreeable to both MSDH and the successor Vendor;
   2. The Vendor shall turn over all data to MSDH, within a mutually agreed upon timeline. All data shall be properly disposed of after turnover, within a timeframe specified by MSDH according to the executed Business Associate Agreement (BAA) required to be executed at contract signing.
   3. Provide the schedule necessary and overlap expected providing a reasonable path to meet with, scheduling with, export data, import data, review, test, and collaborate such that the successor has access to the Vendor during turnover;
   4. Describe the process of transferring user-based documentation and any MSDH-specific/derived configurations, rules, and workflows to the successor;
   5. Describe how file formats, message formats, mappings, 3rd party integration, import/export procedures and templates developed for MSDH that are not unique to or proprietary to the solution shall be packaged and provided to the successor; and
   6. Describe the process and timeline that ensures all MSDH data is purged from the solution, verification process, quality assurance testing, and MSDH staff involvement.

m. Vendor shall describe how the following will be addressed and include the MSDH staff hours/level of involvement necessary, if applicable:

1. Ensuring Software Licenses are adequate to meet MSDH's needs;
2. Maintenance schedule; and
3. Technical Infrastructure Changes.

n. The Vendor shall complete system updates as required by new mandates from state and federal legal authorities.

o. The Vendor shall ensure the system remains in compliance with all applicable federal and state rules, regulations, rulings, and MSDH policy. The Vendor is responsible for the timely discovery of compliance issues and shall implement system changes such that they can be tested and incorporated into MSDH worker processes prior to production implementation. Compliance is considered routine system health maintenance covered by the maintenance budget.

p. The Vendor shall maintain known product defects and reported incidents in an appropriate incident tracking system. MSDH staff shall have access to the system to review known incidents, track progress, and provide information.

q. The Vendor shall propose an incident reporting system that allows incidents to be reported by MSDH staff and outside entities. Outside entities interact with the system through electronic reporting and the public-facing Web site.

r. The Vendor shall ensure that secure protection, backup, and Disaster Recovery measures are in place and operational as a prerequisite to cutover from the current M&O Vendor to the Vendor's hosting and operations of the production (i.e., for end of Start-Up Period) and for the duration of the contract. The Vendor shall ensure no loss of data or configuration of the environments.

s. The Vendor shall maintain and use MSDH approved operations quality assurance procedures defined in the Operations Guide.

231. The Vendor shall develop a knowledge base SOP/Configuration Guide describing how the software is configured, integration with MSDH personnel, user management, error reporting, defect management, rule, and parameter changes, updated requirements resulting from discovery and JAD sessions, change requests, and interoperability with internal and external interfaces as well as external users. The SOP/Configuration Guide allows the Vendor to demonstrate a mature process, and a robust system, networking, and integration infrastructure. Infrastructure goes beyond cloud offerings to show the Vendor has a robust, flexible, and mature technical solution. Along with providing a mechanism for capturing requirements and configurations from JAD Session, the plan establishes the Vendor's methods and procedures for technical infrastructure, and communications protocols during M&O. The guide is intended to remain current and operate as a definitive guide for M&O.

a. Describe processes used by MSDH and external users to report errors, omissions, and change requests. It includes descriptions of any automated processes, escalation procedures, timeframes, prioritization processes, and any other necessary details.

b. Describe the process for reporting and making any form, rule, and parameter changes. Include timeframes, MSDH roles and responsibilities, and other factors necessary to ensure smooth and accurate updates.

c. Describe process for Vendor discovered errors or planned upgrades, updates, and software maintenance, not directly related to MSDH nor reported by MSDH. Include notification timeframes and notification approach as well as MSDH roles and responsibilities.

d. Describe the process used to request and receive ad hoc reports. Ad hoc reports can be requested to support special legislative or judicial requests, internal research, auditing, and other reporting.

e. Provide the product maintenance schedule and the processes used to manage the schedule, exceptions, emergency releases, and other release management descriptions. This includes product versions, release notes, testing results, opting out of a release, and other release specific information.

    1. Describe how other customer changes are integrated into the product offering, notifications, testing opportunities, scheduling, and options available (if any) to reject or delay changes.

f. **MANDATORY:** Growth and Surge Plan

    i. The Vendor shall provide a Growth and Surge Plan with the proposal.

    ii. The Growth and Surge Plan shall include services and costs for to accommodate growth from normal operations. Normal operations are defined as not operating under national or local public health emergency scenarios, as defined by the State Health Officer, where a surge in users and / or data will be evident.

    iii. The Growth and Surge Plan shall include a description of the vendor's methodology for their proposed system to respond to surge situations. A surge is defined as a situation that requires an increase in users and/or incoming data due to a nationally deemed Public Health Emergency, a state defined emergency such as a local epidemic, disaster response, or other event that increases the IDSP users and / or data at a rate / volume which MSDH support staff or the proposed system cannot accommodate. All costs for increased capacity and required services due to a surge shall be included in the Cost Information Submission as a separate line item. Cost must include resources for surge and user management and resources for ELR onboarding.

        1. During surge conditions, the Vendor shall provide all external user management services and also additional ELR onboarding.

g. Business Continuity Plan (BCP): Identification of the core business processes involved in the production solution. The BCP must be included with the Vendor's proposal response. For each core business process include:

    1. Identification of potential failures for the process;

    2. Risk analysis;

    3. Impact analysis;

    4. Definition of minimum acceptable levels of service/output;

5. Definition of triggers for activating contingency plans;
6. Procedures for activating any special teams for business continuity;
7. Plan for recovery of business functions, units, processes, human resources, and technology infrastructure within RTO and RPO timeframes; and
8. Communication protocols and processes for restoring operations in a timely manner.

h. Disaster Recovery Plan (DRP): Procedures for data backup, restoration, and emergency mode operations in the event of Hardware or Software Failures, Human Error; Natural Disaster; and/or Other unforeseeable emergencies. The DRP must be included in the Vendor's proposal response. Additional Disaster Recovery Plan Topics must include:

1. Retention and storage of backup files and software procedures;
2. Hardware backup for critical solution components procedures;
3. Facility backup procedures;
4. Backup for any telecommunications links and addresses incoming ELR/eCR interfaces, outgoing CDC reporting, manual entry, and any other tools identified and utilized by MSDH;
5. Backup procedures and support to accommodate the loss of any online communications;
6. A detailed file backup plan, procedures, and schedules, including rotation to an off-site storage facility;
7. Describe an off-site storage facility that providing security of the data stored there, including protections against unauthorized access or disclosure of the information, fire, sabotage, and environmental considerations;
8. An enumeration of the prioritized order of restoration for the Vendor's proposed solution in accordance with RTO and RPO objectives; and
9. Describe the Vendor's method, process, and content for providing annual Disaster Recovery test results.

i. Narratives addressing the following:

1. Systems Monitoring;
2. Points-of-contact and backups;
3. Technical Support;
4. Health Insurance Portability and Accountability Act (HIPAA) Compliance;
5. Data Replication;
6. Solution Warranty;
7. Certificate Expiration Date Tracking; and
8. Other items as mutually agreed upon during discovery.

j. Describe the technical architecture and software that make up the solution. Description is accompanied by technical architecture schematic demonstrating where the hardware and software exist in the product infrastructure.

III. IMPLEMENTATION REQUIREMENTS

L. Knowledge Base Requirements

232. The Vendor shall provide an entity relationship diagram and data dictionary, in a format approved by MSDH.

233. The Vendor shall describe all business rules/edit checks that will be used for the solution.

234. The Vendor shall provide a mockup or actual screen designs presented to the appropriate MSDH personnel.

235. The Vendor shall request and incorporate feedback on screen designs from MSDH and describe their process for selecting and implementing requested changes and suggestions into the design.

M. Vendor Acknowledgement

236. This section outlines the MSDH minimum expectations of the awarded Vendor for implementation of the selected solution. Implementation deliverables will reveal the Vendor's expertise in project management, process management and improvement, data migration, and acceptance testing, etc. MSDH expects the proposed preliminary Implementation Plan to be refined by the awarded Vendor and MSDH project managers during the implementation process. Whether the awarded Vendor will need to be onsite at any time will be determined by the implementation project demands. MSDH reserves the right to require onsite Vendor participation if it would be in the best interest of MSDH.

237. The State expects the awarded Vendor to be responsible for design, configuration, implementation, testing, training (technical and program oriented), hosting, maintenance, and support of the awarded solution.

238. The State expects implementation with limited interruption to incumbent services and business operations. Any interruption to such operations must be approved by MSDH and conducted in a way to prevent loss of service.

239. Upon award, MSDH intends for the requirements set forth in this Attachment A and the Vendor's proposal, including any subsequent, agreed upon provisions and revisions, to act as the Implementation Statement of Work.

N. Project Management Requirements

240. The Vendor shall provide a preliminary Implementation Plan with the proposal with timelines and MSDH resources (triple constraints). The Implementation Plan shall include a description of the methodologies and strategies, timelines, MSDH resource requirements, etc. (e.g. timeframes and strategies for completing all discovery (JAD Sessions) related plans required for implementation). NOTE: MSDH SMEs shall have no more than 25% availability to support the implementation of the IDSP).

241. *Background: MSDH's Information Technology Strategic Realization Office has conducted a preliminary assessment of the IDSP project with the program area*

stakeholders in order to identify the criticality and flexibility of the triple constraints of this project.

MSDH is providing information to the RFP partners in order to give them foreknowledge of the areas that have the least and most flexibility for planning purposes. Where applicable, slack in each constraint is an opportunity for the respondent to provide additional features/recommend improvements in business processes and generally advise MSDH of best practices that will improve the final IDSP result.

The Constraint Information below is provided <u>for informational purposes only</u> and will need to be reassessed during discovery and contract negotiations with the selected vendor. This information will not be scored however it may provide the responding vendors opportunities to be innovative in their response which may lead to up-scoring.

Project Triple Constraints

i. Performance Criteria (See Functional Requirements)

ii. Schedule Constraint (2 Year Implementation)

iii. Budget Constraint ($XXXXXXX)

a. Driver and Weak Constraint

i. Driver: Performance Criteria

ii. Weak Constraint: Schedule

242. The Vendor shall follow industry standard best practices Project Management Institute (PMI), Project Management Body of Knowledge (PMBOK), and the specific project management processes at MSDH. These processes do not dictate how the project must be managed but demand deliverable standards supporting review and referencing without undue burden or training.

243. The Vendor must follow an Agile Project Management approach and use Microsoft (MS) Project, DevOps (CI/CD), or another comparable tool to manage and track project progress and implementation. The Vendor shall describe the implementation and scheduling methodology.

244. The Vendor shall prepare a Project Management Plan, maintain the plan throughout the project, and utilize the plan for the comprehensive management of the project. The first draft of the PMP must be included with the proposal response. An updated PMP must be provided after Implementation.

245. The Vendor shall develop Project Artifacts when appropriate in the schedule including responsibility for:

a. Periodic Progress Reports, as defined by MSDH;

b. Project Workplan updates every other week;

c. A key project states breakdown with criteria defining success for each;

d. All deliverables and plans described in Section E; and

e. Vendor must provide and realistic sample product Maintenance Schedule with the response to the RFP.

246. The Vendor is responsible for discovery and clarification to ensure it has a clear understanding and interpretation of the requirements, the MSDH environment, interoperability, technical infrastructure, and MSDH policies. Discovery is considered JAD sessions, validation sessions, and working sessions. The following are Vendor responsibilities:

    a. Scheduling discovery meetings and sending invites;

    b. Providing agendas, diagrams, handouts, prior meeting recaps, parking lot capture; and

    c. Notes, JAD Notes, decisions, action items, minutes, and roll.

247. The Vendor shall prepare a Project Workplan with MSDH and Vendor tasks, timelines, MSDH SME and Vendor resource allocation, integration, testing, data migration, move to production, warranty period, and transition to the new system using the proposed development lifecycle processes. An example will be submitted with the proposal. The Workplan will contain:

    a. Activities required for the project;

    b. Sequencing of activities, considering dependencies;

    c. Resources assigned to the activities and their hourly allocations;

    d. Durations of the activities; and

    e. Timeline schedule

O. Test Plan

248. The Vendor shall provide in the proposal a description of their testing methodologies, processes, tools, roles / responsibilities and descriptions of other client integrated disease surveillance system UAT experiences.

249. If awarded, The Vendor shall collaborate with MSDH programs and OHIT to produce an updated Test Plan to be approved by MSDH before UAT begins. The Test Plan shall describe any testing methodologies used for the MS IDSP as well as MSDH resource requirements, specific MS documentation and supporting resources (e.g. updated test scripts, test data, schedules, etc.) that will used to produce a product / process that meets all requirements.

250. The Vendor shall submit a Test Plan with the proposal. After award and discovery, the final Test Plan shall include:

    a. The Vendor shall develop test scripts and test data set for UAT. Please describe the methods and tools used to create and update all test scripts.

    b. The Vendor shall describe the methods and tools used to report, triage, estimate, track, and resolve defects and change requests.

    c. The Vendor shall describe the testing methodology used to conduct a holistic system test that culminates in the delivery of a product meeting all MSDH requirements and warranted to be defect free by the Vendor.

    d. The Vendor shall describe the testing methodology used to conduct data quality testing of all ELR interfaces to the new system. The testing methodology will be used to establish a data quality baseline for each interface.

e. The Vendor shall provide a clear testing process for validating the vendor's onboarding of ELR/eCR providers from initial connection through all testing required to ensure proper data mapping, and approval for making the connection live in production.

f. The Vendor shall describe the testing methodology used to conduct a user acceptance test that validates to MSDH that the system meets all MSDH requirements and operates within MSDH infrastructure, meets state and federal requirements, and operates within user workflows to accomplish the IDSP mission.

g. The Vendor shall describe all environments necessary to accomplish testing.

h. The Vendor shall describe all roles and responsibilities related to testing.

251. The Vendor shall provide the following updated documents prior to system or acceptance testing: system test cases, test data sets and scripts (to include ELR and all/other interoperability functionality), user acceptance test cases and scripts, the execution method, a Requirements Traceability Matrix (RTM), and testing entrance and exit criteria.

252. The Vendor shall provide periodic (as defined by MSDH) testing status updates designed to show progress against the baseline and evidence the testing progress is adequate to meet schedule expectations.

253. The Vendor shall plan, organize, and manage an MSDH user acceptance testing period. MSDH requires a testing period after system delivery in a pre-production environment (User Acceptance Testing).

254. MSDH plans to review system functionality, ELR workflow, converted data, inter-system interfacing, deduplication, matching and merging functionality and policy compliance within the new system prior to implementation.

255. The Vendor shall provide a holistic system demonstration after System Testing, at the start of UAT. The demonstration will show the system is fully functional, all requirements are implemented, data conversion is complete, and the system does fit state and MSDH policy, security, staff, and external user usage scenarios.

256. The Vendor shall provide the completed RTM at the completion of UAT showing each requirement, the system and UAT testing performed for each requirement, and the testing results.

P. User Training and Documentation

257. Training Plan

a. The Vendor shall submit a Training Plan with the proposal. The Vendor shall describe their proposed training approach that meets MSDH requirements and achieves adequate end user, program administrator training, MSDH OHIT system administrator training. At a minimum, the Vendor shall include in the Training Plan specific training for each separate program area (EPI, TB, STD/HIV). The plan must include scheduling, curriculums, and training modalities (e.g. interactive computer-based training, webinars, on-site, train-the trainer models, etc.). The Vendor shall provide program and OHIT training to include, but not limited to: ad hoc querying, reporting, exporting, data entry, forms creation, Health Level 7 (HL7) messaging, data visualization and analytics capabilities, Fast Healthcare Interoperability Resources (FHIR), and

eCR (Electronic Case Reporting) and Electronic Laboratory Reporting (ELR) management, geographical, and disease management, etc.

b. The Training Plan shall describe end user training (to include external end users who use the online reporting tool) that is role specific and includes all aspects of using the proposed system to support their program role. Final details regarding an MSDH specific training plan for end users will be included in the updated Training Plan submitted after JADS/discovery.

c. The Training Plan shall describe program administrator training that includes all aspects of configuring the system and functionality for use. Examples to include but not limited to: how to create surveys and forms, how to configure new data sources, disease mapping, GIS mapping, how to manage queues, data quality monitoring tools, analytics, how to change business rules, user level access and security, alter drop down lists, modify diseases from data entry screens, etc. without the help of a programmer. Final details regarding a MSDH specific training plan for program administrators will be included in the updated Training Plan submitted after discovery.

d. The Training Plan shall describe OHIT system administrator training to include, but not limited to: all electronic incoming data flows (workflow(s) and management), message baseline monitoring, and integrations. The Training Plan shall include training for OHIT staff to support the system in off-hours or in emergencies, all areas where MSDH staff can interact, quality control, correct, and maintain the Solution when circumstances require such actions. Final details regarding a MSDH specific training plan for OHIT / system administrators will be included in the updated Training Plan submitted after discovery,

258. The Training Plan shall include a description of all environments and training resources (to include MSDH staff) needed to meet the RFP requirements, during implementation and M&O. Vendor shall provide a Training environment use after implementation.

259. The Vendor will be responsible for conducting all trainings during implementation and after system updates unless noted in the final, accepted Training Plan delivered after award and JADS/discovery.

260. In addition to conducting trainings, the Vendor shall develop a variety of short, program oriented, how-to sheets for MSDH staff that will encompass all training provided. A final federated administrator training list will be established by the Vendor with the client once all system capabilities are known.

261. In addition to conducting trainings, the Vendor shall provide modifiable user documentation to include a user manual, electronic training guides, and training materials for Agency review and approval prior to system implementation.

262. In addition to conducting trainings, the Vendor shall use a variety of training materials to include but not limited to Computer-Based Training (CBT) solutions, videos, Technical Administrative training, Program Administrative training, user training (train-the-trainer), update training manuals, quick reference guides, and system/version update training.

263. The Vendor shall regularly update user documentation, in a timely manner, training materials, and electronic training guides and materials to support training instruction after each system update or as required.

IV. Software Administration and Security

Q. General

264. For hosted services, the design must be compliant with the State of Mississippi Enterprise Cloud, Offsite Hosting Security Policy, and MSDH Vendor Risk Management Policy. The State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy can be found on the ITS website (www.its.ms.gov).

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

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

267. Solution must prevent unauthorized access to the system.

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

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

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

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

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

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

274. Solution must accommodate two-factor authentication.

275. The Vendor shall provide a System Security Plan (SSP) that is based on National Institute of Standards and Technology (NIST) 800 standards. The plan includes the following at a minimum:

    a. Establish the standards and best practices that ensure security for all data and messages specific to protected public health data;

    b. The plan must remain current to NIST 800 changes and list the NIST 800 sections and controls covered in the SSP.

    c. The SSP is expected to support periodic audits and shall be structured and revised as necessary to accomplish that purpose.

R. Cloud Hosting Requirements

276. Data Ownership: MSDH 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 MSDH User accounts, or MSDH 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 MSDH's written request.

277. 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 MSDH information at any time. To this end, the Vendor shall safeguard the confidentiality, integrity, and availability of MSDH information and comply with the following conditions:

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

    b. At no time shall any data or processes which either belong to or are intended for the use of MSDH 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 MSDH.

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

279. Encryption

    a. The Vendor shall encrypt all non-public data in transit regardless of the transit mechanism using MSDH approved encryption methodologies and standards which are NIST 800 data in transit encryption standards.

    b. The Vendor must submit encryption methodologies in writing annually for MSDH approval.

    c. For engagements where the Vendor stores non-public data, the data shall be encrypted at rest. The key location and other key management details will be discussed and negotiated by both parties. Where encryption of data at rest is not possible, the Vendor must describe existing security measures that provide a similar level of protection. Additionally, when the Vendor cannot offer encryption at rest, it must maintain, for the duration of the contract, cyber security liability insurance coverage for any loss resulting from a data breach. The policy shall comply with the following requirements:

        1. The policy shall be issued by an insurance company acceptable to MSDH and valid for the entire term of the contract, inclusive of any term extension(s).
        2. The Vendor and MSDH shall reach agreement on the level of liability insurance coverage required.
        3. The policy shall include, but not be limited to, coverage for liabilities arising out of premises, operations, independent contractors, products, completed operations, and liability assumed under an insured contract.
        4. At a minimum, the policy shall include third party coverage for credit monitoring. notification costs to data breach victims; and regulatory penalties and fines.
        5. The policy shall apply separately to each insured against whom claim is made or suit is brought subject to the Vendor’s limit of liability.
        6. The policy shall include a provision requiring that the policy cannot be cancelled without thirty (30) days written notice.
        7. The Vendor shall be responsible for any deductible or self-insured retention contained in the insurance policy.

8. The coverage under the policy shall be primary and not in excess to any other insurance carried by the Vendor.
9. In the event the Vendor fails to always keep in effect the insurance coverage required by this provision, MSDH 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.

280. Breach Notification and Recovery: Unauthorized access or disclosure of non-public data is a security breach. The Vendor will provide immediate notification, and all communication shall be coordinated with MSDH. 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 three (3) years, mailing costs, Website, and toll-free telephone call center services. MSDH 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 MSDH to hold a Vendor harmless. All breach and recovery measures shall be in compliance with MSDH policy.

281. Notification of Legal Requests: The Vendor shall contact MSDH 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 MSDH. The Vendor shall not respond to subpoenas, service of process, and other legal requests related to MSDH without first notifying MSDH unless prohibited by law from providing such notice.

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

a. Suspension of services: During any period of suspension of this Agreement, for whatever reason, the Vendor shall not take any action to intentionally erase any MSDH data.

b. Termination of any services or agreement in entirety: In the event of termination of any services or of the agreement in its entirety, the Vendor shall not take any action to intentionally erase any MSDH 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 MSDH data and shall thereafter, unless legally prohibited, dispose of all MSDH data in its systems or otherwise in its possession or under its control as specified in section 283(d) below. Within this 90-day timeframe, Vendor will continue to secure and back up MSDH data covered under the contract.

c. Post-Termination Assistance: MSDH 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 Level 6 in Table 3: SLA Matrix.

d. Secure Data Disposal: When requested by MSDH, the provider shall destroy all requested data in all 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 MSDH.

283. 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 MSDH's information among the Vendor's employees and agents.

284. Security Logs and Reports: The Vendor shall allow MSDH 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 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.

285. Contract Audit: The Vendor shall allow MSDH to audit conformance including contract terms, system security as appropriate. MSDH may perform this audit or contract with a third party at its discretion at MSDH’s expense.

286. Sub-contractor Disclosure: The Vendor shall identify all 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.

287. 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.

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

V. SUPPORT AND MAINTENANCE

S. Service Level Agreements

289. In the interest of consistency across all MSDH’s IT systems, the following table is used to categorize and define service level, service request, and breach condition severity and impact levels of reductions in system performance from the baseline. The awarded vendor shall agree to adhere to the structure of the SLA Matrix and shall provide reporting to MSDH on ticket volume and SLA breaches based on the Time to Respond and Time to Resolve metrics. NOTE: Incident/Problem Resolution Time is calculated from the time an incident/problem is reported to the vendor, until the problem has been identified as resolved by MSDH. It is not calculated from when it is entered into a help desk ticketing tool.

Table 3: SLA Matrix

The purpose of the SLA Matrix is to objectively measure the quality of service, identify areas for improvement, and maintain business continuity. By using the SLA Matrix, the agency is hoping to meet these objectives while avoiding a zero-defect mentality.								
Ver #1								
SLA Level	**Severity**	**Impact**	**Time To Respond**	**Time To Resolve (RTO)**	**RPO**	**Acceptable Percentage**	**Compliance Method**	**Enforcement Mechanism**
6	Non-critical Functionality Degraded with Workaround	Less than 10 users	24 Hours	168 Hours	NA	98%	Monthly SLA Metrics Report	1% a day if more than 50 Level 6 tickets are open.
5	Non-critical Functionality Degraded with Workaround	10+ Users	12 Hours	72 Hours	NA	98%	Monthly SLA Metrics Report	1% a day if more than 50 Level 5 tickets are open.
4	Non-critical Functionality Unusable w/o Workaround or Critical Functionality with Workaround	Less than 10 users	1.5 Hours	24 Hours	NA	97%	Monthly SLA Metrics Report	1% a day if SLA percentage drops below 97%
3	Non-critical Functionality Unusable w/o Workaround or Critical Functionality with Workaround	10+ Users	45 Minutes	12 Hours	NA	96%	Monthly SLA Metrics Report	1% a day if SLA percentage drops below 96%
2	Critical Functionality Interrupted, Degraded, or Unusable w/o Workaround	Less than 10 users	1 Hour	6 Hours	NA	96%	Monthly SLA Metrics Report	2% per day if SLA drops below 96%
1	Critical Functionality Interrupted, Degraded, or Unusable w/o Workaround	10+ Users	30 Minutes	4 Hours	Zero	95%	Monthly SLA Metrics Report	2% per day if SLA drops below 95%
CO	**Complete Outage**	**NA**	**30 Minutes**	**1 Hour**	**Zero**	**95%**	**Monthly SLA Metrics Report**	**0.5% per hour if SLA drops below 95%**

290. Root Cause Report: The Vendor shall provide a Root Cause Analysis (RCA) for all complete system outages within five (5) business days of the resolution. The report

shall describe the root cause of the incident, the actions that resolved the incident, and steps taken to avoid future similar incidents.

291. **MANDATORY:** Reporting Requirements: Vendor shall provide a monthly report to MSDH by the seventh (7th) business day of the following month. Failure to provide the monthly report by the seventh (7th) working day of the following month shall be assessed a penalty of $2,500 per day until the report is delivered. The Monthly SLA report should include:

a. SLA performance metrics by instance;

b. Internal monitoring, including metrics and tools used;

c. Incidents and/or problems incurred per defined SLAs;

d. Help desk statistics including contacts by users, MSDH staff and beneficiaries, tickets generated and closed by severity, who reported the issue, by instance, escalations, problem resolution rates, opt-in and opt-out requests, and those that were processed;

e. Total ticket volume with aging by severity, tickets opened and closed during the last period, by support, maintenance, and upgrades;

f. Monthly hardware statistics and monitoring reports; and

g. Other metrics to be defined by MSDH in coordination with the Vendor

292. Scheduled Downtime: Agreed upon and scheduled downtime shall occur only between 1:00 a.m. and 4:00 a.m. Central Time. Solution downtime outside of the allowable downtime period shall be categorized as unscheduled downtime and is subject to a monetary penalty for each occurrence, as is outlined in Table 3: SLA Matrix.

293. The Vendor shall host the proposed solution in a United States-based Tier 2 data center or better, with written approval from MSDH on any change in the selection of the data center, data center Vendor, and location. MSDH reserves the right to physically audit (by State or State contracted personnel) the data center the proposed solution is hosted in and the Disaster Recovery (DR) site. By the first ninety (90) days after contract execution and on every August 30th thereafter, the Vendor must provide MSDH with an annual data center report, specifying their Tier Certification of Constructed Facility rating or Technology Innovation Agency (TIA)-942 Data Center Standard Rating, specifying the Tier rating of their facility and specifying what certifications have been awarded to the facility, including but not limited to Leadership in Energy and Environmental Design (LEED), Statement on Standards for Attestation (SSAE) 16 (i.e.,. System and Organization Controls [SOC 1], HIPAA, etc.

294. Vendor shall have a failover process and documented Failover Plan that shall be provided to MSDH for approval upon system go-live.

295. Vendor shall have a Disaster Recovery (DR) Plan approved by MSDH upon system go-live, including a separate DR site with a separate physical location from the primary hosting site. Upon each anniversary of contract execution, the Vendor(s) shall provide documentation that the DR environmental test has been conducted within the past year and shall provide written results to MSDH. The written results shall include any remediation and the accompanying remediation

schedule necessary to correct any failures or findings that were identified because of the DR test.

296. Vendor and all subcontractors shall adhere to the appropriate SLAs. All subcontractor non-performance and delays are the responsibility of the prime Vendor, and all penalties will be assessed to the prime Vendor.

297. Failure for any Vendor or subcontractor to meet the requirements of the Business Associate Agreement (BAA) ($2,500.00 per occurrence). An occurrence means each failure to comply with the BAA requirements, regardless of the number of persons or clinicians involved.

298. If any Vendor or subcontractor fails to notify MSDH of a privacy breach (potential or otherwise) both in writing and by telephone within twenty-four (24) hours of discovery, the Vendor shall be assessed damages of $25,000 per day until MSDH is properly notified. The Vendor shall pay the costs for notification of any breach, as well as for credit monitoring for all persons whose data is breached for the term of one year.

299. Failure by any Vendor to meet mutually agreed upon project deliverables and/or milestones by the due date or as otherwise required, without an approved change request may result in a penalty of $500.00 per instance, per calendar day that the deliverable or milestone remains late or deficient.

300. Failure by any Vendor to maintain staffing levels, including the number and qualifications of staff, and provision of key positions that are outlined in the requirements, is subject to a credit of $2,500.00 per calendar day.

301. Failure by the Vendor to obtain approval in writing by MSDH for publishing material requiring MSDH approval is subject to a penalty of up to $1,000.00 per instance.

302. Unauthorized use of MSDH's name, brand, or likeness is a violation of this contract ($1,000.00 per occurrence). An occurrence means each unauthorized use.

303. Failure of Vendor to comply with close out and turnover requirements may result in the assessment of damages of up to $25,000.00 that, if imposed, shall be deducted from the final payment to be made to Vendor.

304. Unauthorized utilization of any MSDH derived data is a violation of the requirements listed herein is subject to a penalty of up to $10,000.00 per occurrence. An occurrence means each unauthorized use, regardless of the number of persons or Trading Partners involved.

305. Failure to meet the requirements of Health Insurance Portability and Accountability Act (HIPAA) ($1,000.00 per occurrence). An occurrence means each improper use or disclosure of person information.

306. Any other failure of any Vendor that MSDH determines constitutes substantial non-compliance with any material term of the Contract not specifically enumerated herein, may result in a penalty of up to $5,000.00 for each failure.

307. Liquidated Damages and Corrective Action Plans

a. MSDH may require corrective action if any deliverable, report, SLA, or the like should indicate that the Vendor is not in compliance with any provision of this RFP. MSDH may also require the modification of any policies or procedures of the Vendor relating to the fulfillment of its obligations pursuant to this Contract.

MSDH may issue a deficiency notice and may require a corrective action plan be filed within fifteen (15) calendar days following the date of the notice. A corrective action plan shall delineate the time and way each deficiency is to be corrected. The Corrective Action Plan (CAP) shall be subject to approval by MSDH, which may accept it as submitted, accept it with specified modifications, or reject it. MSDH may extend or reduce the time frame for corrective action depending on the nature of the deficiency and shall be entitled to exercise any other right or remedy available to it, whether it issues a deficiency notice or provides Vendor with the opportunity to take corrective action.

b. Because performance failures by the Vendor may cause MSDH to incur additional administrative costs that are difficult to compute, MSDH may assess liquidated damages against the Vendor pursuant to this section and deduct the amount of the damages from any payments due the Vendor. MSDH, at its sole discretion, may establish an installment deduction plan for any damages. The determination of the number of damages shall be at the sole discretion of MSDH, within the ranges set forth below. Self-reporting by the Vendor will be taken into consideration in determining the number of damages to be assessed. Unless specified otherwise, MSDH shall give written notice to the Vendor of the failure that might result in the assessment of damages and the proposed amount of the damages. The Vendor shall have fifteen (15) calendar days from the date of the notice in which to dispute MSDH's determination. MSDH may assess damages for specific performance failures set forth below. MSDH may assess higher liquidated damages amounts when the Vendor consistently fails to meet specific performance standards, and the deficient performance has not been corrected.

c. Assessment of actual or liquidated damages does not waive any other remedies available to MSDH pursuant to this RFP or state and federal law. If liquidated damages are known to be insufficient, then MSDH has the right to pursue actual damages.

d. Failure to timely submit a MSDH approved Corrective Action Plan (CAP), MSDH may assess liquidated damages of $2,500.00 per business day until the CAP is submitted.

e. Failure to successfully carry out a MSDH approved CAP within the time frames outlined in the CAP, MSDH may assess $5,000.00 per business day until the CAP is completed.

f. In the event of repeated violations of a single SLA measure or multiple failures across SLA measures over two consecutive months, MSDH reserves the right to renegotiate SLA measures and/or escalate the applicable reductions by 50% of the stated liquidated damages after non-responsiveness. Repeated violations may be grounds for Termination for Cause.

T. Customer Support

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

309. Vendor must provide a toll-free telephone number for MSDH staff to call 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.

310. 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.

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

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

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

U. Issue Tracking

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

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

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

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

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

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

320. Details of MSDH 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.

321. The Vendor shall provide a monthly issue tracking report as defined by MSDH. 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 MSDH.

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

V. System Monitoring

323. Vendor shall describe their monitoring services to cover all the provided services including but not limited to:

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

    b. Application monitoring;

c. Services running on the operating systems;

d. Performance indicators such as metrics and logs across application resources and technology stacks, database and application servers, operating system, load balancers, network latency, and queues, etc.;

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

f. Trending (for minimum of one year); and

g. Sharing of the monitored data with MSDH through a portal.

324. Vendor shall describe how it is alerted to conditions that represent a failure to meet the agreed upon SLA thresholds in Table 3: SLA Matrix and how that information will be provided to the State.

W. Product Updates

325. The State requires notice in advance of product updates.

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

1. Security Updates;

2. System Maintenance;

3. System Enhancements; and

4. Education and Training.

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

327. Enhancements and updates must be included with annual maintenance fees which must be included in RFP No. 4635, Section VIII, Cost Information Submission.

X. Software Updates

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

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

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

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

330. 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.

331. 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.

332. 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. Any and all obligations of the third-party software are the responsibility of the proposing Vendor. The State will not execute any third-party software agreements.

Y. Warranty/Maintenance Requirements

333. The solution shall minimize requirements for in-house technical maintenance resources, specialized training, or knowledge in order to implement, configure, update, and/or maintain the system.

334. The Vendor shall be capable of providing ongoing maintenance, support, upgrades, and troubleshooting.

335. Vendor shall include applicable support fees to include maintenance and hosting to be included in the initial implementation costs.

336. Vendor shall be able to provide warranty on the software and system operability for a minimum of one year, beginning on the date of acceptance.

VI. DELIVERABLES

337. Vendor must agree to provide the deliverables described in **Table 4** below. The vendor's Implementation Plan must include and consider resource and project constraints. Implementation approaches that take into consideration MSDH resource availability may be awarded additional points or consideration in the proposal evaluation.

So that the State can evaluate Vendor capabilities, proposing Vendors must submit preliminary deliverables as specified with the proposal. Preliminary deliverables should contain as much detail as possible to show understanding of and compliance with the specific RFP requirements. Post award and prior to implementation, the Vendor will conduct sufficient discovery and with MSDH approval, will amend deliverables as stated in the table. MSDH approval is required for all deliverables prior to implementation.

Table 4: Deliverables

Deliverable	Due/Update
Deliverable/Milestone #1 Project Initiation - Project Planning Schedule (Discovery / JAD Schedule, Milestones, etc.) - Kickoff/Discovery and Project Methodology	Due with proposal; Final due after JADs/discovery and MSDH approval before implementation begins
Deliverable /Milestone #2 Approved Plans for Implementation Project Management Plan Staffing Plan* Requirements Traceability Matrix (RACI) Data Migration Plan* Integration/Interoperability Plan* Training Plan* Test Plan*	Final due after JADs/discovery and MSDH approval before implementation begins NOTE: Plans with * are to be delivered with the proposal

Growth / Surge Plan* Cloud Architecture Diagram and SOP* System Security Plan SaaS Product Development Plan* SaaS Data Turnover Plan Business Continuity Plan* Disaster Recovery Plan* Failover Plan SOP/Configuration Guide Implementation Plan* (Other IT Required Plans)	
Deliverable / Milestone #3 - Solution Implementation Implemented Data Conversion/Migration Plan Project Work Plan Implemented Testing Plan Implemented Training Plan Implemented Integration / Interoperability Plan User interface and system configurations Alerting/Dashboard Capabilities Message Mapping guide implementation RVCT Implementation User Documentation and User Manuals Surveys/Forms Capabilities ELR / eCR Capabilities GIS Capabilities QHIN Connectivity / TEFCA Public Health Uses Cases Implemented All required CDC and Other Federal Reporting Auditing and Security Tier 1 and Tier 2 Help Desk Support Project Management Activities Other use cases identified during discovery	Due as defined in the Implementation Plan, RFP Functional Requirements, SOP/Configuration Guide, and final Plans Required for Implementation
Deliverable Milestone #4 On-Going Project Management On-Going Post Implementation On-Boarding and Data Quality Monitoring On-Going Tier 2 Help Desk Support On-Going Sustainment Training Monthly Project Status Reports Required SLA Reports Monthly IDSP Steering Committee Updates Quarterly MSDH Executive Update Other Project Management duties as required	
Deliverable Milestone #5 System Acceptance - Approved Final Deliverable	

338. The Vendor shall prepare a Project Management Plan, including but not limited to the components listed below, that will assist in the comprehensive management of the project.

- Scope Management;
- Schedule Management;
- Quality Management;
- System Change Management;
- Configuration Management;
- Communications Management;
- Issues & Risks Management;
- Assumptions and Constraints;

339. The Vendor shall provide electronic copies of draft and final documentation and deliverables. Electronic copies shall be provided in MS Office format unless otherwise specified or approved by the State.

340. Deliverable Standards: For each required deliverable or group of related deliverables, the awarded Vendor must develop a Deliverable Expectation Document (DED) in advance of the scheduled start of any tasks or subtasks that produce the deliverable as described above.

341. Approval and Rejection of Deliverables: The awarded Vendor must submit each deliverable to the State for review, comment, and approval. The State's review period varies with the type, complexity, and volume of the deliverable. The Vendor must include adequate estimates for State review, comment, and any Vendor re-work time in the Project Schedule. For the Vendor's estimation purposes, the State's default review period shall be ten (10) business days, unless an alternative review period length is requested in writing.

342. In the event the State finds a deliverable to be unsatisfactory, the State shall notify the awarded Vendor of the reason(s) for deliverable rejection in writing. The State shall meet and confer with the Vendor to provide clarifications as requested or needed. The Vendor must then correct and resubmit the deliverable within agreed timeframes that vary with the type, complexity, and volume of the deliverable. Rejection of a deliverable by the State does not provide permission for delays in delivering subsequent deliverables unless approved by the State.

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