Medicaid Management Information System Replacement (MMISR) Project

Contractor Qualifications and Work Products

System Integrator

June 30, 2020

Table of Contents

Introduction

The Human Services Department (HSD) requires any organization awarded this System Integration contract possess the necessary resources, knowledge, business techniques, and technical abilities to manage the completion of this system.

To confirm a baseline level of these qualifications, this document details ten (10) essential areas related to system design, development, and implementation. An eleventh section addresses ongoing maintenance and operations.

In many cases, not all areas of technical expertise are available within one (1) contractor organization. These criteria also serve to clarify the HSD's expectations for any subcontracted expertise utilized to complete the project under the Contractor's supervision. Contractors are encouraged to create subcontractor relationships to bring the "best of industry" companies and qualifications into this engagement.

A separate document titled Instructions for Responding to this Request for Quote (RFQ) instructs how the responding Contractor must describe their expertise related to these qualifications and how to present their fixed price quote for each of the work products.

The engagement resulting from this RFQ will form the central integrating component of the larger Medicaid Management Information System Replacement (MMISR) project and the Health and Human Services 2020 (HHS2020) Enterprise initiative. Contractors should inform themselves regarding these projects by reading the overview approach below and consulting the procurement library of related procurements and supporting documentation.

The NM Procurement Library link is https://webapp.hsd.state.nm.us/Procurement/

Initial Enterprise Milestone Estimates:

In preparing this RFQ, the New Mexico (NM) HSD Information Technology Department (ITD) team developed the initial estimates below for the work required to complete the final production ready instantiation tasks for the key functionality required by the MMISR enterprise partners

Milestone	Due Date
ASVV Instantiation	1/07/21
EDM/CCM Instantiation	2/08/21
ESB Instantiation	2/19/21
Infrastructure Configured/Available	3/08/21
IDM Instantiation	5/04/21
MDM Client	8/04/21
MDM Provider	9/07/21

The milestone due dates above, are not-to-exceed dates, to make the base functionality of the Commercial off-the Shelf (COTS) product/services available (instantiated) in the shared System Integration Test (SIT) environment to be consumed as a service by the enterprise - both modules and enterprise partners.

After instantiation, the ongoing configuration of these COTS product/services with the modules and support for enterprise partners' business needs will continue to build out the service.

Beginning in 2021, as COTS product/services mature and the enterprise is ready to transition these to a production environment, the environment and services must be established, and the required Maintenance and Operation (M&O) support activity begins. During M&O there will be continuous integration and development efforts to enhance the services and technology as the enterprise matures.

1.0 Service Orientation

1.1 Contractor Qualifications

The procuring HSD believes that for a successful outcome, the Contractor qualifications must meet the following minimums:

1) Two (2) or more proven successful implementations of Oracle Fusion Middle Ware (OFMW) currently operating in production systems.
2) Five (5) or more years of company experience with OFMW development and implementation.
3) Proven and well-defined requirements elicitation, validation, and traceability processes.
4) Proven iterative and continuous development implementation processes to support multiple integrated systems' simultaneous development and enhancement lifecycles with many production promotion events.
5) Ability to fully staff multiple workstreams to support multiple simultaneous product development lifecycles in various stages of progress ultimately converging into one interoperating enterprise. Staff the engagement team with:
    a) Sufficient staffing with certified Oracle professionals
    b) Business Analysts and development professionals experienced with OFMW
    c) Proven Service Oriented Architecture (SOA) experience and SOA certified staff
    d) Proven Jama/Jira/Confluence experience
    e) Proven Medicaid systems and Centers for Medicare and Medicaid Services (CMS) certification experience

1.2 Work Products

1.2.1 Orchestration Plan and Implementation

As part of System Integrator (SI) role, it is required that the SI conduct business analysis in order to develop and implement the rules that will leverage the OFMW and other technology components to orchestrate different MMIS modules to communicate between each other and outside enterprise partners. The OFMW includes an Enterprise Service Bus (ESB), a Business Rules Engine (BRE), Business Process Execution Language (BPEL), Electronic Data Interchange (EDI) and numerous other components to enable this work. As part of this work, the state requires the following to be addressed in the Implementation Plan for Orchestration requirements discovery and solution implementation:

1) Elicit requirements from business and technical Subject Matter Experts (SMEs).
2) Define end-to-end system flows from Medical Assistance Division (MAD) and the HHS 2020 partners provided Business Transformation Council Journeys, user stories, and known requirements including:
    a) Module contractor coordination
    b) Discovery of module functionality

   c) Define integration points with modules
   d) Service Oriented Architecture (SOA) enablement of Medicaid business flows
3) Define SOA enabling of Medicaid and HHS2020 partners end-to-end data flows in conjunction with system flows. Of particular importance is the routing of Medicaid claims transactions and other standardized electronic transactions between legacy modules, new modules, State agencies and external partners such as clients, providers, managed care organizations, employers, and CMS.
4) Define OFMW implementation to build service enablement, encapsulation, and abstraction of the integrated Commercial off-the Shelf (COTS) products and module applications creating a loosely coupled enterprise.
5) Implementation plan must:
   a) Include all applications and components of OFMW
   b) Meet business needs and module contractor functionality needs
6) Define a plan for incorporating applications and modules into the enterprise as they are acquired, and interoperations needs become apparent. Including:
   a) Approach for anticipating and organizing the work
   b) Methodology of requirements elicitation and validation with module contractors and gaining agreement on integration scope and interoperability details
   c) Methodology for structuring the work into segments that are easily monitored, evaluated, and reported for progress
   d) Methodology for organizing and sustaining work progress in multiple streams because many applications and modules will require parallel time frames for integration.
   e) Backlog methodology
   f) Methodology for testing integration tools and frameworks
   g) Methodology for testing end-to-end business processes and gaining user acceptance.
   h) Management and coordination of multiple timelines
   i) Management of and reporting on multiple parallel and staggered SDLC phases regardless of Module Contractor's chosen Software Development Life Cycle (SDLC) methodology i.e. agile, waterfall, hybrid, etc.
   j) Release management and production promotion of converging integration projects
   k) Incorporation of these above activities into the contractor's project schedule and summarized into the Enterprise Project Management Offices (EPMO's) Enterprise Project Schedule (EPS)
   l) Progress and velocity reporting on all workstream integrations
7) Fully implement items from the Orchestration Implementation Plan described in bullets 1 through 6 above; as approved by the HSD.

1.2.2 Interfaces Plan and Implementation

In consideration of the role of system integration across modules and systems, the need to create and/ or access interfaces is a must. In addition to the Oracle Fusion Middle Ware suite, additional Application Programing Interfaces, as well as future identified interfaces will need to be created and/or accessed. As part of this work, the HSD requires the following to be addressed in the Implementation Plan for interface development and Application Programming Interface (API) service enablement requirements discovery and solution implementation:

1) Assess current installation of interface API service enablement in four (4) environments.
    a) Identify deficiencies of configuration/setup
    b) Define a plan to correct deficiencies or replace interface configuration(s)
    c) Test plan/testing/ test results to validate interface service readiness
2) Assess AS-IS interface catalog.
    a) Determine completeness
    b) Elicit requirements from business SMEs, HSD technical SMEs and module contractor technical SMEs for enterprise sharing of interface(s)
3) Define a plan for service enablement of interfaces using middleware products such as API manager and Managed File Transfer (MFT).
4) Create backlog of interfaces.
5) Create interface projects in combination with end-to-end system flows.
6) Define a plan for incorporating applications and modules into the enterprise as they are acquired, and interface needs become apparent. Including:
    a) Approach for anticipating and organizing the work
    b) Methodology for structuring the work into segments that are easily monitored, evaluated, and reported for progress
    c) Methodology for organizing and sustaining work progress in multiple work streams because many applications and modules will require parallel time frames for integration
    d) Methodology for testing interface within the OFMW
    e) Methodology for testing end-to-end business processes and gaining user acceptance
    f) Backlog methodology
    g) Management and coordination of multiple timelines
    h) Management of multiple parallel and staggered interface development and deployment
    i) Release management and production promotion of converging interface projects
7) Fully implement items from the Interfaces Implementation Plan described in bullets 1 through 6 above; as approved by the HSD.

1.2.3 Assessment, Remediation, Plan, and Implementation for Oracle IDM Service

The HSD's current Oracle IDM implementation is in a state of partial completion. In order to complete this critical component for the modular MMIS system as well as enterprise partner agencies, the following work must be done:

1) Assess current instantiation(s) of Identity and Access Management (IdAM) in four (4) environments.
    a) Identify deficiencies in the current configuration/setup
    b) Create remediation plan for deficiencies that exist
    c) Create test plan, perform testing, provide test results to validate application readiness and participate in UAT
2) Assess IdAM service enablement.
    a) Validate service enablement
    b) Create test plan/perform testing, provide test results to validate service enablement and participate in UAT

3) Plan service enablement of IdAM for upcoming modules.
4) Fully implement service enablement of IdAM as assessed and planned above; as approved by the HSD.

1.2.4 Assessment, Remediation, Plan, and Implementation for Master Data Management (MDM)

Master Data Management (MDM) exists in a state of partial completeness using a NoSQL based on the Mark Logic tool set. In addition, MDM exists as both a service and a data set. In order to complete the service enablement, the following work must be done:

1) Assess current installation and configuration of MDM in four (4) environments.
    a) Identify deficiencies in the current configuration/setup
    b) Create remediation plan for deficiencies that exist
2) Assess MDM service enablement.
    a) Validate service enablement
3) Plan service enablement of MDM for upcoming modules.
4) Fully implement service enablement of MDM as assessed and planned above; as approved by the HSD.

1.2.5 Assessment, Remediation, Plan and Implementation for Address Standardization, Validation, and Verification (ASVV)

Address Standardization, Validation, and Verification exists in a start of partial completion. In order to successfully complete this critical item and make it available to the enterprise the following work must be done:

1) Assess current installation and configuration of ASVV in four (4) environments.
    a) Identify deficiencies of the current configuration/setup
    b) Create remediation plan for deficiencies that exist
2) Assess ASVV service enablement.
    a) Validate service enablement
3) Determine Verification possibilities.
4) Plan service enablement of ASVV for upcoming modules.
5) Fully implement ASVV and the service enablement as assessed and planned above; as approved by the HSD.
6) Perform ASVV database updates and maintenance activities.

1.2.6 Implement Hyland OnBase and Content Composer Implementation and Conversion

Hyland OnBase and Content Composer exist in a state of partial completion. In order to successfully complete this critical item and make it available to the enterprise the following work must be done:

1) Install and configure Hyland's OnBase and Content Composer in coordination with Hyland contract Statement of Work (SOW).
    a) Coordinate with Hyland for installation and configuration in four (4) environments
    b) Perform service enablement implementation (API Manager)
    c) Perform unit/integration/system testing and produce test results, assist with UAT testing.

d) Create conversion plan, converting electronic documents and notices from the existing systems to the new solutions.
e) Create conversion plan converting alerts and notifications from the existing systems to the new solutions
f) Execute conversion plans required in bullets above

1.2.7 Mailroom Imaging Plan and Integration

Contractor must integrate the Hyland OnBase and Content Composer applications with the HSD's current scanning/printing/communicating applications and locations.

2.0 Infrastructure

The HSD's infrastructure for the SI is in a state of partial completion. The platform is built upon the Dell/EMC VxRack Flex system leveraging VMware, Linux, and Windows Server software. In order to bring the infrastructure to a successful state of completion the following work described below must be completed. The work described below is not an exhaustive list of what will be required. There may be other tasks necessary for the successful implementation of the infrastructure.

2.1 Contractor Qualifications

The infrastructure contractor must have experience and expertise in the following categories:

Dell/EMC VxRack Flex includes

1) Configure, manage, support VxRack, VxFlexOS/ScaleIO
2) Upgrade Release Certification Matrix (RCM)
3) Monitor and update systems with Flex Manager

VMware includes:

1) Design, configuration, and management of VMware infrastructure
2) Implementation and management of the vRealize suite for resource management, monitoring, and automation
3) Implementation and management of VMWare network virtualization NSX both on premise and with expansion into the cloud

Strategic environment and capacity planning include:

1) Capacity analysis, planning and ongoing monitoring
2) Minimize infrastructure hardware requirements with flexible, build and use as needed in virtual environments
3) Cloud expansion and hybrid cloud environments

Disaster recovery, business continuity planning and backups/data protection includes:

1) Determine optimal disaster failover locations and configurations
2) Create a disaster recovery/business continuity plan
3) Create and document the process for failover and fall back
4) Plan and execute a backup, restore, and archive strategy
5) Knowledge of Dell's Integrated Data Protection Suite

Infrastructure, hardware, and virtual system performance monitoring, tuning, and troubleshooting includes:

1) Use proven tools to monitor the system, including vRealize Operations Manager (vROPs), and Flex Manager
2) Tune systems to increase performance
3) Determine root cause for performance issues

System administration includes:

1) Microsoft Windows operating systems
2) Red Hat Enterprise Linux
3) Microsoft Active Directory (AD), Domain Name System (DNS), Active Directory Federation Services (ADFS)
4) Cloud administration

Security infrastructure and operating systems includes:

1) Apply Minimum Acceptable Risk Standards for Exchanges (MARS-E) v2.0 and Pub 1075 Internal Revenue Service (IRS) Security Controls and Standards and other required controls to operating systems
2) Regular compliance and vulnerability scanning of all servers and remediation of findings
3) Regular vulnerability patching
4) Role-based and granular security for administration of servers
5) AD integration of all server operating systems (Red Hat Linux)
6) SElinux

Network includes:

1) Design an interconnected SOA platform
2) Switches, routers, firewalls, load balancers
3) VMware NSX

ServiceNow platform includes:

1) Administer and operate Information Technology Service Management (ITSM)/Information Technology and Operations Management (ITOM), Software Asset Management (SAM), Security Operations, and Compliance modules
2) Manage the Configuration Management Database (CMDB) and Discovery

Proven methods for infrastructure documentation include:

1) Inventories
2) Server builds and deployments
3) Server and infrastructure configurations
4) Standard Operating Procedures
5) Validation of all builds and configurations
6) Gathering requirements for infrastructure based on capacity analysis, Service Level Agreements (SLAs), design, and application specifications

Proven track record of sustaining long-term employment of many staff members holding certifications related to this infrastructure environment such as:

- VMware Certified Professional (VCP)

- VMware Certified Advanced Professional (VCAP)
- VMware Certified Design Expert (VCDX)
- Red Hat Certified System Administrator (RHCSA)
- Red Hat Certified Engineer (RHCE)
- Microsoft MCSA, MCSE
- Cisco CCNA

2.2 Work Products

Work Products below are applicable initially to the current infrastructure and ongoing to changes made to follow contractor recommendations and changes due to the normal evolution of the infrastructure.

2.2.1 Assessment of Current Infrastructure and Implementation of Approved Recommendations

Assess the current infrastructure, make recommendations on any reconfigurations or other changes, implement changes as approved by the HSD in the following areas:

1) VxRack hardware platform and inventory.
2) Virtual Machines and environments.
3) Current design, installation, and build documents.

2.2.2 Platform Management

Manage the integration platform on the VxRack VMware infrastructure including:

1) Create/update secure templates for server deployment.
2) Implement and configure vRealize suite, including automation for server/environment deployment.
3) Monitor and support the infrastructure.
4) Investigate the interactions with the HSD's Active Directory (AD) domain and advise on costs and benefits of creating and maintaining a test AD domain.
5) Work with the HSD security team to ensure the infrastructure is compliant with all security requirements.

2.2.3 Infrastructure Design

Create and document the infrastructure design based on the assessment, recommendations, and contractor best practices. Design should be specific to this project and the design of the integration platform including:

1) VMware virtual infrastructure
2) VMware vRealize Suite
3) VMware NSX

2.2.4 Capacity Analysis

Use the HSD's current Capacity Plan to assist with performing and documenting a capacity analysis of the current environment and future environment needs including:

1) Thorough understanding of the integration platform design and specifications.
2) Capacity needs for disaster recovery.

3) Any recommendations for capacity expansion, including to the cloud.
4) Process for capacity expansion.

2.2.5 Disaster Recovery/Business Continuity Plan and Implementation

Complete a robust Disaster Recovery (DR)/Business Continuity plan for the integration platform that includes how the other module contractors will coordinate with and use the plan including:

1) Analysis of capacity needs.
2) Propose and implement a DR site and strategy designed to meet the negotiated Recovery Point Objective (RPO)/Recovery Time Objective (RTO) according to the Business Impact Analysis (BIA).
3) Detail failover procedure.
4) Annual DR test lead by the SI and includes the Business Process Outsourcing (BPO) module contractors.
5) Implement the components of the plan and conduct testing.

2.2.6 Backup Strategy, Implementation and Management

Create, implement, and manage the platform backup strategy including:

1) Ensure that the platform is backed up and data retained according to the HSD's data retention requirements.
2) Work with the HSD's system administration team to configure the backups on the enterprise backup system.
3) Provide the HSD with accurate requirements for the amount of data from the integration platform that needs to be backed up with the HSD's backup solution.
4) Ensure that any lost or corrupted data can be recovered quickly, according to defined SLAs.

2.2.7 NSX Analysis and Implementation Plan

1) Assess the need and practical uses of NSX within the integration platform.
2) Design and plan the implementation of NSX in detail including timelines, with knowledge of the HSD's time constraints for purchasing.

2.2.8 Performance Test Plan

Create and implement a performance test plan that includes:

1) A strategy for performance testing in all environments at multiple steps along the process of implementing the integration platform.
2) Include load and stress testing.
3) Test and report the integration platform performance compared to performance SLAs.
4) Report integration platform performance results and recommended performance tuning.

2.2.9 ServiceNow CMDB Implementation Plan and Management

Implement and manage the ServiceNow CMBD:

1) Follow the established Requirements Management and Change Management Plans, create, and complete a project implementation plan for ServiceNow, the platform for enterprise management.
2) Instantiate, populate, and manage the ServiceNow CMDB.

3.0 Security

The SI is responsible for insuring system-wide compliance with state, federal, and industry standards on security. The unique nature of the SI at the center of the MMIS system puts it in a critical path for all security. The following are qualifications and work products necessary to successfully complete this role.

3.1 Contractor Qualifications

1) Expertise in implementing MARS-E v2.0, HIPAA, and Pub 1075 IRS Security Controls and Standards in a complex, multi-system interoperating transactional enterprise.
2) Two (2) or more successful implementations of MARS-E v2.0, HIPAA, and Pub 1075 IRS Security Controls and Standards currently operating in a production environment.
3) More than five (5) continuous years employing multiple staff members with certifications from International Information System Security Certification Consortium and Global Information Assurance Consortium.
4) Proven methods for creating technical security documents, requirements, use cases and test cases and test results.
5) Proven expertise in Confluence/Jama/Jira, Splunk, Nessus Scans (Contractor Supplied) and Safeguard Computer Security Evaluation Matrix (SCSEMs).
6) Proven experience implementing CMS & IRS Security Controls.

3.2 Work Products

3.2.1 Security Artifact Assessment

1) Assess current enterprise security infrastructure for completeness; identify deficiencies and recommend improvements. Artifacts to be reviewed and used in the infrastructure assessment include:
    a) Security Approach
    b) System Security Plan
    c) Security Design Plan
    d) Privacy Impact Analysis
    e) HSD Incident Response Plan
    f) HSD Plan of Action and Milestones
    g) HSD Business Continuity Plan
    h) HHS 2020 RFP Addendums, 14 - HHS 2020 Security Privacy and Standards
    i) HHS 2020 RFP Addendums, 21 - HHS 2020 Security Operational Guidelines
2) Implement the recommendations from above as approved by the HSD.

3.2.2 Security Document Creation

Write and gain HSD approval of security documents including:

1) Risk Assessment
2) Security Certification and Accreditation Letters
3) Security Questionnaire Document

4.0 Canonical Message Models

4.1 Contractor Qualifications

1) Two (2) or more proven successful implementations of a service-based enterprise integration platform using a Canonical Data/Message model approach preferably in healthcare payor, provider, pharmaceutical or medical device industries.
2) Five (5) or more years of company experience in Canonical Data/Message model development and implementation.
3) Proven expertise taking over an existing Canonical model implementation vs. starting from new model creation.
4) Proven expertise in COTS industry-specific canonical models, e.g. IBMs' Unified Data Model for Healthcare (UDMH).
5) Proven approach and expertise in adding model elements not covered by an existing functional standard, applying new element definition, naming etc.
6) Proven expertise in maintaining Canonical metamodel elements in IBM Information Governance Catalogue (IGC) or similar enterprise-level metamodel management platforms
7) Proven expertise modeling Canonical data and messages using Sparx Enterprise Architect (EA) tools or similar modeling platforms and notations.
8) Proven expertise using an industry standard model to extend an existing Canonical model to cover a Medicaid domain.

4.2 Work Products

4.2.1 Functional Analysis and Message Identification

Complete a functional requirement analysis to identify common and specialized Canonical messages to be exchanged amongst integrated modules.

4.2.2 Static Structure Designs

Design canonical message static structures expressed as Unified Modeling Language (UML) Class diagrams with appropriate Class-to-Class relationships (Inheritance, Association etc.) in SparxEA tool or as fully importable exports (without any loss of modeling or diagraming detail) generated in a UML modeling tool of choice.

4.2.3 Communication Dynamic Designs

Create canonical communication dynamic designs expressed in Business Process Execution Language (BPEL) orchestration, routing, message transformation and other related diagrams taken from Oracle JDeveloper IDE for Fusion Middleware integration platform.

5.0 Identity and Access Management

An enterprise Identity and Access Management System (IdAM) and Role Based Access Configuration (RBAC) exists in a state of partial readiness. In order to implement the IdAM and RBAC solution using Oracle Identity Management (IdM) the following expertise and work products are required.

5.1 Contractor Qualifications

1) Two (2) or more proven successful implementations of an enterprise IdAM and RBAC capability using Oracle Identity Management (IDM) COTS platform currently operating in production environments, preferably implementations that required the takeover of an existing IdAM implementation versus starting from scratch.
2) Five (5) or more years of company experience with IdAM development and implementation.
3) Proven expertise with solutions combining Active Directory-based authentication for clients' employees and Oracle Unified Directory (OUD) based authentication for external users.
4) Proven expertise with Single Sign On (SSO) implementations using Oracle IDM, including experience where subsequent authentications into more strict applications required additional credentialing, compared to the initial and more basic secret-based challenges.
5) Proven expertise with configuring coarse and fine-grained authorization for access of service URIs exposed on OFMW platform.
6) Proven expertise in extending off-the-shelf fine-grained authorization mechanism available from IdM with any custom solutions. For example, to prevent access based on the relationship of the requesting user to the data (trying to manipulate one's own medical claims).
7) Proven approach to identification and implementation of Enterprise Roles including relationship between such roles and access permissions identified in system requirements for various services.
8) Proven expertise exposing IdM capabilities for user provisioning, self-service password management or any other IdM functions as enterprise shared services for inclusion into various custom application and portal workflows. Include details on the approach to such shared service design and enablement.

5.2 Work Products

Assessment and identification of potential improvements to meet performance requirements for:

1) Existing IDM platform design
2) Existing IDM functional design and key capabilities of:
    a) SSO
    b) User authentication
    c) Multi-factor authentication (MFA)
    d) Authorization
3) Existing security elements (authentication, authorization) attached to various functional requirements.
4) Implement recommendations as approved by the HSD.

5.2.1 Roles and Permissions Definition and Implementation

1) Derivation and implementation of temporary roles and permissions required for integrated modules' security requirements to enable initial integrated end point testing.
2) Derivation and implementation of Enterprise roles and permission sets to enable end-to-end integrated module testing and production operations.
3) Management of high level and detail level access to applications.

5.2.2 IdM Solution Design

Design IdM solutions expressed and documented as UML component diagrams with appropriate element-to-element relationships (Dependency, Interface Implementation etc.), and deployment / communication diagrams showing relevant elements of component placement into computing nodes, communication protocols, addresses, sub-nets etc. All modeling is to be produced in SparxEA tool or as fully importable exports (without any loss of modeling or diagraming detail) generated in Contractors' UML modeling tool of choice.

5.2.3 Implementation

Implementation of IdM functionality for SSO, authentication, authorization, role management and user provisioning.

6.0 Master Data Management (MDM)

6.1 Contractor Qualifications

1) Two (2) or more proven successful implementations of a MarkLogic MDM solution currently operating in a production environment.
2) Four (4) or more years of company experience with MarkLogic solutions.
3) Proven and well-defined requirements elicitation, validation, and traceability processes.
4) Proven iterative and continuous development and implementation processes to support multiple modules and programs with unique data mastering requirements.
6) Ability to fully staff multiple workstreams to support the continuous development and implementation described above and HSD project management processes. Staff the engagement team with:
    a) Sufficient staffing with certified Mark Logic professionals
    b) Business analysts and development professionals experienced with Master Data Management
    c) Proven SOA experience and SOA certified staff
    d) Proven Jama/Jira/Confluence experience
    e) Proven Medicaid systems and CMS certification experience
    f) Regular and frequent onsite presence

6.2 Work Products

6.2.1 Master Data Management Assessment and Remediation

Assess current MDM artifacts, propose recommendations, and implement changes as approved by HSD.

1) Assess existing master data management artifacts.
    a) Review MDM current Client and Provider data models for best practices
    b) Review MDM hardware environments for optimal configuration and sizing
    c) Review MDM software and database components for optimal configuration
    d) Provide recommendations for MDM data models, hardware, and software
2) Implement master data management artifact recommendations.
    a) Update MDM design documentation

   b) Update MDM hardware environments
   c) Update MDM software and database component configuration
3) Use of HHS 2020 toolset for management of artifacts, including SharePoint for documents, Sparx Enterprise Architect for models, and Jama for requirements.

6.2.2 Requirements, Data Sources, and Capabilities Definition

Document MDM business and source requirements including:

1) Lead discussions on business requirements and use of the MDM, including survivorship rules and data stewardship workflows.
2) Identify and discover MDM source systems.
3) Profile MDM source system data to inform requirements discussions.
4) Document MDM capabilities for Client, Provider, and Employer domains based on best practices, use case discussions and leveraging the canonical model.

6.2.3 MDM Development and Implementation

Modify and augment current MDM implementation based on assessment and requirements including:

1) Augment with capabilities required.
2) Complete definition of data elements for MDM
3) Create or modify application configurations to take data in from identified systems and merge/unmerge/survive data according to business requirements with flexibility for future data profile changes.
4) Create data access/edit services to expose MDM capabilities for module use and participation in service orchestrations.
5) Prepare MDM for future expansion of data sources beyond initial set of Omnicaid, ASPEN and BPO modules to include Children Youth and Families Department (CYFD)'s system, Department of Health (DOH) systems, and other HHS 2020 partners.
6) Prepare MDM for future mastering of employers.
7) Facilitate user acceptance testing of MDM capabilities.
8) Maintain defect resolution processes.
9) Transfer/report operational metadata according to metadata strategy.

7.0 Data Migration, ODS/RDL, Data Models and Reference Data

The migration of data, from Medicaid Systems and partner systems, to our Operational Data Store (ODS) and Data Warehouse require the following expertise and work products.

7.1 Contractor Qualifications

1) Two (2) or more proven successful implementations of Data Migration, Operational Data Store (ODS)/Raw Data Lake (RDL), Data Models and Reference solution utilizing MarkLogic solutions to migrate data to disparate data repositories currently operating in a production environment.
2) Four (4) or more years of company experience with similar solutions.
3) Proven and well-defined requirements elicitation, validation, and traceability processes.
4) Proven iterative and continuous development and implementation processes to support multiple modules and programs with unique data mastering requirements.

5) Ability to fully staff multiple workstreams to support the continuous development and implementation described above and HSD project management processes. Staff the engagement team with:
    a) A majority of staff holding a MarkLogic Professional Certification
    b) Business analysts and development professionals experienced with Data Migration, ODS/RDL, Data Models and Reference solutions
    c) Proven SOA experience and SOA certified staff
    d) Proven Jama/Jira/Confluence experience
    e) Proven Medicaid systems and CMS certification experience
    f) Regular and frequent onsite presence

7.2 Work Products

7.2.1 Data Migration Assessment, Recommendations and Remediation

Assess current implementation of data migration process and tools, propose recommendations, and implement changes as approved by HSD.

1) Assess existing System Migration Repository (SMR) processes.
    a) Analysis and recommendation for ongoing data validation processes
    b) Analysis and recommendation for MarkLogic ingestion, transformation, and materialization processes
    c) Analysis and recommendation for performance tuning
    d) Analysis and recommendation for changes and tuning of Extract, Transform, Load (ETL) processes
    e) Analysis and recommendation for data flow outlining ingestion, materialization, and conversion of data from source
2) Implement HSD approved data migration recommendations.

7.2.2 Development and management of ETL processes and rules

1) Convert legacy data.
    a) Configure for one-time ingestion and materialization of legacy data from multiple systems
2) Develop processes for incremental data load.
    a) Definition of recurring data refresh for incremental data load
    b) Implementation of recurring data refresh for incremental data load
3) Develop and maintain data cleansing rules and processes to advance data quality in careful coordination with HSD SME's and within NM policies.
4) Develop and maintain ETL documentation.
5) Utilize version control and change control for changes for ETL processes.
6) Validate data for one-time and incremental data load.
7) Transfer/report operational metadata according to metadata strategy.

7.2.3 Creation and management of enterprise test data

1) Define enterprise data de-identification scheme and strategy for data usability within HIPAA, FTI and Safe Harbor constraints.

2) Develop and test enterprise data de-identification scheme.
3) Define data materialization strategy to demonstrate defect resolution.
4) Define regular data refresh process for feeding of test systems.

7.2.4 Creation and configuration of production environment

1) Install and secure data migration software in a production environment using the existing HSD infrastructure.
2) Materialize production data from source to enterprise data model.

7.2.5 Operational Data Store and Raw Data Lake Assessment, Recommendations, and Remediation

Consideration and update of current state design and configuration documentation.

1) Assess current documentation for the RDL and ODS implemented in MarkLogic.
2) Provide recommendations for ODS strategy, goals, and objectives based on discovery sessions with business and technical teams.
3) Perform updates of design documentation for RDL and ODS to include diagrams and descriptions of data flow.
4) Perform HSD approved updates of configuration for RDL and ODS based on intended use.

7.2.6 Data Model Artifacts Assessment, Recommendations and Remediation

Assessment and update of current state data model artifacts:

1) Assess current data model artifacts and processes for completeness, accuracy, repeatability, and conformance to the Federal Health Information Model (FHIM) and Fast Healthcare Interoperability Resources (FHIR) standards including the Conceptual, Logical, Physical, and MarkLogic Persistent data models for the following data domains:
    a) Client
    b) Claim
    c) Drug Rebate
    d) Third Party Liability
    e) Prior Authorization
    f) Provider
    g) Managed Care
    h) Financial
2) Profile and review profiling results of contributing data sources, including ASPEN and Omnicaid.
3) Recommend changes to data model storage.
4) Recommend changes to data modeling maintenance or recommend creation of a new data modeling process and maintenance.
5) Prepare data models for future expansion of data sources beyond initial set of Omnicaid, ASPEN and BPO modules to include other HHS 2020 partners.
6) Implement recommendations as approved by the HSD.

7.2.7 Reference Data Management Assessment, Recommendations and Remediation

Assessment of reference data.

1) Identify sources of reference data.
2) Identify reference data needs for each HHS 2020 enterprise partner.
3) Characterize reference data based on format, frequency, licensing requirements, cost, and data sharing capabilities.
4) Confirm structure of domain-specific reference data as best practice.
5) Make recommendations for reference data management.

Implement reference data recommendations as approved by the HSD.

1) Create reference data repository with relevant permissions.
2) Provide reference data to SMR as needed.
3) Create reference data management plan for future reference data feeds and governance.

8.0 Testing

8.1 Contractor Qualifications

1) Two (2) or more proven successful integration testing and end to end testing implementations aligning to Centers for Medicare and Medicaid Services (CMS) testing framework of similar scale and complexity currently operating in a production environment.
2) Four (4) or more years of company experience providing similar post- production testing support to operations.
3) Proven ability to support iterative and continuous development, testing and implementation processes for multiple modules and products being promoted into production operations on varying timelines and with converging dependencies.

8.2 Work Products

While HSD has a preference to some of the existing work products and tools that are currently operational, we are looking for recommendations and suggestions from the SI contractor for equivalent or better tools that are more suitable for the proposed testing activities and implementation using industry best practices.

8.2.1 Test Management Plan

Create a SI Test Management Plan that, while complying with the HSD Test Management Plan, defines and describes how testing will be conducted for the work products of this engagement. The plan should include the contractor's standards and best practices to be utilized and cover, at a minimum, the following topics:

1) Test Strategy, Test Plans, Test Schedules, Test Cases, Test Execution Results, Test Summary Reports, Defect Reports
2) Test Process/Procedure documents
3) Test Case Management, Defect Management using Xray for Jira tools
4) Web Services and API testing using SOAP UI, Postman or equivalent

5) Performance testing tools using Apache JMeter or equivalent
6) Section 508 Testing using Job Access with Speech (JAWS) or equivalent
7) Infrastructure Testing
8) Security Testing
9) Integration Testing

8.2.2 Test Execution

Conduct all activities of testing as described in the SI Test Management Plan. The quote for this work product should include the establishment of milestone completions and payment points for testing covering the work products of this engagement.

9.0 Project Management

9.1 Contractor Qualifications

1) Five (5) or more years of company experience in project management on projects of similar scale and complexity.
2) Two (2) or more proven successful project management engagements on projects of similar scale and complexity.
3) Two (2) or more proven successful project management engagements managing multiple subcontractors on projects of similar scale and complexity.
4) Proven expertise in industry best practices (e.g. Project Management Body of Knowledge (PMBOK)), with experience gained on projects of similar size and complexity.
5) Experience leading or assisting a State Medicaid agency successfully through the CMS certification process.

9.2 Work Products

9.2.1 Project and Enterprise Management Plans Updates

Comply with and update, in coordination with the EPMO, the following enterprise project management plans incorporating, if needed, contractor's provision of the requested work products and services:

1) Project Management Plan
2) Schedule Management Plan
    a) Include impact and planning from velocity reports
    b) Include earned value management and reporting
3) Staffing Model and Resource Management Plan
4) Enterprise Configuration Management Plan
5) Enterprise Change Control Management Plan
6) HSD Project Team Onboarding Plan
7) Communications Management Plan

9.2.2 Lifecycle Management Plans Addendums

Comply with the following enterprise life cycle management plans, or if preferred by the Contractor, create their own addendums to the plans that are in alignment with the enterprise plans:

1) Requirements Management Plan
2) Requirements Traceability Matrix
3) Test Management Plan
4) Quality Management Plan

10.0 CMS Certification

10.1 Contractor Qualifications

1) Experience by the contractor or its employees providing major certification support to at least one (1) state that has completed MMIS certification.
2) Demonstrated knowledge of the CMS Certification Review Process
3) A full-time Certification Manager dedicated to this project.

10.2 Work Products

10.2.1 Assessment and Remediation Plan

Assessment and identification of potential improvements to the Certification Process Guide to bring it up to date and improve it as needed so it reflects the offeror's plan for CMS certification. After the Certification Process Guide has been updated, it will require approval by the HSD prior to implementation on this project.

10.2.2 Certification Review Preparation

The Contractor shall, with HSD and the MMISR Independent Verification and Validation (IV&V) Contractor collaboration, perform the following activities through the entire CMS MMIS certification process:

1) Ensure that the SI module meets CMS certification requirements and complies with the HSD Certification Plan.
2) Comply with applicable CMS MMIS MECT checklist System Review Criteria for the SI module per Addendum 18 in the procurement library or Outcomes Based Certification (OBC).
3) Provide the necessary artifacts and evidence for CMS Operational and Final Milestone reviews as defined in the HSD's Certification Plan.
4) Work with HSD and the MMISR IV&V Contractor to review the artifacts and evidence and update the documentation if needed.
5) As part of weekly and monthly status report, provide update on SI Certification activities.
6) Resolve issues that prevent the HSD from receiving certification based upon components of the SI Module.
7) Any further work related to completing certification of the SI module.

10.2.3 Responsibilities During Certification Reviews

The Contractor is responsible for the following Certification Activities during all Milestone Reviews:

1) Coordinate, participate, and prepare for SI Certification activities and artifacts.
2) Respond to questions from the HSD, IV&V or CMS and MITRE for SI components.
3) Provide follow up documentation for action items from CMS and MITRE to assure the HSD can receive final certification.

11.0 Maintenance and Operations

Once MMIS modules and partner agencies begin to use the system integration platform to access data and tool sets, maintaining it in a high state of readiness, performance, and security is necessary. The following are the minimum qualifications and work products necessary.

11.1 Contractor Qualifications

1) Two (2) or more proven successful implementations of maintenance and operations engagements of similar scale and complexity currently operating in a production environment.
2) Four (4) or more years of company experience providing similar maintenance and production operations.
3) Proven and well-defined maintenance and operations processes.
4) Proven ability to support iterative and continuous development and implementation processes for multiple modules and products being promoted into production operations on varying timelines and with converging dependencies.

11.2 Work Products

11.2.1 Maintenance and Operations Plan

Maintenance and Operations Plan to support all workstreams and products described in this RFQ and in the HHS200 plan for multiple module integration and implementation. All environments except disaster recovery are on-site environments in the HSD data centers.

1) Staffing plan
2) Monitoring tools
3) Helpdesk and end-user support tools
4) Support for COTS products and contractor developed applications
5) Performance monitoring plan
6) Use of industry best practices

11.2.2 Maintenance and Operations Services

Provision of the services described in the Maintenance and Operations Plan, including staffing and tools required to assure reliable operations and meet SLAs.

12.0 Appendices

12.1 Appendix A: List of Acronyms

Acronym	Definition
AD	Active Directory
ADFS	Active Directory Federation Services
API	Application Programming Interface
ASVV	Address Standardization, Validation, and Verification
BPEL	Business Process Execution Language
BPO	Business Process Outsourcing
CCM	Customer Communication Management
CCNA	Cisco Certified Network Associate
CMDB	Configuration Management Database
CMS	Centers for Medicare and Medicaid Services
COTS	Commercial Off the Shelf
CYFD	Children Youth and Families Department
DNS	Domain Name System
DOH	Department of Health
DR	Disaster Recovery
EA	Enterprise Architect
EDM	Electronic Document Management
ETL	Extract, Transform, Load
EPMO	Enterprise Project Management Office
EPS	Enterprise Project Schedule
ESB	Enterprise Service Bus
FHIM	Federal Health Information Model
FHIR	Fast Healthcare Interoperability Resources
FTI	Federal Tax Information
HHS	Health and Human Services
HIPAA	Health Information Privacy and Accountability Act
HSD	Human Services Department
IdAM	Identity and Access Management
IdM	Oracle Identity Management
IGC	Information Governance Catalogue
IRS	Internal Revenue Services
ITOM	Information Technology and Operations Management
ITSM	Information Technology Service Management
M&O	Maintenance and Operation
MAD	Medical Assistance Division
MARS-E	Minimum Acceptable Risk Standards for Exchanges
MCSA	Microsoft Certified Solutions Associate
MCSE	Microsoft Certified Systems Engineer
MDM	Master Data Management
MFA	Multi-factor Authentication
MFT	Managed File Transfer
MMISR	Medicaid Management Information System Replacement
NM	New Mexico
NSX	VMWare Network Virtualization

Acronym	Definition
OBC	Outcomes Based Certification
ODS	Operational Data Store
OFMW	Oracle Fusion MiddleWare
OUD	Oracle Unified Directory
PMBOK	Project Management Body of Knowledge
RBAC	Role Based Access Configuration
RCM	Release Certification Matrix
RDL	Raw Data Lake
RFQ	Request for Quote
RHCE	Red Hat Certified Engineer
RHCSA	Red Hat Certified System Administrator
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAM	Software Asset Management
SCESM	Safeguard Computer Security Evaluation Matrix
SDLC	Software Development Life Cycle
SI	System Integrator
SLA	Service Level Agreements
SME	Subject Matter Expert
SMR	System Migration Repository
SOA	Service Oriented Architecture
SOW	Statement of Work
SSO	Single Sign On
UDMH	Unified Data Model for Healthcare
UML	Unified Modeling Language
VCAP	VMware Certified Advanced Professional
VCDX	VMware Certified Design Expert
VCP	VMware Certified Professional
vROPs	VRealize Operations Manager