APPENDIX B
SCOPE OF WORK AND TECHNICAL REQUIREMENTS

The Vendor will lead and provide consulting support services to develop the next MITA State Self-Assessment and provide a SaaS solution for MITA SS-A management and SS-A submission. Vendor to be prepared to lead and provide consulting support if and when new versions of the SS-A becomes the standard. The SaaS solution provided should also be prepared to pivot to as needed--the State wants to be able to produce SS-A's, identify maturity, and track progress against the MITA roadmap. Additionally, State staff are not accustomed to periodic large MITA projects that take a lot of time. It is our goal to have the vendor MITA team prepare as much, if not the majority of the documentation for subject matter expert review, in advance, based on existing information to alleviate the burden on State staff.

The Vendor must address every section of Appendix B – Scope of Work and Technical Requirements, in the Vendor Proposal, and must respond with their approach to handling each task in the following sections.

1. Project Management

- 1.1. Project Kickoff Meeting
- 1.2. Project Plan and Updates
- 1.3. Change Request Review and Approval
  - 1.3.1. Management of all MITA SS-A tool changes
    - 1.3.1.1. Implementation
    - 1.3.1.2. Maintenance
- 1.4. Weekly/Monthly CMS Status Reports
- 1.5. Monthly Steering Committee Meetings Invite
  - 1.5.1. Agenda
  - 1.5.2. Minutes (hour turn around to stakeholders)

2. MITA SS-A

- 2.1. MITA SS-A Kickoff
  - 2.1.1. Include all stakeholders
  - 2.1.2. Leadership State Subject Matter Experts (SME's)
  - 2.1.3. If needed-Other vendors that support the Medicaid Enterprise
- 2.2. Medicaid Management Information System (MMIS) System Assessment
  - 2.2.1. Review the latest Delaware SS-A
  - 2.2.2. Upload Delaware latest SS-A into the MITA tool
  - 2.2.3. Year 1 is a full MITA SS-A and remaining years are updates
  - 2.2.4. Business Architecture (BA) SS-A – As-Is and To Be Assessments
    - 2.2.4.1. Validate the as-is level of maturity for each MITA business areas and business processes using MITA Business Capability Matrix (BCM)

2.2.4.2. Work with the Fiscal Agent, State SMEs, and other system vendors to understand the MMIS systems business architecture and how individual MITA business processes map to the MMIS system software modules and vice versa

2.2.4.3. Become familiar with the operational MMIS system by accessing the user acceptance testing (UAT) environment, system documentation (rLink), operational documentation to determine the as-is levels of maturity for each business process as measured against the BCM

2.2.4.4. Complete the as-is Business Architecture (BA) scorecard

2.2.4.5. Create a MITA Business Capability Matrix (BCM) Business Process (BP) Analysis Score Summary

2.2.4.6. Work with the State and Fiscal Agent to establish goals and objectives for each business area and business process to determine to-be levels (capabilities, priorities, and dependencies) that are feasible within the constraints of the current the MMIS system architecture

2.2.4.7. Identify the to-be levels of maturity and timeframes; complete the to-be BA scorecard and fill in the as-is and to-be levels on the business architecture profile

2.2.4.8. The BA assessment must contain the associated artifacts identified in the SS-A Companion Guide

2.2.5. Information Architecture (IA) SS-A – As-Is and To-Be Assessments

2.2.5.1. Use the MITA BPM and information capability matrices (ICMs), to evaluate the as-is IA environment for each of the ten business areas with a focus on secure and consistent data throughout the State, assess each of the four information capabilities: data management strategy (DMS), conceptual data model (CDM), logical data model (LDM), and data standards

2.2.5.2. Assign an as-is IA level of maturity for each business area

2.2.5.3. Complete the as-is IA scorecard

2.2.5.4. Work with the State and the Fiscal Agent to establish IA goals and objectives for each business area and business process to create a to-be view

2.2.5.5. Identify the to-be levels of maturity and timeframes; complete the to-be IA scorecard and fill in the as-is and to-be levels on the architecture profile

2.2.5.6. The IA assessment must contain the associated artifacts identified in the SS-A Companion Guide

2.2.6. Technical Architecture (TA) SS-A – As-Is and To-Be Assessments

2.2.6.1. Use the MITA BPM and technical capability matrices (TCMs), to evaluate the as-is technical architecture (TA) environment for each of the ten business areas Evaluate as-is TA environment from the perspectives of the technical management strategy, business services, technical services, application architecture, and technology standards

2.2.6.2. Develop the as-is technical service models for important high-level functions and messages of each of the business areas Document the as-is technical service areas and classifications

2.2.6.3. Assign an As-is TA level of maturity for each business area

2.2.6.4. Complete the as-is TA scorecard
2.2.6.5. Work with the State and the Fiscal Agent to establish TA goals and objectives for each business area and business process to create a to-be view
2.2.6.6. Identify the to-be levels of maturity and timeframes; complete the to-be IA scorecard and fill in the as-is and to-be levels on the technical architecture profile
2.2.6.7. The TA assessment must contain the associated artifacts identified in the SS-A Companion Guide

2.2.7. Assessment of Compliance with Seven Conditions and Standards (SC&S)
2.2.7.1. The Vendor must work with the system vendors and the State to understand the system architecture (business, information, and technical) and to what extent it meets each of the seven conditions and standards
2.2.7.1.1. The Vendor must complete the seven conditions and standards steps (as defined in the SS-A Companion Guide) including, but not limited to the following
2.2.7.1.2. Evaluate as-is BA, IA, and TAs as they relate to the seven conditions and standards using the SCM to assess the current level of maturity
2.2.7.1.3. Document BA, IA, and TA compliance for each of the seven conditions and standards.
2.2.7.1.4. Assign an as-is level of maturity for each of the seven conditions and standards Work with the State and the Fiscal Agent to establish goals and objectives for each business area as it relates to the seven conditions and standards and create a to-be view
2.2.7.1.5. Identify the to-be levels of maturity and timeframes.
2.2.7.1.6. Complete the seven conditions and standards scorecard and fill in the as-is and to-be levels on the seven conditions and standards profile
2.2.7.2. The SC&S assessment must contain the associated artifacts identified in the SS-A Companion Guide

2.3. MITA/MMIS Concept of Operation
2.3.1. Include all related MMIS systems (Data warehouse and Decisions Support System, Eligibility System, Electronic Visit Verification System, Pre-Admission Screening and Resident Review, Asset Verification System, etc.)
2.3.2. Provide High-Level Business Workflows
2.3.3. COO must contain the associated artifacts identified in the SS-A Companion Guide

2.4. MITA Roadmap
2.4.1. Gap Analysis: As-Is to To-Be
2.4.2. Review projects in process and projects on the horizon
2.4.3. Work with stakeholders to determine what would have to be modified or implemented to reach greater maturity according to the maturity curves for MITA and the seven conditions and standards
2.4.4. Document the information in the MITA system and produce a MITA roadmap
2.4.5. The MITA Roadmap must contain the associated artifacts identified in the SS-A Companion Guide

3. Software as a Service (SaaS) Tool

3.1. The Vendor will provide a SaaS tool to assist the State of Delaware in completing and submitting the annual Centers for Medicare and Medicaid Services (CMS) Medicaid Information Technology Architecture State Self-Assessment (MITA SS-A). The vendor will configure as well as provide ongoing maintenance and current versioning of the tool. The selected vendor for this project will be required to provide a MITA tracking system that will automate and assist Delaware in updating and implementing its MITA (and all future versions) SS-A, allowing Delaware to prioritize new projects and enhancements based on business capabilities and alignment with the CMS Seven Conditions and Standards

3.2. General System Technical Requirements

- 3.2.1. The solution shall be a vendor hosted system
- 3.2.2. The solution shall support online, browser-based web capabilities with no client component download(s) for all authorized users
- 3.2.3. Maintain target uptime for the hosted service at 95% availability to all users
- 3.2.4. Ensure the provision of appropriately sized servers and backup servers, technical support personnel, systems security and disaster recovery procedures to support a day Recovery Point Objective (RPO) and a five (5) business day Recovery Time Objective (RTO)
- 3.2.5. Ensure the hosting environment is within the United States and no offshore staffing supporting this SaaS solution
- 3.2.6. Ensure the browser support includes at minimum, Microsoft Edge, Google Chrome, and Firefox

3.3. SaaS Tool Implementation

- 3.3.1. Complete customization, set-up, and overall management of the tool to facilitate successful MITA SS-A completion and all Delaware requirements
  - 3.3.1.1. Upload the entire previous Delaware SS-A (s)
- 3.3.2. Continued Maintenance and Operations services for the SaaS tool

3.4. SaaS Tool Training

- 3.4.1. Develop an overall demonstration for the State MITA SS-A team
  - 3.4.1.1. Present SaaS tool overview to Delaware leadership as needed
- 3.4.2. Maintain all CMS policies and guidelines
- 3.4.3. Maintain all Delaware DTI policies and guidelines

3.5. SSA Tool must support all requirements as outlined in Appendix B - Scope of Work and Technical Requirements

3.6. MITA Reporting

- 3.6.1. SaaS tool must provide as needed Advanced Planning Document (APD) submissions support, and Streamlined Modular Certification support as it is related to the overall MITA maturity advancement of the Delaware MMIS

3.7. MITA Dashboards

- 3.7.1. SaaS tool must have dashboard capabilities that at a minimum present MITA Maturity levels across the Delaware Medicaid Enterprise

3.8. Security and Privacy Compliance

3.8.1. The proposed solution must be fully compatible with the DHSS technical environment. Proposed solutions that are not fully compliant with State standards will be disallowed

3.8.2. The Standards and Policies web page links to DHSS and DTI policies and standards and other documentation

3.8.3. The DTI Systems Architecture Standard contains information confidential to the State and is not published on the internet. However, DTI has set up an email address, which will automatically send a response with this document attached. The email address is join-tasc_policies@lists.state.de.us

3.8.4. The application will have at least tiers with the tiers configured and secured as in the sample diagram included in the DHSS Information Technology Environment Standards. Please see State of Delaware Systems Architecture Standard. The link to this document is can be found here.

3.8.5. All components of the proposed solution, including third party software and hardware, are required to adhere to the policies and standards described above, as modified from time to time during the term of the contract resulting from this RFP, including any links or documents found at the above referenced web sites

3.8.6. State DTI and Policies: – The Vendor must maintain best practices adopted by the Department of Technology and Information (DTI), through the Technology and Architecture Standards Committee (TASC)The Vendor will develop solutions using architecture, software and hardware deemed to be in a Standard or Acceptable category by DTI. When architecture, software, or hardware is moved to a category of discontinue the Vendor must develop a plan to move to a solution considered Standard

3.8.7. All Vendor staff working on this project will be subject to a Criminal Background Check (CBC)The vendor will be solely responsible for the cost of the CBC. DHSS will review the CBC results. DHSS at their sole discretion may request that a vendor staff member be replaced if their CBC result is unsatisfactory. Vendor CBC Instructions

3.8.8. Vendor staff will be required to fill out DTI's BAA and DTI T&Cs for necessary authorizations before starting work under the contract. See Appendix C, of RFP HSS-26-081.

3.9. Architecture Requirements

3.9.1. Securing and protecting data is critical to DHSS. This protection is required for data whether hosted onsite or offsite. As such it is required that the Vendor include in the response to this section proposed architectural diagram(s) in Visio format demonstrating how DHSS data is being secured

3.9.2. The diagram must include any interfaces between the solution and other solutions. The diagram needs to be clearly documented (ports, protocols, direction of communication). It does not need to contain the inner workings of the solution or proprietary information. In addition, the Vendor shall include in its response a description of its security processes and procedures for all these interfaces

3.9.3. Technical documentation will be required to be produced as part of the contract negotiations process. These will be submitted to DHSS for attachment to a DTI business case. The business case must be in "Recommended" status prior to contract signature or

have a clear indication that the contract can be signed subject to conditions listed in the business case. The project business case is a DHSS responsibility. Technical documentation includes a final architecture diagram for each system environment (Prod, UAT, etc.), non-proprietary data dictionary and a high-level process flow diagram. This documentation shall be produced at no cost to DHSS prior to contract signature

3.9.4. Architecture changes can be highly risky if not planned and tested correctly and must go through the change control process. The architecture diagram may have to be updated along with other documents for prior approval. Architecture changes must be staged in lower environments at least at the SIT level for integration testing. Formal UAT approval is required for scheduling production implementation

3.9.5. The Vendor shall express business rules using a technology-neutral standard format corresponding with the core data elements identified through the National Information Exchange Model (NIEM)

3.10. Standard Practices

3.10.1. The vendor(s) shall be responsible for ensuring that all services, products and deliverables furnished to DHSS are consistent with practices utilized by, or policies and standards promulgated by, the Department of Technology and Information (DTI).

3.11. Confidentiality and Data Integrity

3.11.1. All data generated from the original source data shall be the property of the State of Delaware. The control of the disclosure of those data shall be retained by the State of Delaware and the Department of Technology and Information

3.12. Security Controls

3.12.1. As computers, network, and information security are of paramount concern, the State wants to ensure that computer/network hardware and software do not compromise the security of its IT infrastructure. Therefore, the Vendor is guaranteeing that any systems or software meets or exceeds Critical Security Controls. The link to this document can be found here.

3.13. Cyber Security Liability

3.13.1. It shall be the duty of the Vendor to ensure that all products of its effort do not cause, directly or indirectly, any unauthorized acquisition of data that compromises the security, confidentiality, or integrity of information maintained by the State of Delaware. Vendor's agreement shall not limit or modify liability for information security breaches, and Vendor shall indemnify and hold harmless the State, its agents and employees, from any and all liability, suits, actions or claims, together with all reasonable costs and expenses (including attorneys' fees) arising out of such breaches. In addition to all rights and remedies available to it in law or in equity, the State shall subtract from any payment made to Vendor all damages, costs and expenses caused by such information security breaches that have not been previously paid to Vendor

3.14. Cloud/Remote Hosting Requirements

3.14.1. The State prefers a vendor or cloud-hosted solution. This section is mandatory for Vendors proposing to host systems and/or DHSS data outside of the State network.

Vendors must respond as required for each subsection below. Failure to respond as instructed may be cause for rejection of the entire proposal

3.14.1.1. Remote Hosting Agreements

3.14.1.1.1. The data classification for this procurement is Non-Public

3.14.1.1.2. Vendor is instructed to review the following two agreements and sign, scan, and include with your response

3.14.1.1.2.1. DTI Terms and Conditions (DTI T&C's) (Found in Appendix D)

3.14.1.1.2.2. Business Associates Agreement (BAA) (Found in Appendix D)

3.14.1.1.3. If Vendor can only accept a clause with conditions (Accept Conditionally) or does not agree with (Reject) a clause as written, then please fill out the following Cloud Services/Data Usage Exceptions table as part of your response to this section. Please include a Comment for each exception stating why you Accept Conditionally or Reject. If you can Accept Conditionally, state what controls are or can be put into place to provide for the same or similar level of compliance

3.14.1.2. Any exceptions specified will be vetted by DTI prior to contract signature. Individual clauses may be negotiated and updated by DHSS. In this case, DTI's written approval of the negotiated Agreement version will be attached to the final contract

3.14.1.3. "[Company Name] is proposing a solution will encrypt non-public data at rest."

3.14.2. However, if the Vendor cannot comply with this requirement, then Vendor must purchase adequate Cyber Liability Insurance as specified in Section Cyber Responsibilities, Liability and Insurance. Please include the following statement in your response to this section:

3.14.2.1. "[Company Name] is proposing a solution will not encrypt non-public data at rest and intends to purchase Cyber Liability Insurance as specified in Section prior to contract signature"

3.14.2.2. The selected Vendor will present a valid certificate of cyber liability insurance for attachment to the contract prior to contract signature

3.15. Terms and Conditions for Subcontractors

3.15.1. Subcontractors involved in offsite/cloud data hosting are not required to sign the DTI T&C's however, the primary vendor is expected to hold them responsible to the same or more stringent security requirements to ensure that State data is adequately secured

3.16. Standard Practices

3.16.1. The vendor(s) shall be responsible for the professional quality, technical accuracy, timely completion, and coordination of all services furnished to DHSS. The vendor(s) shall follow practices consistent with generally accepted professional and technical policies and standards

3.17. Mandatory Inclusions for Cloud/Remote Hosting

3.17.1. Network Diagram

3.17.1.1. The Vendor must include a network diagram of the user's interaction with the solution and any interfaces between the solution and the State need to be clearly

documented (ports, protocols, direction of communication). The network diagram does not need to contain the inner workings of the solution or proprietary information

3.17.2. DTI/DHSS-Specific Security Requirements

3.17.2.1. The requirements in this section are mandatory. See Standards and Policies.

3.17.3. Encryption of Data at Rest

3.17.3.1. Vendor will describe the method(s) for encrypting DHSS confidential/PII/ePHI data at rest in their proposed solution

3.17.4. Encryption of Data in Transit

3.17.4.1. All data in transit must be encrypted whether transmitted over a public or private network. Vendor will describe the encryption method(s) proposed

3.17.5. DHSS Data Rights

3.17.5.1. All DHSS data (Public and Non-Public) related to services provided under this contract will remain the sole property of DHSS. De-identified or derived/aggregated DHSS data is not exempted from this requirement. This provision shall survive the life of the contract. Vendor does not acquire any right, title or interest in DHSS data under this contract. Except as otherwise required by law or authorized by DHSS in writing, no DHSS data shall be retained by the Vendor for more than days following the date of contract termination. After the -day timeframe the following provisions will remain in effect: vendor will immediately delete or destroy this data in accordance with NIST standards and provide written confirmation to DHSS; vendor is expressly prohibited from retaining, transferring, repurposing or reselling DHSS data except as otherwise authorized by DHSS in writing; vendor retains no ongoing rights to this data except as expressly agreed to by DHSS in the contract

3.17.6. Offsite Project Work

3.17.6.1. DHSS will permit project work to be done offsite, within the United States and its territories and Canada. For offsite work, DHSS requires strong management of the resources and assigned tasks; adequate, timely and accurate communications and completion of assigned work by specified deadlines. This is important to any offsite relationship. If Vendor is proposing offsite project work, Vendor must specifically address each of the bulleted items below in this section of the proposal. Otherwise, Vendor will respond to this section as follows: “No offsite project work proposed”

3.17.6.1.1. Note: For the purposes of this section, the Vendor staff organization includes subsidiary vendors

3.17.6.1.1.1. Provide a detailed description of work to be completed offsite along with a breakdown of the type of work to be provided on-site. Quantify this by estimating for each of the deliverables identified in this Section, the percentage of work to be done offsite

3.17.6.1.2. Provide an organization chart with job titles of offsite staff and their relationship to the Vendor

3.17.6.1.3. Provide a description of what tasks each job title is responsible for performing

3.17.6.1.4. Clearly identify if offsite work is to be performed by Vendor staff or subcontractors

3.17.6.1.5. For offsite subcontractor or Vendor staff, please include the names and resumes of key staff, highlighting prior participation in similar projects. Also provide named or sample resumes for lower-level staff

3.17.6.1.6. Provide a detailed plan for managing offsite work including communication strategies to accommodate time differences if any. Include contingency plan for completing work should offsite relationship be terminated

3.17.6.1.7. Propose a meeting schedule for project status discussions with offsite management staff

3.17.6.1.8. Identify the offsite single point of contact who will serve as the project manager of offsite resources. Describe how this project manager and the on-site project manager will interact. DHSS prefers that the offsite project manager be a vendor employee

3.17.6.2. Provide a contingency plan for substituting on-site staff if offsite relationship becomes problematic as determined by DHSS

3.17.6.3. Provide a description of prior Vendor organization experience with use of offsite Vendor staff or subcontractors and provide US client references for that work

3.17.6.4. Provide a detailed description of proposed project manager's experience in directing offsite staff and/or subcontractors

3.17.6.5. Describe your understanding that DHSS will only provide management of this project and Vendor resources through the on-site project manager. All management/relationships with offsite resources, whether Vendor staff or subcontractors, will be handled by the respective bidding organization

3.18. Offshore Prohibitions

3.18.1. Offshore is defined as not being within the United States or its territories and Canada. DHSS will not permit any project work to be performed offshore either by the prime vendor, subsidiary, subcontractor or by any other third party. Offshore storage and transmission of DHSS data is prohibited. Onshore project data and project artifacts including backup and recovery files in any form shall not be accessed by offshore staff and shall not be copied or moved offshore. This prohibition extends to maintenance and operations services, technical support services and any other subsequent services under this contract. Violation of any provision in this paragraph will be considered breach of contract. Vendor shall respond with their understanding of and their intent to comply with the requirements in this paragraph

3.19. Other Technical Considerations

3.19.1. While not required, DHSS prefers a Commercial Off-The-Shelf (COTS) solution that is web browser based and that:

3.19.1.1. Uses Microsoft Windows Server as the operating system

3.19.1.2. Uses Microsoft Internet Information Server (IIS) as the web and application server software

3.19.1.3. Uses Microsoft SQL Server for the data store

3.19.1.4. Has been developed using Microsoft C#NET

3.20. Data Interfaces

3.20.1. The Vendor must collaborate with the State and its designees to develop requirements for all data transfers. The Vendor must complete, subject to approval by the State, all interfaces needed for the efficient operation of the MITA SS-A System

3.21. Tracking Capabilities

3.21.1. Map and revise new or existing system impacts to the MITA maturity of any BA/IA/TA or CMS and C&S capability

3.21.2. Track and retrieve the versioning of the MITA SS-A supporting evidence, MITA Roadmap and Concept of Operations

3.21.3. Track all new and existing performance measures and/or critical success factors to determine existing gaps or improvement opportunities for MITA maturity process/system improvements

4. Other Work

4.1. In addition to the assessment artifacts relating to the seven conditions and standards and MITA, the Vendor must produce the deliverables that are detailed in this RFP and keep all assessment reports and other artifacts in the Vendor specific tool. These artifacts must be checked into the repository at the time of delivery

5. Project Location, Work Hours and Conditions

5.1. Core working hours for State Staff are 8AM to 5PM EST/EDT Monday through Friday. Vendor staff must be available during core business hours. The State may require that some Key Project Personnel work from a state location as deemed necessary by the state to support project meetings, training, and other project tasks. Currently all work may be performed remotely. Utilizing teleconferencing platforms such as Skype for Business or Zoom is required

5.2. The State will provide Vendor on-site workspace as needed for the Project, as delineated in the State and Vendor approved Project Plan. Any work requiring assistance from the State staff or completion by State staff will be performed at a State location. The State will provide Internet connection and printer access. The Vendor will be required to provide laptop and phone service for their staff

6. Minimize the project impact on state staff

5.3. Due to current workload and the size of the workforce in DMMA, it is necessary to take steps to minimize time that SMES must spend working on this project by doing the following:

5.3.1. Provide agendas and documents in advance of meetings

5.3.2. Preview questions with state project lead and Information System Unit staff prior to meeting with SMES

5.3.3. Review the following resources to gain an understanding of a business process or technology:

5.3.3.1. System documents

5.3.3.2. Vendor documentation

5.3.3.3. System manuals
5.3.3.4. Process flow diagrams
5.3.3.5. Operational manuals
5.3.3.6. Information System Unit support documentation
5.3.3.7. Previous SS-A artifacts
5.3.3.8. Closed change order documentation
5.3.3.9. RFA's and APD's