DRAFT TECHNICAL SUBMITTAL:
LOT 1: PROGRAM INTEGRITY MANAGEMENT SERVICES ("PIMS")

I-1. Statement of the Project. State in succinct terms your understanding of the problem presented, and the service required by Lot 1 of this RFP. The Offeror's response should demonstrate that the Offeror fully understands the scope of services to be provided, the Offeror's responsibilities, and how the Offeror will effectively manage the contract. The statement of the problem should discuss specific issues and risks associated with the PIMS Services and should include proposed solutions for each. The Offeror should demonstrate how they would develop and maintain relationships with the other selected Offerors for the MMIS 2020 Platform modules.

I-2. Management Summary. Include a narrative description of the proposed effort and a list of the items to be delivered or services to be provided. Include a description of the proposed collaboration with the SI/DH Contractor, the ITC/QA Contractor, the IV&V Contractor, the Tier 1 Support Center Contractor, and other module contractors. The summary will condense and highlight the contents of the Lot 1 Technical Submittal in a manner that allows a broad understanding of the entire Lot 1 Technical Submittal.

I-3. Qualifications.

A. Company Overview. The Offeror must describe the corporate history and relevant experience of the Offeror and any subcontractors. The Offeror must detail information on the ownership of the company (names and percent of ownership), the date the company was established, the date the company began operations, the physical location of the company and the current size of the company. The Offeror must provide a corporate organizational chart.

The Offeror must describe its corporate identity, legal status, including the name, address, telephone number, and email address for the legal entity that is submitting the proposal. In addition, the Offeror must provide the name of the principal officers, a description of its major services and any specific licenses and accreditations held by the Offeror.

If an Offeror is proposing to use the services or products of a subsidiary or affiliated firm, the Offeror must describe the business arrangement with that entity and the scope of the services the entity will provide.

If the experience of any proposed subcontractor is being used to meet the qualifications and requirements of Lot 1 of this RFP, the Offeror must provide the same information as listed above for the subcontractor. This information must be presented separately within this section, clearly identifying the subcontractor's experience and name.

References. The Offeror must provide a list of at least three (3) relevant contacts within the past four (4) years to serve as corporate references. The references must be outside clients (non-PA DHS). This list must include the following for each reference:

1. Name of customer
2. Type of contract
3. Contract description, including type of service provided
4. Total contract value
5. Contracting Officer's name, email, and telephone number
6. Role of subcontractors (if any)
7. Time period in which service was provided.

The Offeror must submit a Corporate Reference Questionnaire, directly to the contacts listed. The references should return the completed questionnaires in sealed envelopes to the Offeror. The Offeror must include these sealed references with its Lot 1 hardcopy Technical Submittal.

The Offeror must disclose any contract or agreement cancellations, or terminations within five (5) years preceding the issuance of this RFP. If a contract or agreement was canceled or terminated for lack of performance, the Offeror must provide details on the customer's allegations, the Offeror's position relevant to the allegations, and the final resolution of the cancellation or the termination. The Offeror must also include each customer's Company or entity name, Address, Contact name, Phone number, and Email address.

The Department may disqualify an Offeror based on a failure to disclose such a cancelled or terminated contract or agreement. If the Department learns about such a failure to disclose after a contract is awarded, the Department may terminate the contract.

B. Prior Experience. The Offeror should include experience, or similar experience with modular implementations, particularly PIMS implementations that were similar in size and complexity as the Pennsylvania's MMIS 2020 Platform Project. Experience includes implementation activities, operations, project management activities, CMS Medicaid Enterprise Certification, knowledge of MMIS, CMS Conditions and Standards, MITA, and MECT checklists, Health Care Exchanges, and supporting the transition from a legacy MMIS or healthcare systems to modern modular systems.

Highlight any modular MMIS or healthcare-related experience that your organization performed within the last four (4) years.

Experience shown should be work done by individuals who will be assigned to this project as well as that of your company. Referenced studies or projects must be identified, and the name of the customer shown, including the name, address, and telephone number of the responsible official of the customer, company, or agency who may be contacted.

C. Offeror Personnel. Include the number of executive and professional personnel, analysts, auditors, researchers, consultants and other staff who will be engaged in the work. Show where these personnel will be physically located during the time they are engaged in the work. For key personnel, include the employee's name and, through a resume or similar document, the key personnel's education and experience. Indicate the responsibilities each individual will have and how long each has been with your company. Identify by name any subcontractors you intend to use and the services they will perform.

A minimum of three (3) client references for Key Personnel must be identified. All client references for Key Personnel must be outside clients (non-Pennsylvania DHS) who can provide information on the individual's experience and competence to perform project tasks similar to those requested in this RFP. Key Personnel may be a member of the Offeror's organization, or any subcontractor included in the Offeror's proposal.

The Offeror must submit a Personnel Reference Questionnaire, directly to the contacts listed. The references should return completed questionnaires in sealed envelopes to the Offeror. The Offeror must include these sealed references with its Lot 1 hardcopy Technical Submittal.

Submitted resumes are not to include personal information that will or will be likely to require redaction prior to release of the proposal under the Right-to-Know Law, including but not limited to home addresses and phone numbers, Social Security Numbers, Drivers' License numbers or numbers from state identification cards

issued in lieu of a Drivers' License, and financial account numbers. If the Commonwealth requires any of this information for security verification or other purposes, the information will be requested separately and as necessary.

The Department has identified five (5) key personnel:

PIMS Executive Account Director
PIMS Project Manager
PIMS Functional Lead
PIMS Testing Manager
PIMS Surveillance Utilization and Review ("SUR") Specialist

Table 3 provides the minimum qualifications and high-level responsibilities for each key personnel. This table also provides the minimum onsite requirements for each key personnel for the phases prior to M&O and the M&O phase. The phases prior to M&O are: 1) Initiation and Planning; 2) Requirements, Design, and Development; 3) Integration, Test, and Implementation. Final onsite percentages will be finalized during contract negotiations. The percent of time onsite during M&O will be as needed determined by future enhancements or other MMIS 2020 Platform changes.

Table 3: Key Personnel Qualifications

ROLE NAME	RESPONSIBILITIES	QUALIFICATIONS	MINIMUM % ONSITE PRIOR TO M&O	MINIMUM % ONSITE DURING M&O
PIMS Executive Account Director	1. Provide overall leadership, coordination, and implementation of the PIMS solution. 2. Communicate with Commonwealth executives and other MMIS module contractors, as needed. 3. Function as the primary point of contact with the MMIS 2020 Platform Executive Review Board, MMIS 2020 Platform Steering Committee and the MMIS 2020 Platform Project Team for activities related to contract administration, overall project management and scheduling, correspondence between the Department and the selected Offeror, dispute resolution, and status reporting to the Department. 4. Oversee Disaster Recovery. 5. Responsible for approving the invoices submitted to the Department.	1. Ability to commit selected Offeror resources as needed to successfully perform work. 2. Ability to identify and resolve project-related issues and risks requiring escalation within the selected Offeror organization. 3. Ability to resolve project-related issues and risks requiring action by subcontractors. 4. Minimum of ten (10) years of experience working on and/or leading large, complex system implementation projects for similar clients. 5. Knowledge of the Health and Human Services ("HHS") industry.	25	10
PIMS Project Manager	1. Provide day-to-day management and be the principal liaison for the PIMS Executive Account Director,	1. Minimum of five (5) years of experience managing large, complex system development, and with	50	As Needed

ROLE NAME	RESPONSIBILITIES	QUALIFICATIONS	MINIMUM % ONSITE PRIOR TO M&O	MINIMUM % ONSITE DURING M&O
	DHS MMIS 2020 Platform Project Manager, Department staff, and other MMIS 2020 module contractors. 2. Guide the project by using project management processes, organizing the project, and managing team work activities consistent with the approved PIMS work plan. 3. Schedule and report activities. 4. Coordinate use of personnel resources. 5. Point of contact for issue identification and resolution. 6. Facilitate implementation of the PIMS Solution. 7. Responsible for all project deliverables. 8. Responsible for CMS Certification. 9. Responsible for QA/QC. 10. Provide oversight for Tier 2 Support.	implementation and operation projects of a scale similar to the MMIS 2020 Platform project. 2. Preferably at least five (5) years of experience managing design and development of healthcare information systems or MMIS. 3. Experience leading teams of more than ten (10) staff, including staff from diverse organizations to successfully implement and operate technology-based solutions.		
PIMS Testing Manager	1. Coordinate testing efforts for the PIMS Module to support implementation, continuity of operations within PROMISe™, and overall MMIS function. 2. Develop the Test Plan for the PIMS and integration with PROMISe™ and other MMIS 2020 Platform modules. 3. Oversee test case and test script development and approval for PIMS integration testing efforts. 4. Facilitate the PIMS test environment setup. 5. Coordinate defect management efforts during PIMS integration testing efforts 6. Work in cooperation with the SI/DH Contractor, ITC/QA Contractor, and other MMIS 2020 Platform module contractors. 7. Participate in Disaster Recovery testing.	1. Minimum of six (6) years of experience with planning and executing all phases of system testing – unit testing, system testing, integration testing UAT, regression testing, performance testing. 2. Experience with and expertise in selection and use of automated test tools and other testing-related tools. 3. Experience managing test teams comprising individuals from multiple organizations.	25	As Needed
PIMS Functional Lead	1. Serve as the PIMS SME to the Commonwealth and other MMIS module contractors.	1. Minimum of five (5) years of experience as a business/functional SME	50	As Needed

ROLE NAME	RESPONSIBILITIES	QUALIFICATIONS	MINIMUM % ONSITE PRIOR TO M&O	MINIMUM % ONSITE DURING M&O
	2. Coordinate Configuration Management activities. 3. Develop, revise, refresh, and deliver PIMS training materials to the ITC/QA Contractor for the PIMS Module. 4. Oversee PIMS Module training. 5. Oversee Tier 2 support.	within an HHS, health system or IT environment.		
PIMS SUR Specialist	1. Provide day-to-day coordination with BPI regarding data analysis schemes and algorithms.	1. Minimum of five (5) years of experience as a data analyst, preferably with a clinical background with an HHS, health system or IT environment.	25	As Needed

Staffing Requirements. The selected Offeror must supply staff who will provide PIMS services. The selected Offeror must be able to work cooperatively with Commonwealth staff and other individuals and entities during the MMIS 2020 Platform Project. The selected Offeror must coordinate and receive direction from designated Department staff.

The selected Offeror may acquire specialized expertise using subcontracts and must identify any proposed subcontractors in response to **Section I-3.D. Subcontractors.**

The selected Offeror may not assign Key Personnel to more than one role or to any other position under the PIMS contract.

For all other personnel, describe job title, position descriptions, responsibilities, and qualifications.

The Offeror must include organizational charts outlining the staffing, reporting relationships and staff members in its response. Show the total number of staff proposed and indicate the Full Time Equivalency to account for any additional staff that are not assigned on a full-time basis. Provide similar information for any subcontractors that are proposed. The organizational chart must illustrate the lines of authority, designate the positions responsible and accountable for the completion of each component in the RFP, indicate the names or job title and number of personnel that will be assigned to each role, and the number of hours per week each person is projected to work on the PIMS contract. The organizational chart must clearly indicate any functions that are subcontracted along with the name of the subcontracting entities and the services they will perform.

Due to the ever-changing landscape of MMIS 2020 Platform Project and its complexity, the Department needs to have consistency when dealing with the selected Offeror's staff and other contractors. The selected Offeror must maintain a core team of qualified staff who are able to support the aspects of the DHS MMIS 2020 Platform as detailed in Lot 1this RFP.

In the case that it is necessary to identify a resource who will not be 100% dedicated to the MMIS 2020 Platform contract, the Offeror must indicate the percent of time that the personnel will be assigned during Design, Development, and Implementation ("DDI") activities and the percent of time that the personnel will be assigned to concurrent projects.

Key Personnel Diversions or Replacement. Once Key Personnel are approved by DHS, the selected Offeror may not divert or replace personnel without the prior approval of the DHS Contract Administrator. The selected Offeror must provide notice of a proposed diversion or replacement to the DHS Contract Administrator at least thirty (30) calendar days in advance of the change and provide the name, qualifications, and background check (if required) of the person who will replace the diverted personnel. The DHS Contract Administrator will notify the selected Offeror within ten (10) business days of the diversion notice whether the proposed diversion is acceptable and if the replacement is approved.

"Divert" or "diversion" is defined as the transfer of personnel by the selected Offerors or its subcontractor to another assignment within the control of either the Offeror or subcontractor. Advance notification and approval does not include changes in Key Personnel due to resignations, death, disability, or dismissal for cause or dismissal as a result of the termination of a subcontract or any other causes that are beyond the control of the selected Offeror or its subcontractor. DHS must approve all replacement personnel.

The DHS Contract Administrator may request that the selected Offeror remove a person from this project at any time. In the event that a person is removed, the selected Offeror will have ten (10) business days to fill the vacancy with a person acceptable in terms of experience and skills, subject to the DHS Administrator's approval. DHS may require the removal of an assigned resource to the PIMS contract at any time.

Key personnel status will be reviewed monthly as part of the **Monthly Status Report** - see **Section II-8.C.** of this RFP.

D. Subcontractors. Provide a subcontracting plan for all subcontractors, including SDB and SB subcontractors, who will be assigned to the PIMS contract. The selected Offeror is prohibited from subcontracting or outsourcing any part of this Project without the written approval from the Commonwealth. For each subcontractor included in your subcontracting plan, you must provide:

1. Name of subcontractor;
2. Address of subcontractor;
3. Number of years worked with the subcontractor;
4. Number of employees by job category to work on this project;
5. Description of services to be performed;
6. What percentage of time the staff will be dedicated to this project;
7. Geographical location of staff; and
8. Resumes (if appropriate and available).

The Offeror's subcontractor information must include (through a resume or a similar document) the employees' names, education, and experience in the services outlined in Lot 1 of this RFP. Information provided will also indicate the responsibilities each individual will have in this Project and how long each has been with the subcontractor's company.

I-4. Training. The ITC/QA Contractor is responsible for the MMIS 2020 Platform training; however, the selected Offeror will provide the ITC/QA Contractor with system and technical documentation to support the creation and development of training materials for end users. The selected Offeror must use the train the trainer approach to train the ITC/QA Contractor for initial training and for follow up training on enhancements and modifications to the PIMS Module. Training will be a collaborative process; the ITC/QA Contractor is the lead trainer working collaboratively with the selected Offeror, the SI/DH contractor and other MMIS 2020 Platform Contractors. The selected Offeror will

provide the ITC/QA Contractor with follow up training materials to support enhancements to the PIMS Module. The selected Offeror, with the ITC/QA Contractor, will conduct training of each module's functionality, user interfaces, technical components, interfaces, reporting, and other operational requirements. The selected Offeror must provide and maintain its own training environment.

The selected Offeror will focus training requirements on technical end users and the ITC/QA Contractor will focus training requirements to the MMIS 2020 Platform stakeholders. The selected Offeror must design, develop and implement a comprehensive training plan with training materials to provide technical training to the Department and MMIS 2020 Platform module contractors on PIMS Module components and functionality. The training must communicate an overview of the solution, which includes technical framework, integration touchpoints, governance processes, new system components, business processes, services, implementation requirements, and other project requirements. The ITC/QA Contractor will lead training activities on CRM functionality for the MMIS 2020 Platform module contractors and stakeholders.

The Offeror must describe its training solution, the training approach and a sample of the training plan to support the training of the ITC/QA Contractor in its Lot 1 Technical Submittal.

I-5. Financial Capability. Describe your company's financial stability and economic capability to perform the contract requirements. Provide your company's financial statements for the past two (2) fiscal years. If your company is a publicly traded company, please provide a link to your financial records on your company website in lieu of providing hardcopies. Financial statements must include the company's Balance Sheet and Income Statement or Profit/Loss Statements. Also include a Dun & Bradstreet comprehensive report, if available. The Commonwealth may request additional information it deems necessary to evaluate an Offeror's financial capability as part of its contractor responsibility determination.

I-6. Work Plan. Describe in narrative form your technical plan for accomplishing the work. Modifications of the task descriptions are permitted; however, reasons for changes should be fully explained. Indicate the number of person hours allocated to each task. Include a Program Evaluation and Review Technique or similar type display, time related, showing each event. If more than one approach is apparent, comment on why you chose this approach. Where appropriate, the selected Offeror must use automation to facilitate completion of tasks. Describe the relationship between primary staff described in **Section I-3.C Offeror Personnel** and the specific tasks, assignments, and deliverables proposed to accomplish the scope of work. Indicate the number of staff hours allocated to each task.

The Department will provide strategic leadership and regulatory oversight. Describe how your approach will establish standards that maintain fidelity to the MMIS 2020 Platform Project objectives while minimizing disruptions. Describe how communications and work flow between your team and the MMIS 2020 Platform stakeholders will occur.

Describe your management approach, including how you will implement the proposed work plan. Where possible, the Offeror must provide specific examples of methodologies or approaches, including monitoring approaches, it will use to fulfill the Lot 1 technical submittal requirements and examples of similar experience and approach on comparable projects. The Offeror must describe the management and monitoring controls it will use to achieve the required quality of contract services and all performance requirements. The Offeror must also describe the approach to internally monitor and evaluate the effectiveness of meeting the contract requirements.

Items to be addressed in the work plan approach are included in the Tasks section below:

Tasks:

A. Program Management. The Department will provide strategic oversight for the MMIS 2020 Platform Project, including oversight of all contractors. The selected Offeror has primary responsibility for the services, under a resulting contract, for the lifecycle of the PIMS Module. Under the strategic guidance of the Department, the ITC/QA contractor will be the primary project management office for the MMIS 2020 Platform Project.

Throughout the life of the PIMS Module contract, the selected Offeror must use project management techniques that include a comprehensive project plan that is designed, developed, implemented, monitored, tracked and maintained. The selected Offeror must develop status reports and project plan updates as defined in **Section I-8 Reports and Program Control.**

The selected Offeror must design, develop, implement, and maintain the PIMS Master Work Plan ("PIMS-MWP") for the successful completion of services within scope, budget, and schedule throughout the term of the PIMS Module contract. The work plan must adhere to industry best practices for project management, such as Information Technology Infrastructure Library ("ITIL") or Project Management Body of Knowledge ("PMBOK®"). Offerors must describe the standard that it will use and its rationale for choosing that project management tool.

The selected Offeror must have a PIMS-MWP that will act as a confirmation of project scope, MECL phases, implementation objectives, and result in the product being delivered on time and meeting all requirements specified in Lot 1 of the RFP.

The selected Offeror must develop the PIMS-MWP that, at a minimum, includes the following deliverables:

1. PIMS Charter and Project Roles
2. PIMS Defect Management Plan
3. PIMS Change Management Plan
4. PIMS Release Management Plan
5. PIMS Business Rules Engine Management Plan
6. PIMS Quality Management Plan
7. PIMS Test Plan
8. PIMS Rollback Plan
9. PIMS CMS Certification Plan
10. PIMS Data Management Strategy Plan
11. PIMS Closeout Plan
12. PIMS Maintenance and Operations Plan
13. PIMS Technical Infrastructure Document
14. PIMS System Design Document
15. PIMS Turnover Plan

Upon approval by the Department, the selected Offeror must execute and monitor the PIMS-MWP. As changes are approved through the Change Management process, the selected Offeror must update plans and provide the Department with a summary of the changes as part of its reporting requirements. Offerors may recommend an alternative to this reporting requirement and provide a rationale for their recommendation. The selected Offeror must immediately alert the Department to any risk to the project identified as the result of the change.
Deliverable: PIMS-MWP

The Offeror must describe its approach to designing, developing, implementing, and maintaining the PIMS-MWP with recommended timelines for completion of the components. Additionally, the Offeror must describe how it will coordinate and work with MMIS 2020 Platform stakeholders to execute and monitor the PIMS-MWP.

The selected Offeror's specific roles in designing, developing, implementing and maintaining the following components of the PIMS-MWP are addressed below.

B. PIMS Charter and Project Roles. The selected Offeror will design, develop, implement, and maintain the PIMS Charter and Project Roles to document and maintain end-product scope. The selected Offeror must deliver the initial PIMS Charter and Project Roles for the Department's approval within twenty-two (22) business days after the purchase order date and update as needed throughout the MMIS 2020 Platform lifecycle. At a minimum, the PIMS Charter and Project Roles will address:

1. **PIMS Charter**
   a. Project leadership and key stakeholders
   b. Overview of the project
   c. Project approach
   d. Scope
   e. High-level schedule
   f. Assumptions
   g. Constraints and risks
   h. Responsibility matrix

2. **PIMS Project Roles**
   a. **Project Plan.** Under the strategic guidance of the Department**,** the ITC/QA Contractor will design, develop, implement and maintain the Integrated Master Schedule ("IMS") that includes each MMIS 2020 Platform module. The IMS will serve as the MMIS 2020 Platform baseline schedule, including the transition from the legacy system. Development and modifications to the PIMS project plan occurring throughout the MMIS 2020 Platform lifecycle must be approved by the Department. The Department requires that the PIMS project plan is both business and technically-oriented with a focus on the technical aspects of the PIMS Module. The selected Offeror must coordinate the PIMS Module detailed project plan with the ITC/QA Contractor's IMS for distribution to the SI/DH Contractor, and other MMIS 2020 Platform module contractors. The selected Offeror must document its project role in the PIMS Charter and Project Roles deliverables. The selected Offeror must maintain a detailed project plan and include in the weekly report as defined in **Section I-8 Reports and Program Control**.

   b. **Communications**. Under the strategic guidance of the Department, the ITC/QA Contractor will design, develop, implement, and maintain the Master Communications Plan for the MMIS 2020 Platform. The Master Communications Plan will address communications to all stakeholders, MMIS 2020 Platform contractors, and the legacy system contractor. The ITC/QA Contractor will develop a standard template that the selected Offeror must complete for the PIMS Module communications. Modifications to the OPD Module communications occurring throughout the MMIS 2020 Platform lifecycle must be approved by the Department. The Department requires that the OPD Module communications is both business and technically oriented with a focus on the technical aspects of the OPD module. The selected Offeror must coordinate and share the plan with the ITC/QA Contractor for distribution to the SI/DH Contractor and other MMIS 2020 Platform module contractors. The selected Offeror must document in the PIMS Charter and Project Roles deliverables its project role in the Master Communications Plan for the MMIS 2020 Platform.

c. **Risks and Issues.** Under the strategic guidance of the Department, the ITC/QA Contractor will design, develop, implement, and maintain the Risks and Issues Management Plan for the MMIS 2020 Platform. The Risks and Issues Management Plan will include issue identification, tracking, risk analysis, mitigation recommendations, reporting risk information to the Department and other MMIS 2020 Platform Stakeholders, and resolution. The ITC/QA Contractor must account for the transition from the legacy system to the MMIS 2020 Platform in the Risks and Issues Management Plan. The selected Offeror must develop, maintain, and share the PIMS Module Risks and Issues with the ITC/QA Contractor for distribution to the Department, SI/DH Contractor, and other MMIS 2020 Platform module contractors. At a minimum, the PIMS Module Risks and Issues must include, risk identification, issue identification, tracking, analysis, mitigation recommendations, reporting, and both interim and final resolutions. The Department anticipates risks and issues are both business and technically oriented with a focus on the technical aspects of the PIMS Module. The selected Offeror must document in the PIMS Charter and Project Roles deliverables its project role in the communication of risks and issues to the ITC/QA Contractor for inclusion in the MMIS 2020 Platform Risks and Issues Management Plan.

d. **Requirements Management**. Under the strategic guidance of the Department, the ITC/QA Contractor will design, develop, implement, and maintain the Requirements Management Plan for the MMIS 2020 Platform. The ITC/QA Contractor will at a minimum gather, organize, prioritize, and document business requirements for the lifecycle of the MMIS 2020 Platform, including enhancements made during the M&O phase for the PIMS Module. The process must also identify the requirements for the EDW.

   The ITC/QA Contractor will design, develop, implement, and maintain a detailed requirements collection process to document and verify all requirements have been captured for the PIMS Module. The ITC/QA Contractor will develop and use a process that includes an analysis of business processes and needs, and translating these processes and needs into formal requirements.

   The Department has gathered initial high-level business requirements for the PIMS Module. The requirements are grouped by business functional area and were traced to the CMS certification checklists. The ITC/QA Contractor will use methods to collect requirements that include work sessions, surveys, interviews, policy and regulatory analysis, business rule reviews, facilitated Joint Application Design ("JAD") sessions and any other means necessary to identify all requirements. The selected Offeror is required to provide technical assistance throughout the requirements gathering processs.

   The ITC/QA Contractor will consolidate the final requirements approved by the Department into a Business Requirements Document ("BRD"), and will cross walk the requirements in the BRD to the CMS certification checklist and the PIMS Module's RFP technical submittal requirements. The selected Offeror will collaborate and assist to ensure all requirements are captured.

   The ITC/QA Contractor will complete a Business Gap Analysis to determine if the business requirements meet or exceed what is required for CMS certification, federal and state regulations, and the Department's desired functionality. The selected Offeror will collaborate and assist to ensure the analysis is complete and meets CMS Certification requirements.

   The ITC/QA Contractor will complete the Requirements Traceability Matrix ("RTM") and the selected Offeror will verfy the RTM.

The BRD and the RTM become the initial baseline for the design phase and a reference point throughout the SDLC for determining whether the final product meets the approved requirements. The RTM must, for each identified requirement, contain the source of the requirement, the applicable CMS checklist items, the implementation point, and reference to the test case or script that validates the proper implementation of the requirement. The selected Offeror will collaborate with the ITC/QA contractor to validate the RTM.

Once the Department approves the BRD, the BRD becomes the blueprint for the selected Offeror to build the Business Design Documents ("BDD"), General System Design ("GSD"), and Systems Requirements Design ("SRD"). COTS products are not required to build or provide a GSD or SRD; however, a BDD is required. The selected Offeror will deliver the GSD, SRD, if required, and a Business Design to the ITC/QA Contractor for review with the SI/DH and other impacted MMIS 2020 Module contractors. The ITC/QA Contractor will submit all documents to the Department for final approval.

When the GSD, SRD, if required, and BDD are approved by the Department, the ITC/QA Contractor will conduct a Technical Gap Analysis to confirm that the technical solutions developed by the module contractors meet the business requirements. The selected Offeror will collaborate and verify the Technical Gap Analysis meets the business requirements. If the technical gap analysis reveals deficiencies, the selected Offeror will work with the ITC/QA Contractor to rewrite the GSD. The Department will approve the GSD, and the selected Offeror will commence building the PIMS Module.

The selected Offeror must document in the PIMS Charter and Project Roles deliverable its project role in the Requirements Management Plan for the MMIS 2020 Platform.

e. **Project Documentation.** Under the strategic guidance of the Department, the ITC/QA Contractor will design, develop, implement, and maintain the MMIS 2020 Platform Documentation Management Plan, including the management of the content of the MMIS 2020 Platform Artifact Library, where all MMIS 2020 Platform documents will be stored. The ITC/QA Contractor will develop a standard template or style guide that the selected Offeror must follow when creating PIMS Module documentation. The ITC/QA Contractor will establish and maintain revision control for all artifacts. The PIMS selected Offeror must use ITC/QA supplied templates to create the following documents:
    1) Flow diagrams and reference materials, including system flow to and from the SI/DH.
    2) Design documents, including interface and architecture.
    3) Data documents, including development and management of defined data entities, attributes, data models, and relationships that convey the meaning and use of Medicaid data and information.
    4) List of application servers and usage.
    5) List of web servers and usage.
    6) Network IP and port details.
    7) Environment variables.
    8) Test Plan.
    9) Training Materials.
    10) Hyperlinks.
    11) Document links.
    12) Organization charts.
    13) Contact details.
    14) Tier 2 Technical support procedures.
    15) Other documents requested by the Department

The selected Offeror must document in the PIMS Charter and Project Roles deliverable its role in the preparing PIMS Module documentation in collaboration with the ITC/QA Contractor.

f. **Implementation Plan.** Under the strategic guidance of the Department, the ITC/QA Contractor will design, develop, implement, and maintain the MMIS 2020 Platform Implementation Plans to move MMIS 2020 modules and functionality from DDI and testing to operations. The selected Offeror will collaborate with the ITC/QA Contractor in preparing the PIMS Implementation plan. The plan will provide for the transition from the legacy system to the PIMS Module.

The selected Offeror will collaborate with the ITC/QA contractor in preparing the PIMS Implementation plan. At a minimum, the Implementation Plan will include:

1) Description of intended functionalities and their impact on implemented MMIS 2020 Platform modules
2) BDD, BRD, GSD and SRD if not a COTS product, Business and Technical Gap Analysis
3) Configuration Plan
4) Deployment strategies
5) Rollback Plan
6) Legacy system and installed modules impact analysis
7) Transition Plan from Legacy functionality to the PIMS Module
8) Functionality comparison template comparing Legacy functionality to the PIMS Module
9) Test Result analsysis and review
10) "Go live" checklist
11) Logistics and meeting management
12) Issue reporting and resolution process
13) Defect reporting and resolution process
14) User support, including training Updates to the MMIS 2020 comprehensive user manual

The ITC/QA Contractor will develop a "go live" checklist to document at a minimum, that the system can accept all transaction formats required under HIPAA, accept proprietary forms and formats designated by DHS, produce required EDW extracts, generate reports for users, and operate as designed to meet business needs. The selected Offeror must collaborate with the ITC/QA Contractor to develop, document, and use the "go live" checklist. The Department must approve the "go live" checklist. The selected Offeror must document in the PIMS Charter and Project Roles Deliverable its project role in the preparing the Implementation Plan in collaboration with the ITC/QA Contractor.

g. **Data Conversion Plan.** Under the strategic guidance of the Department, the SI/DH Contractor will design, develop, implement and maintain the MMIS 2020 Platform Data Conversion Plans to move MMIS 2020 modules and functionality from design, development, implementation and testing to operations. The ITC/QA Contractor will evaluate the Data Conversion Plan, identify any gaps, and make recommendations to close gaps. The plan will provide for the transition from the legacy system to the PIMS Module.

The selected Offeror will collaborate with the SI/DH Contractor in preparing the Data Conversion plan. At a minimum, the SI/DH Contractor will include in the MMIS 2020 Platform Module Data Conversion Plan:

1) A data management strategy that will support integration, optimization, quality, stewardship, standards, and governance of data.

2) A description of appropriate skill sets, processes, technologies/tools, and any naming conventions followed.
3) Approach to conversion, cleansing and migration.
4) Approach to risk management for data conversion effort.
5) Approach for testing migration or converted data.
6) Approach to reporting the number of records successfully converted vs. errors or exceptions.
7) Approach for cleansing data to prepare it for loading to the proposed solution that is refined as necessary.
8) Approach to resolving data conversion errors and issues.
9) Approach for supporting the Department validation of converted data.
10) Tasks, timelines, and responsible parties for all conversion and migration tasks.
11) Entrance and exit criteria for each phase of the effort.

Deliverable: PIMS Charter and Project Roles

The Offeror must describe its approach to the design, development, implementation, and maintenance of the PIMS Charter and Project Roles.

C. PIMS Defect Management Plan. The selected Offeror must identify and resolve defects pertaining to the PIMS Module that are identified during testing as well as during production after implementation.

The Department and the ITC/QA Contractor are responsible for overall defect management for the MMIS 2020 Platform and will develop the MMIS 2020 Platform Defect Management Plan to identify, track, monitor, and report defects identified during testing and production to the Department and other MMIS 2020 Platform Stakeholders. The ITC/QA Contractor will develop standards for defect identification, tracking, monitoring, and reporting. The selected Offeror must offer recommendations, as may be appropriate, to enhance the standards.

The selected Offeror will leverage the MMIS 2020 Platform CRM tool, developed by the SI/DH Contractor, to report and track issues and defects. The Department and the ITC/QA Contractor will manage the Change Control Board ("CCB") which is responsible for defect management through the lifecycle of the MMIS 2020 Platform Project. The selected Offeror must participate in the CCB.

The Department will determine the severity and priority of defects and will use defect resolution in accordance with the protocols in the chart below. The Severity Level and Definition columns will be used pre-M&O and the remaining columns will be determined for User Acceptance Testing ("UAT"). During M&O all columns will be used.

Severity Level	Definition	Response Time	Corrective Action Plan	Work-around Time	Final Resolution	Reconciliation Plan
Critical	MMIS 2020 Platform Portals or MMIS 2020 Platform module(s) are unavailable creating an inoperable state. Users unable to perform routine job functions that are mission critical.	15 Minutes	1.5 hours	2 hours	1 calendar day	3 calendar days

Severity Level	Definition	Response Time	Corrective Action Plan	Work-around Time	Final Resolution	Reconciliation Plan
	Qualifying condition examples include: • Inability to adjudicate claims • Failure or Inability to process financial cycle(s) •Failure to provide complete eligibility responses greater than 80% of the time. •Any Commonwealth defined mission critical condition.					
Significant	MMIS 2020 Platform Portals or MMIS 2020 Platform module(s) are creating a serious system functionality loss that requires workarounds. Users are partially incapable of completing their normal functions. Qualifying condition examples include: •Incorrect claims adjudication • Limited access to module(s) • Inability to meet established timeframes for production data imports, exports and loading. • Issue affects large group of users with complicated workaround. • Provider or state staff unable to access remittance advice reports or 835 files less than three (3) months old.	1.5 hours	3 hours	4 hours	2 calendar days	7 calendar days
Moderate	MMIS 2020 Platform Portals or MMIS 2020 Platform module(s) are creating a limited loss of functionality. Moderate system issues where workarounds exist but, on a whole, do not affect production. Qualifying condition examples include: • Report is not available but can be generated manually • Issue affects small subgroup of users with uncomplicated workaround	1 calendar day	5 calendar days	10 calendar days	30 calendar days	40 calendar days

Severity Level	Definition	Response Time	Corrective Action Plan	Work-around Time	Final Resolution	Reconciliation Plan
	• Mouse hover feature not triggering text display					
Minor	Inconsequential loss of functionality. Impact to user is slight to unknown. Effect on MMIS 2020 Platform system functions negligible to no impact. Issue cosmetic in nature such as spelling error or branding issue. Qualifying condition examples include: • Report incorrectly named • Minor page layout issue • Help page missing or incomplete	7 calendar days	30 calendar days	n/a	90 calendar days or as mutually agreed upon	As mutually agreed upon

Deliverables:
1. PIMS Defect Management Plan
2. PIMS Defect Management Report

The selected Offeror must deliver the initial PIMS Defect Management Plan and the initial PIMS Defect Management Report within thirty-three (33) business days of the purchase order effective date; and must update weekly to ensure the project is on schedule and meets CMS Certification requirements. The PIMS Defect Management Plan will be reviewed monthly as part of the **Monthly Status Report** (see **Section I-8.C** of this RFP).

The Offeror must describe its approach to the design, development, implementation, and maintenance of the PIMS Defect Management Plan.

D. PIMS Change Management Plan. The selected Offeror must participate in the Change Control Board ("CCB"), as needed; and react to requested changes to the PIMS Module by providing design documents, estimates, and timelines. The Department and the ITC/QA Contractor manage the CCB and review requested changes for the MMIS 2020 Platform Project. The Department has final approval authority on the priority and scheduling of all changes. Refer to**, Section I-8.E** for information about the CCB meeting.

The selected Offeror is responsible for changes to the PIMS Module and must recommend changes to the CCB for approval.

The selected Offeror must design, develop, implement, and maintain the PIMS Change Management Plan as a participant of the CCB. The selected Offeror will deliver the initial PIMS Change Management Plan within thirty-six (36) business days after the purchase order effective date for the Department's approval; and must update weekly throughout the MMIS 2020 Platform Project. The plan must contain a methodology for determining and reporting the level of effort, hours, resources, scheduling, and cost of the change.

Deliverable: PIMS Change Management Plan

The Offeror must describe its approach to the design, development, implementation, and maintenance of the PIMS Change Management Plan.

E. PIMS Release Management Plan. Under the strategic guidance of the Department, the ITC/QA Contractor is responsible for developing and executing the MMIS 2020 Platform Release Management Plan. The ITC/QA Contractor will develop a standard template to capture information from the MMIS 2020 Platform and legacy system contractors when developing the MMIS 2020 Platform Release Management Plan. The selected Offeror will have an opportunity to offer recommendations to enhance the template.

The Department will set release timelines in coordination with the MMIS 2020 Platform Project contractors and the legacy system contractor. During the transition from the legacy system to the MMIS 2020 Platform, the Department anticipates that the release schedule will be based on the **MMIS 2020 Platform Timeline**.

After the full transition to the MMIS 2020 Platform (during M&O), the release schedule will be determined by other factors, such as state and federal mandates, enhancements and module updates or replacements. During M&O the ITC/QA Contractor will be responsible for developing and executing the Release Management Plans. The selected Offeror will continue to collaborate and support the ITC/QA Contractor in future releases.

The ITC/QA Contractor will lead release planning meetings, which will be attended by the Department, the legacy system contractor, and MMIS 2020 Platform module contractors. The selected Offeror must participate in the Release Planning Meetings – see **Section I-8.E. Meetings** of this RFP. The Department will provide final approval before a release can be implemented into production.

The Department requires that the MMIS 2020 Platform Release Management Plan is business oriented whereas the release management plans developed by the MMIS 2020 Platform module contractors, including the PIMS Release Management Plan, will be both business and technically oriented with a focus on the technical aspects of the release. Regardless, the selected Offeror must coordinate the PIMS Release Management Plan with legacy and other MMIS 2020 Platform contractors.

The selected Offeror will design, develop, implement, and maintain the PIMS Release Management Plan using the MMIS 2020 Platform Release Management Plan. The selected Offeror will deliver the initial PIMS Release Management Plan within forty (40) business days after the purchase order effective date; and will update no later than twenty-nine (29) business days prior to each module or functionality release. The selected Offeror must coordinate the PIMS Release Management Plan with the ITC/QA Contractor and the legacy system and MMIS 2020 Platform contractors to maintain ongoing operations of the Department's program and facilitate a seamless transition to the MMIS 2020 Platform with the ultimate goal of achieving CMS certification.

Deliverable: PIMS Release Management Plan

The Offeror must describe its approach to the design, development, implementation, and maintenance of the PIMS Release Management Plan.

F. PIMS Business Rules Engine Management Plan. The selected Offeror will design, develop, implement, and maintain a PIMS Business Rules Engine Management Plan that describes its approach to tracking and controlling changes of the PIMS Module specific business rules. All business rules which interact with other MMIS 2020 modules must be provided to the SI/DH Business Rules Engine. The selected Offeror must submit the initial PIMS Business Rules Engine Management Plan within forty-three (43) business days after the purchase order effective

date and review the plan monthly and update with changes. The plan must include a description including how the selected Offeror manages business rule changes to the PIMS Module.

Deliverable: PIMS Business Rules Engine Management Plan

The Offeror must describe its approach to the design, development, implementation, and maintenance of the PIMS Business Rules Engine Management Plan.

G. PIMS Quality Management Plan. The MMIS 2020 Platform is subject to IV&V oversight. The list of artifacts for CMS Certification subject to IV&V oversight can be found at https://www.medicaid.gov/medicaid/data-and-systems/mect/index.html.

The ITC/QA Contractor will provide Quality Management ("QM") services. The documents prepared by the selected Offeror including: system and cyber security plan, test plans, COOP and DR plans, data conversion plans, and rollback plans are subject to QA reviews by the ITC/QA Contractor as well as the IV&V Contractor. Under the strategic leadership of the Department, and with feedback from the MMIS 2020 Platform module contractors, the ITC/QA Contractor will develop MMIS 2020 Platform standards; such as those for defect identification, tracking, monitoring, and reporting. The ITC/QA Contractor is responsible for the application of standards through quality control ("QC") measures.

In addition to IV&V Contractor oversight and the QM measures described above, each MMIS 2020 Platform module contractor must have QM processes for its modules and services.

The selected Offeror will design, develop, implement, and maintain a PIMS QM Plan to maintain quality practices for the lifecycle of the PIMS Module. The selected Offeror will deliver the initial PIMS QM Plan within seventy-fifty-four (54) business calendar days after the purchase order effective date. The selected Offeror will develop a PIMS QM Plan that includes quality assurance of processes and quality control to provide fidelity to MMIS 2020 Platform standards. The selected Offeror must include in its PIMS QM Plan, at a minimum:

1. Overview of QM activities and tasks to be performed;
2. Processes and procedures for conducting QA/QC activities, including procedures for documenting, resolving, and reporting issues and risks identified during QA/QC activities, or problems that may be identified by the Department;
3. Performance monitoring reviews, measures, and reports;
4. Roles and responsibilities of the selected Offeror and Subcontractors if applicable, in performing QA/QC activities; and,
5. QC procedures for modules' fidelity to standards developed by the selected Offeror such as data exchanges, telecommunications set up ("VPN", etc.), interfaces, and single sign-on requirements.

Deliverable: PIMS Quality Management Plan

The Offeror must describe its approach to the design, development, implementation, and maintenance of the PIMS QM Plan.

H. PIMS Test Plan. In the Testing Phase of the SDLC, the ITC/QA Contractor, selected Offeror, and MMIS 2020 Platform module and legacy system contractors have varying roles dependent upon the level and objective of the test being conducted. While the Department must approve all test results, tests are led by different entities, and test artifacts are subject to QA and IV&V review. Accordingly, the selected Offeror and all MMIS 2020 Platform

module contractors must cooperate with the Department to develop a comprehensive testing plan that provides for each component meeting or exceeding the functional, technical, security, and performance requirements, including bi-directional traceability to requirements and design prior to its implementation. Note: The scope of testing refers to testing of modules or functionality prior to release during the lifecycle of the MMIS 2020 Platform.

The selected Offeror and module contractors must update the module or functionality being tested as well as the testing environment as the result of defects identified. The selected Offeror must communicate testing status to the Department and appropriate stakeholders throughout this phase.

MMIS 2020 Platform testing must be conducted in accordance with industry best practices. For this RFP, the Department has chosen the Guide to the Software Engineering Body of Knowledge Version 3.0 (SWEBOK®) as its reference; however, Offerors may choose a different reference. Offerors must identify their reference and provide a rationale for the standard it chooses.

The minimum levels of MMIS 2020 Platform testing are defined below along with the test lead, participation, and QA requirements. Offerors may recommend additional levels or strategies for the Department to consider.

1. **Unit Testing**: Unit testing verifies the functioning of a single module in isolation, including the PIMS Module, or other functionality that is tested. Unit testing is self-led by the module contractor and subject to QA where applicable. For example, COTS products are exempt; however custom code is not.

2. **Integration Testing**: Integration testing verifies the interactions between the PIMS Module and the SI/DH. The SI/DH Contractor leads this level of testing in collaboration with the selected Offeror.

3. **System Testing**: System testing tests downstream and end-to-end module-to-module functionality between the PIMS Module and the SI/DH. System testing includes assessing non-functional system requirements, including security, speed, accuracy, and reliability; and assessing functionality to external interfaces to other applications, utilities, hardware devices, operating environments, providers, business partners, and other stakeholders. The SI/DH Contractor will submit to the Department, the results of security vulnerability testing, and the results are subject to QA.

The levels of MMIS 2020 Platform testing contain various objectives. Offerors may recommend additional objectives or strategies for the Department to consider. The objectives below are the minimum to be conducted:

1. UAT
2. Installation User Testing (Operational Readiness)
3. Regression Testing
4. Performance Testing
5. Stress Testing
6. Back-to-Back Testing
7. Recovery Testing
8. Interface Testing
9. Usability and Human Computer Interaction Testing

The selected Offeror, in collaboration with the ITC/QA Contractor and SI/DH Contractor, must develop test plans that measure and test the MMIS 2020 Platform's ability to function as designed and meet the Department's business needs. The selected Offeror must deliver each PIMS Test Plan thirty-three (33) business days prior to the testing of each PIMS Module upgrade. Test Cases and scripts must include positive and negative scenarios. The negative scenarios must include stress testing the system with bad or invalid data to validate that it is rejected

correctly. Test scripts must provide step-by-step instructions for executing test cases, including the expected results.

The selected Offeror must provide and maintain its own testing environment; however, the SI/DH Contractor will provide and maintain a testing environment for the SI/DH that allows the MMIS 2020 Platform modules, including the PIMS Module, to use for the appropriate level of test. The selected Offeror, in collaboration with the SI/DH Contractor, will provide the various system environments needed to perform the required testing and training activities for the MMIS 2020 Platform, including UAT. The environments must include an integrated test environment to accommodate testing the successful implementations of modules and technical integration activities. The integrated test environment must allow for end-to-end testing and be capable of a mirror of the production system.

The selected Offeror, in collaboration with the SI/DH Contractor, must develop test plans and test summary reports in accordance with industry standards. Plans must outline various parameters, resources, methods, and criteria to fully test the system. The selected Offeror must track defects in the CRM tool.

The SI/DH Contractor and the selected Offeror will create and maintain the logical environments for development and testing, which includes UAT. The selected Offeror must cooperate with the IV&V Contractor, who is responsible for evaluating the test results of all contractors.

The selected Offeror, in collaboration with the SI/DH Contractor, must report the results of testing to the MMIS 2020 Platform module and legacy system contractors, and the Department. The report must identify successes, failures, defects and deviations of the expected results. The report must also identify risks, issues and dependencies that could prevent successful implementation. The selected Offeror, in collaboration with the SI/DH Contractor, must provide recommendations for corrective action. The Department will approve the test deliverables and results.

Deliverables:

1. PIMS Integration Test Plan
2. PIMS System Test Plan

The Offeror must describe its approach to the design, development, implementation, and maintenance of the PIMS Test Plan.

I. PIMS Rollback Plan. The selected Offeror must design, develop, implement, and maintain the PIMS Rollback Plan. Every module must have a rollback plan to halt or restore the system to its original, pre-conversion condition because of an issue or defect found during implementation or post-implementation. The selected Offeror must develop a rollback plan related to the PIMS Module and functionality. The ITC/QA Contractor is responsible for the QA of individual rollback plans and the plans are subject to IV&V review.

The ITC/QA Contractor is responsible for developing a standard template that the selected Offeror must follow when creating its individual rollback plan. The selected Offeror is able to offer recommendations to enhance the template.

The ITC/QA Contractor will compile the PIMS Rollback Plan as part of the MMIS 2020 Platform Master Rollback Plan. The Master Rollback Plan must contain checkpoints for the Department's review where a decision will be made to execute or rollback the release. The plan must include factors and risks to be considered in making the decision. The selected Offeror will deliver the initial PIMS Rollback Plan sixty-five (65) business days prior to the

implementation of each module and update the PIMS Rollback Plan eight (8) business days prior to the actual module implementation for the Department's approval.

Deliverable: PIMS Rollback Plan

The Offeror must describe its approach to the design, development, implementation, and maintenance of the PIMS Rollback Plan.

J. PIMS CMS Certification Plan. The ITC/QA Contractor will develop a plan for CMS certification of the MMIS 2020 Platform. The selected Offeror will deliver the initial PIMS CMS Certification Plan within one hundred twenty-nine (129) business days after the purchase order effective date and update within twenty-two (22) business days after a module is onboarded. The Department will use the MMIS module checklists for certification found at https://www.medicaid.gov/medicaid/data-and-systems/mect/index.html. The selected Offeror will work with the ITC/QA Contractor to complete the evidence columns of the checklists for review by CMS for the PIMS Module. The selected Offeror must complete certification activities from a technical perspective for the PIMS Module to complete MECT checklists prior to gate reviews.

The selected Offeror must collaborate with the ITC/QA Contractor, IV&V Contractor, and the Commonwealth, to obtain CMS Certification.

The selected Offeror, in collaboration with the SI/DH Contractor and the ITC/QA Contractor, must design, develop, implement, and maintain the PIMS CMS Certification Plan that includes processes and procedures to manage certification requirements throughout the MMIS 2020 Platform lifecycle.

The Plan must include:

1. Completing the certification checklists and artifacts
2. Completing certification deliverables
3. Validating solution functionality against the checklist
4. Creating traceable deliverables to the checklist
5. Document and artifact delivery to the MMIS 2020 Platform Artifact Library

The selected Offeror will participate in CMS Certification activities, as needed by the Department, which include:

1. Cooperating with the SI/DH, IV&V and ITC/QA Contractors
2. Completing applicable certification checklists
3. Creating any necessary artifacts for certification
4. Responding to CMS queries before, during, and after gate reviews and site visits in collaboration with the Department.

Deliverables:

1. PIMS CMS Certification Plan
2. Completed Certification Checklists
3. Artifacts required by the ITC/QA Contractor, IV&V Contractor, DHS or CMS

The Offeror must describe its approach to the development and execution of the PIMS CMS Certification Plan.

K. PIMS Data Management Strategy Plan. The selected Offeror must design, develop, implement and maintain the PIMS Data Management Strategy Plan. The data management strategy plan must include the following concepts: Data Integrity (data cannot be modified undetectably), Data Availability (access is not inappropriately blocked or denied), Data Authenticity (validation of transactions), Data Security (encryption and Department

approved security protocols and processes), Non-repudiation of Data (parties to a transaction cannot deny their participation in the transaction). The selected Offeror must demonstrate through data analysis that the implementation outcomes have been validated and are accurate. The methodology of the data analysis must be described in the data management security plan. The selected Offeror will deliver the initial PIMS Data Management Strategy Plan within forty-three business days after the purchase order effective date and review the plan monthly and update with changes.

Deliverable: PIMS Data Management Strategy Plan

The Offeror must describe its approach to the design, development, implementation, and maintenance of the PIMS Data Management Strategy Plan.

L. PIMS Closeout Plan. The selected Offeror must design, develop, implement, and maintain the PIMS Closeout Plan. The selected Offeror will deliver the initial PIMS Closeout Plan within twenty-two (22) business days after the implementation of the PIMS Module. When the PIMS Module is implemented, the selected Offeror must certify, in writing, to the Department that all SDLC activities have been completed per the implementation plan and all risks, issues, and action items are closed for the PIMS Module in collaboration with the SI/DH Contractor, ITC/QA Contractor, and IV&V Contractor.

The Department will evaluate the PIMS Closeout Plan documentation from the selected Offeror. Upon acceptance, the Department will prepare an acceptance letter addressed to the selected Offeror indicating that the module was accepted as fully operational.

The acceptance criteria include:

- Deliverables and documentation that have been submitted and accepted by the Department.
- No critical or significant defects are open.
- No change orders identified as required for CMS certification are open.

The IV&V Contractor will prepare a post-implementation assessment and problem resolution report. The report will include identification of all problems and corresponding resolutions found during the implementation; any operational items that could be impacted; and recommendations on improving the rollout process until the final report (after final certification of all modules). Within ten (10) business days after the IV&V Contractor issues the Post-Implementation Assessment after each implementation, the selected Offeror must submit an Issue Resolution Plan identifying a resolution plan for any items that are contained in the IV&V Contractor's Post-Implementation Assessment Report. The Closeout Plan will be reviewed monthly as part of the Monthly Status Report (see **Section I–8.C Reports and Program Control** of this RFP).

The selected Offeror must review the Post-Implementation Assessment report and develop issue resolution plans, and strategies and recommendations for future rollouts to prevent recurrences as they relate to the PIMS Module.

Deliverables:
1. PIMS Closeout Plan
2. Issue resolution plan resulting from the Post-Implementation Assessment report
3. Written certification from the selected Offeror

The Offeror must describe its approach to the design, development, implementation, and maintenance of the PIMS Closeout Plan.

M. PIMS Maintenance and Operations Plan. The selected Offeror must design, develop, implement, and maintain the PIMS M&O Plan. The selected Offeror will deliver the initial PIMS M&O Plan thirty-three (33) business days before the implementation of the PIMS Module and will review monthly thereafter. The objective of the M&O phase of SDLC is to stabilize and maintain the deployed solution. The selected Offeror must provide operational and maintenance support of the selected Offeror's solution, including any customer service support and system/product/application upgrades such as operational performance metrics and performance standards service, as needed.

During M&O, the selected Offeror must monitor the day-to-day PIMS Module operations.

At a minimum, the selected Offeror must:

1. Maintain current versions and licenses for all software, hardware, or other infrastructure.
2. Maintain backwards compatible versions of software.
3. Perform necessary upgrades to COTS products and components, if applicable.
4. Perform routine preventative maintenance.
5. Collaborate with the ITC/QA Contractor, SI/DH Contractor, other MMIS 2020 Platform module contractors, and the Department to create a standard schedule for maintenance activities.
6. Provide support for production both during and outside of the Department's business hours, and coordinate with the Department for the level of expected support (e.g. what communication methods will be used outside of normal business hours and the expected response time).
7. Collaborate with other MMIS 2020 Platform contractors to perform defect triage, determining the severity of defects, responsibility, and resolution timeline.
8. Initiate work order to change or enhance the PIMS Module.

Deliverable: PIMS Maintenance and Operations Plan

The Offeror must describe its approach to the design, development, implementation, and maintenance of the PIMS Maintenance and Operations Plan.

N. PIMS Technical Infrastructure Document. The selected Offeror must design, develop, implement, and maintain a Technical Infrastructure Document that describes all the hardware, system software, and tools necessary for each of the environments proposed, which includes:

1. A comprehensive system assets inventory (hardware, software, services, processes, configuration, etc.) preferably maintained and managed through a centralized Configuration Management Database ("CMDB") developed and hosted by the SI/DH Contractor.

2. A detailed product currency and license inventory, preferably maintained and managed through a centralized CMDB, including:
   a) List of all software licenses, current installations version, latest version (for each particular product), and next target installation version such as upgraded Oracle to 11.2.0.4 version although the latest version is 12.c,
   b) Software end-of-life; and,
   c) Software end-of-support.

3. Network connectivity diagrams, including:
   a) Entire network diagram representing physical and logical links between nodes including servers, load balancers, and firewalls, and,

b) Secure boundary representation diagrams.

4. Network configuration inventory, preferably maintained and managed through a centralized CMDB, including:
   a) IP management (subnets, Virtual Local Area Networks ("VLANs"), IP assignment inventory, etc.);
   b) Network ports in use;
   c) Network protocols in use;
   d) Secure tunnels; and,
   e) Certificates.

5. Data flow diagrams, including:
   a) Node to node traffic (from data source to data destination), including all data repositories and pass-through systems involved; and,
   b) Between various logical elements of a particular unique solution or application (e.g. link between front-end and back-end elements).

6. Approach to capacity planning.

The selected Offeror must submit the PIMS Technical Infrastructure Document to the Department for approval one hundred (100) business days after the purchase order effective date and must update it weekly thereafter.

Deliverable: PIMS Technical Infrastructure Document

The Offeror must describe its approach to the design, development, implementation, and maintenance of the PIMS Technical Infrastructure Document.

O. PIMS System Design Document. The selected Offeror must design, develop, implement, and maintain the PIMS System Design Document ("SDD"). A SDD is not necessary for COTS products, but an interface design document (including APIs) is required. The PIMS SDD must include:

1. A list of all local and off-site facilities.
2. A network schematic showing all network components and technical security controls.
3. A description of each component, including basic functions and the business areas supported.
4. An enterprise system diagram, including all components, identifying all logic flow, data flow, systems functions, and their associated data storage.
5. A bi-directional traceability to requirements and test plan.

The selected Offeror must submit the PIMS SDD to the Department eighty (80) business days after the purchase order effective date and update the plan within eleven (11) business days after the GSD is approved by the Department for each MMIS 2020 Platform module.

Deliverable: PIMS System Design Document

The Offeror must describe its approach to the design, development, implementation, and maintenance of the PIMS System Design Document.

P. PIMS Turnover Plan. Turnover is defined as those activities that the selected Offeror must perform at the end of the contract term, to turnover service delivery to a successor Offeror or to Commonwealth resources. During the turnover period, the selected Offeror must actively and cooperatively participate with the Department and its

incoming contractor, if any. Offerors must submit a draft outgoing turnover plan with its Lot 1 Technical Submittal. The Offeror awarded a contract under Lot 1 of this RFP must provide the Department Contract Administrator and incoming contractor with all data, content, files, instructions, processe**s,** and all other items deemed appropriate by DHS to successfully transition services and work effort. The selected Offeror must provide data in a format that is considered an industry-standard and approved by the Department Contract Administrator or designee.

The outgoing turnover plan must include at a minimum:

1. Data turnover tasks;
2. Custom interface turnover tasks;
3. Reusable code turnover tasks;
4. Documentation regarding files, interfaces, and work flows not considered to be part of the COTS proprietary documentation tasks; and,
5. A timeline with milestones for the PIMS Turnover to include planning, execution, and implementation approval.

Additionally, the selected Offeror must develop an outgoing turnover plan when requested by the Department Contract Administrator or designee. The outgoing transition plan must be reviewed and approved by the DHS MMIS 2020 Project Administrator and stakeholders. Once approved by the DHS MMIS 2020 Project Administrator, the selected Offeror must complete all activities included in the outgoing turnover plan within nine (9) months.

Deliverable: PIMS Turnover Plan

The Offeror must describe its approach to the design, development, implementation, and maintenance of the PIMS Turnover Plan.

I-7. Requirements

A. Disaster Recovery ("DR"). The selected Offeror must develop and document a DR plan for approval by the Commonwealth that integrates with the Commonwealth's enterprise DR standards and timing objectives for electronic records and files relating to the PIMS Module. The DR plan must comply with the following standards:

1. 24-hour Recovery Point Objective.
2. 36-hour Recovery Time Objective.
3. Encryption for data at rest.

In addition, the selected Offeror must:

1. Participate in and provide support for Commonwealth-led DR testing. In the event of a failed test, the selected Offeror must submit a Corrective Action Plan ("CAP") for review and approval. Once approved, the selected Offeror must retest the DR plan utilizing the approved CAP.
2. Review and test the DR Plan six (6) months after the purchase order effective date and every six (6) months thereafter and provide the results to the Commonwealth.
3. Restore the PIMS Module in the event of a system-wide outage, provide technical assistance to restore the MMIS 2020 Platform based on the Department's prioritized order of module restoration.

The DR plan must include at a minimum:

1. A procedure to return to limited twenty-five percent (25%) operation within twenty-four (24) hours of the DR event.
2. The ability to return to full operation within three (3) calendar days of the DR event.
3. A plan to confirm that the post-disaster software version is the same as before the disaster.
4. A procedure to confirm that pre-disaster data is not lost or corrupted.
5. A complete backup of all non-software data sets at the end of each production business day.
    a. The selected Offeror's datacenter architecture must consist of multiple geographically disbursed datacenters. Any datacenters being used in a back-up function must be at least fifty (50) miles apart from the associated primary location for the service. The selected Offeror must list the address of all datacenter locations from which the selected Offeror will provide the services. The plan must identify the backup sites.
    b. If the resultant backup media (for example, tapes and disks) are utilized, they must be removed to an external secure site. Back-up media must be cycled on a weekly basis.
    c. Upon the installation of any software (new or upgraded), a complete backup (copy) of the software must be made with the resultant backup media removed to an external secure site.
6. Servers must be designed to employ a method of redundancy for operational integrity and production.
7. All workstations attached to the network must have sufficient processing capability to be used interchangeably and must backup one another until repair or replacement can be affected.
8. The selected Offeror must utilize appropriate methods to achieve datacenter sustainability, such as realizing a low Power Usage Effectiveness ratio.
9. Servers must be connected to an Uninterrupted Power Supply system, which will condition incoming power to the server and provide sufficient processing time for the server to be correctly shutdown in the event of a power failure.
10. In the event of damage of a sufficient magnitude to the primary operational site, a second company location must be modified to accommodate the system.
11. The DR plan must include a description of the chain of communication and command, by level, in the case of a systems or power failure.
12. The selected Offeror must have a Business Continuity Plan to maintain business operations via a semi-automated or manual mode to mitigate complete disruption of services until systems have been restored to normal operating capacities.
13. In a datacenter environment that hosts both Commonwealth and non-Commonwealth clients, the selected Offeror must provide segregation of Commonwealth data and computing resources from other clients' data and computing resources. The selected Offeror is required to provide system and data segregation between different agency application environments.
14. Each datacenter must have the capability to provide DR for other datacenters for identified critical applications.

Deliverable: PIMS DR Plan

The selected Offeror must deliver the DR Plan forty-three (43) business days prior to the PIMS Module implementation and must update annually. The DR Plan will be reviewed with the monthly status report – see **Section I-8.C** of this RFP.

The Offeror must describe how, by whom, and when its DR plan will be tested. The Offeror must describe how its DR test plans support compliance with the required system availability as described in **Section I-9. Performance Standards** of this RFP. The Offeror must also describe its approach to backing up the infrastructure to provide for continuity of operations.

B. Emergency Preparedness. To support continuity of operations during an emergency, including a pandemic or an event that causes major disruption in business or system operations, the Commonwealth needs a strategy for maintaining operations for an extended period of time. The selected Offeror's Continuity Of Operations Plan ("COOP") must align with the DHS's. The strategy ensures that essential contractors that provide critical business services to the Commonwealth have planned for such an emergency and put contingencies in place to provide needed goods and services.

1. Describe how you anticipate such a crisis will impact your operations.
2. Describe your emergency response COOP. Attach a copy of your plan, or at a minimum, summarize how your plan addresses the following aspects of preparedness:
   a. Employee training (describe your organization's training plan, and how frequently your plan will be shared with employees).
   b. Identification of essential business functions and key employees within your organization necessary to carry them out.
   c. Contingency plans for:
      i. How your organization will handle staffing issues when a portion of key employees are incapacitated.
      ii. How employees in your organization will carry out the essential functions if crisis control measures prevent them from coming to the primary workplace.
   d. How your organization will communicate with staff and suppliers when primary communications systems are overloaded or otherwise fail, including key contacts and chain of communications (including suppliers).
   e. How and when your emergency plan will be tested, and if the plan will be tested by a third-party. Include a plan for corrective actions should the testing fail.

Deliverable: PIMS COOP

The selected Offeror must deliver the PIMS COOP forty-three (43) business days prior to the PIMS Module implementation and must update the Plan annually.

C. Records Management. The selected Offeror must comply with records management requirements as defined in Management Directive 210.5 available at: http://www.oa.pa.gov/Policies/md/Pages/Management_AdministrativeSupport(205-260).aspx.

The selected Offeror will retain records until a time the Department determines that they qualify for disposition.

The Offeror must describe its approach to Records Management.

D. PIMS Module Requirements Categories. Detailed requirements have been organized into three (3) categories: General, Technical, and Functional. The selected Offeror's proposed solution must demonstrate its alignment with the PIMS Module detailed requirements. Offerors must respond to each individual requirement.

The requirements listed below are for the PIMS Module. Under the Departments strategic guidance, the ITC/QA Contractor will lead requirements gathering related meetings including JAD sessions in collaboration with the selected Offeror, the SI/DH Contractor and other appropriate MMIS 2020 Platform module contractors to finalize the PIMS Module requirements. The results of the requirements collection will be

consolidated into a BRD, and the requirements in the BRD will be cross walked to the CMS certification checklist and the PIMS Module's RFP requirements.

The ITC/QA Contractor will complete a Business Gap Analysis to ensure the business requirements meet or exceed what is required for CMS certification, CMS and State regulations, and the Department's desired functionality. Offerors may propose additional requirements for consideration to achieve CMS certification.

E. General Requirements. The selected Offeror must meet the following general requirements for the PIMS Module:

1. Provide a package of fully functional business processes that support the MMIS 2020 Platform requirements.
2. Provide a module for PIMS that is independent and separate from other MMIS 2020 Platform modules or external solutions with the exception of shared data.
3. Provide a module that meets all CMS Medicaid Enterprise Certification Toolkit ("MECT") checklist requirements related to the PIMS Module and that will achieve CMS certification.
4. Implement and operate, in the United States, your modular solution through software, data, and interoperable interfaces.
5. Provide, maintain, and host the necessary databases to run the COTS package, custom product, or SaaS for the module.
6. Provide a product base of standard reports to operate, control, manage, and monitor the operations of the module's business processes.
7. Provide for customization of reports included in the module and additional reports defined by the Department to meet critical business needs.
8. Provide the capability for users to produce ad hoc reports based on the data processed and generated by the module.
9. Provide a configurable automated rules engine in the module for defining processing.
10. Maintain code lists and reference files needed only by the selected Offeror's application. Data used by multiple modules will be housed in the ODS.
11. Maintain the code to its module and provide release updates that contain enhancements to the software. When practical, coordinate module enhancements through software updates with other states licensed to use its module.
12. Provide and maintain claim and encounter testing capabilities to be used for systems changes and system verification including complete adjudication cycle and test reports.
13. Design, develop, implement and maintain the capability for providers to test within the module's test environment, and support testing of new claims submission systems by allowing users to submit electronic claims test files that are processed through the adjudication cycle without impact on system data.
14. Collaborate with the SI/DH Contractor, other module contractors, IV&V Contractor, ITC/QA Contractor, and the Commonwealth to ensure MMIS 2020 Platform success.
15. Collaborate with the SI/DH and module contractors to develop a module that accommodates phased-in PIMS services consistent with the Department's overall MMIS 2020 Platform implementation plan.
16. Achieve and maintain HIPAA and CMS compliance in the PIMS Module.
17. Host a minimum of ten (10) years of PIMS data converted from the legacy system via the SI/DH.

18. Collaborate with the SI/DH Contractor, other module contractors, IV&V Contractor, ITC/QA Contractor and the Department to complete data conversion for the PIMS Module from the Legacy system.

The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.FR.7, OM.CL4.37, OM.CL1.15, TA.FR.8, IA.DMS.5, and S&C.MS.14.

F. Technical Requirements. The selected Offeror must meet the following technical requirements for the PIMS Module. These requirements are necessary to provide for interoperability using the DH and related technology. CMS supplied MECT Version 2.3. The MECT checklist requirements support MMIS 2020 Platform certification processes and can be accessed at https://www.medicaid.gov/medicaid/data-and-systems/mect/index.html. The corresponding MECT 2.3 Checklist requirement numbers have been included as applicable. Not all requirements will have an identified PIMS-specific MECT 2.3 checklist requirement.

1. The selected Offeror must utilize the guidance provided in the CMS's Minimum Acceptable Risk Standards for Exchanges, Version 2.0, and is responsible for providing a solution that meets all industry, state, and federal security standards. The selected Offeror must maintain, and make available at any time, security policies and procedures for each contractor and subcontractor module and location. At a minimum, the selected Offeror must provide for the security of the PIMS Module in compliance with the following federal regulations and publications:

    a. 45 CFR § 95.621(f) ADP System Security Requirements and Review Process;
    b. Standards defined in Federal Information Processing Standards ("FIPS") issued by the National Institute of Standards and Technology ("NIST");
    c. NIST Special Publication 800-111 Storage Encryption Technologies for End User Devices;
    d. NIST Cryptographic Module Validation Program (http://csrc.nist.gov/groups/STM/cmvp/validation.html);
    e. FIPS PUB 112 Password Usage Procedure;
    f. FIPS PUB 186-4 Digital Signature Standard, Published July 2013;
    g. 5 U.S.C. § 552a(o)(1)(F), (H) and (I) Records maintained on individuals;
    h. IRS Pub 1075;
    i. Privacy Act of 1974 at 5 U.S.C. 552a;
    j. Computer Matching and Privacy Protection Act of 1988 ("CMPPA");
    k. Federal Information Security Modernization Act ("FISMA");
    l. SSA Information System Security Guidelines for Federal, State, and Local Agencies;
    m. Child Online Privacy Protection Act;
    n. Title XIX Confidentiality Rules;
    o. HIPAA;
    p. Administrative Simplification (HIPAA and ACA), including transactions and code sets, privacy, and security provisions;
    q. Federal security and privacy standards adopted by the DHHS Services for Exchanges;
    r. NIST 800-53 Assessing Security and Privacy Controls in Federal Information Systems and Organizations;
    s. Public Law 114-255 21st Century Cures Act Section 5006;
    t. Title XXI of the SSA;
    u. HITECH; and
    v. CFR Title 45 Part 164 Security and Privacy.

The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.13, TA.SP.15, TA.SP.18, TA.SP.27 TA.SP.28, TA.SP.3, TA.SP.37, TA.SP.38, TA.SP.42, TA.SP.53, TA.SP.57, TA.SP.58, TA.SP.74, TA.SP.75, TA.SP.76, and TA.SP.77.

2. The selected Offeror must comply with all applicable Department and OIT security policies, including the following:

    a. Department security policies and standards: http://www.dhs.pa.gov/provider/busandtechstandards/secdomain/index.htm
    b. Department privacy policies and standards: http://www.dhs.pa.gov/provider/busandtechstandards/privdomain/index.htm
    c. Commonwealth Security ITPs: http://www.oa.pa.gov/Policies/Pages/itp.aspx
        i. ITP_SEC031- Encryption Standards for Data in Transit;
        ii. ITP_SEC020- Encryption Standards for Data at Rest;
        iii. ITP_SEC016- Commonwealth of Pennsylvania – Information Security Officer Policy;
        iv. ITP_SEC014- Identity Protection and Access Management (IPAM) Architectural Standard – Identity Management Technology Standards;
        v. ITP_SEC013- Identity Protection and Access Management (IPAM) Architectural – Identity Management Services;
        vi. ITP-SEC-007- Minimum Standards for IDs and Passwords; and
        vii. Department encryption policies and standards: http://www.dhs.pa.gov/cs/groups/webcontent/documents/communication/p_031963.pdf

    The corresponding CMS MECT 2.3 Checklist requirement number is TA.SP.38.

3. The selected Offeror must adhere to all pertinent federal security mandates, regulations, and standards including, the following:

    a. 18 U.S.C. § 641: Public Money, Property or Records;
    b. 18 U.S.C. § 1905: Disclosure of Confidential Information;
    c. 21 CFR Parts 1-1499: Food and Drugs;
    d. 42 CFR Subchapter C: Medical Assistance Programs
    e. 42 CFR Subpart F: Safeguarding Information on Applicants and Beneficiaries
    f. 45 CFR Parts 160, 162.1301 and 164: Standards for Privacy of Individually Identifiable Health Information;
    g. American Recovery and Reinvestment Act of 2009 (“ARRA”);
    h. Emergency Medical Treatment & Labor Act;
    i. Freedom of Information Act (“FOIA”);
    j. OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems;
    k. The Deficit Reduction Act of 2005 Fact Sheet;
    l. The Patient Protection and Affordable Care Act of 2010 (“ACA”); and
    m. The Sarbanes-Oxley Act of 2002; and ISO 27001 and ISO 27002

    The corresponding CMS MECT 2.3 Checklist requirement numbers are S&C.ISC.6 and PL.RDM1.3.

4. The selected Offeror must implement a security architecture aligned with current MITA Security and Privacy model and other applicable architecture documents. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SOA.1, and TA.DAM.2

5. The selected Offeror's services and infrastructure must adhere to best practices and to Web Services ("WS") security specifications and standards, as appropriate, including:

    a. Messaging
        i. Confidentiality & Integrity: WS-Security, SSL/TLS, XML Encryption;
        ii. Authentication: WS-Security Tokens, SSL/TLS X.509 Certificates, XML Signature;
    b. Resource
        i. Authorization: Extensible Access Control Markup Language ("XACML"), extensible Rights Markup Language, Role Based Access Control, Attribute Based Access Control;
        ii. Privacy: Enterprise Privacy Authorization Language, XACML;
    c. Trust
        i. Establishment: WS-Trust, XML Key Management, X.509;
        ii. Trust Proxying: Security Assertion Markup Language, WS-Trust; Federation: WS-Federation, Shibboleth;
    d. Security Properties
        i. Policy: WS-Policy; Security Policy: WS-Security Policy; and
        ii. Availability: WS-Reliability Messaging, WS-Reliability.

    The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.BPM.4 and TA.DC.9.

6. The selected Offeror must provide for the effective integration of modular solutions, including COTS products, without requiring MMIS 2020 Platform contractors to make significant modifications to the inherent capabilities of their modules, including business rules engine and workflow. If a COTS product does not provide a required function and a Department standard product preference exists, the selected Offeror must utilize the Department's solutions, standards or both. The corresponding CMS MECT 2.3 Checklist requirement number is TA.DAM.3.

7. The selected Offeror must adhere to Atomicity, Consistency, Isolation, and Durability ("ACID") for the handling of transaction rollbacks, validity, and referential integrity checks,. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

8. The selected Offeror must support secure single sign-on**,** roles-based access by integrating with the Department's Identity and Access Management ("IDAM") Single Sign-on solution, CA SiteMinder. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.11, TA.SP.22, TA.SP.5, TA.SP.50, and TA.SP.51.

9. The selected Offeror must leverage the security roles defined by the Department. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

10. The selected Offeror must support access and role changes in real-time. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

11. The selected Offeror must provide a solution that is configurable to add users to multiple user groups. If conflicting access levels occur due to a user being in multiple user groups, the lowest access level will take precedence for a particular action. The corresponding CMS MECT 2.3 Checklist requirement number is TA.SP.51.

12. The selected Offeror must support the unique authentication credentials for each user gaining access to the system and must not support "group" or "corporate" logins. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

13. The selected Offeror must provide the ability for a user to manually initiate a secure logout of the system from the external-facing portal. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

14. The selected Offeror must support fine-grained access control (e.g. field-level) based on a user's role and privileges. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

15. The selected Offeror must provide the ability to define and implement fine-grained exclusion controls on a per-user basis. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

16. The selected Offeror will grant access to and from the DH using a unique user identifier (user ID) and user profile, combined with a strong password - following the Departments IDAM policy. The selected Offeror must be able to trace and audit any transaction or change to data by the module, down to the user ID level. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.24, TA.SP.70, IA.DS.18, and S&C.MS.4.

17. The selected Offeror must create, delete, modify, and assign role-based security to grant view and modify access to individual windows, reports, data elements, and field levels. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.BI.9, TA.SP.11, TA.SP.25, TA.SP.26, TA.SP.32, and TA.SP.50.

18. The selected Offeror must provide the capability to permit or restrict access to sensitive documents, generated forms, and other content based on a user's assigned security roles. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.BI.9, TA.SP.22, TA.SP.25, and TA.SP.32.

19. The selected Offeror must support authentication mechanisms for batch or web-based interfaces for data exchange with the federal government and other business partners. The corresponding CMS MECT 2.3 Checklist requirement number is S&C.IC.6.

20. The selected Offeror must accommodate secure communications between Commonwealth business partners and the Commonwealth via multiple communication methods including email, text, and web portal, as defined by the Commonwealth. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.DC.10 and S&C.BRC.5.

21. The selected Offeror must maintain policies and procedures for Commonwealth-mandated background checks and staffing controls, allowing the selected Offeror's personnel access to Commonwealth-owned confidential information and to restricted areas within the selected Offeror's host environment. Background checks are to be conducted annually and at the expense of the selected Offeror. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

22. The selected Offeror must provide audit logs as requested by the Department in a best of practice format or made compatible for integration to an advanced log correlator. The corresponding CMS MECT 2.3 Checklist requirement number is IA.DS.18.

23. The selected Offeror must maintain a separate audit trail file for all transactions processed by the system, in a format that is logical and meaningful. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.39, IA.DS.18, and TA.LG.1.

24. The selected Offeror must capture root information on all changes to critical records and data fields specific to the PIMS Module, and send this information to the ODS, including identification of the responsible system user and date and time of the change. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.27, TA.SP.37, and TA.SP.39.

25. The selected Offeror must have security audit trail reporting capabilities for a variety of criteria (e.g., security, level, locale, IP address, user ID, modification made, and date/time). The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.37, TA.SP.39, and IA.DS.18.

26. The selected Offeror must utilize automated utilities to review an appropriate subset of audit logs of system activity at least once weekly for unusual, unexpected, or suspicious behavior. The selected Offeror will inspect administrator groups on demand, and at least once every fourteen (14) calendar days, to detect the creation of any unauthorized administrator accounts. The selected Offeror will conduct manual reviews of system audit randomly on demand and must conduct at least once every thirty (30) calendar days. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.18 and TA.LG.1.

27. The selected Offeror must audit user login habits, restrict access, and notify the Department when anomalies are detected. The selected Offeror will produce reports of detected anomalies. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.38 and TA.SP.52.

28. The selected Offeror must generate and maintain audit logging that records user and system access to data to the data level. In addition, the selected Offeror must meet the audit log requirements mandated by all pertinent Department, Commonwealth, and federal guidelines, policies, and standards. The corresponding CMS MECT 2.3 Checklist requirement number is IA.DS.18.

29. The selected Offeror must commission annual third-party auditing of the PIMS Module, including the SSAE 18 SOC 1 report audit, and provide a copy of all audits, including dates they were conducted; to the Department. Audits must be conducted by an independent, third-party auditor. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.18 and IA.DS.18.

30. The selected Offeror must adhere to security and audit controls applying to storage, backup, retrieval, and viewing of archive data records including:

    a. Secure and encrypted storage;
    b. Encrypted backups; and
    c. Audit trails.

    The corresponding CMS MECT 2.3 Checklist requirement number is IA.DS.18.

31. The selected Offeror must support file-based encryption of flat or XML files received from external entities. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.BPM.4 and TA.DC.9.

32. The selected Offeror must support audit controls for hardware, software, and procedural mechanisms that record and examine activity in information systems that contain or use electronic Protected Health Information. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.10, TA.SP.18, TA.SP.36, TA.SP.43, TA.SP.44, TA.SP.7, and TA.SP.9.

33. The selected Offeror must provide for the configurable ability to encrypt both data at rest and data in motion. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.34 and TA.SP.72.

34. The selected Offeror must require message-level encryption (signed, encrypted messages) between system tier boundaries to mitigate against the risk of any one tier being compromised by malicious intent. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.34, TA.SP.41, and TA.SP.6.

35. The selected Offeror must provide transport-level encryption of data submitted from client to server devices using Secure Sockets Layer encryption over HyperText Transfer Protocol (“HTTP”). The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.14, TA.SP.35, TA.SP.6, TA.SP.7, TA.SP.70, and TA.SP.72.

36. The selected Offeror must provide encryption capabilities to secure stored, sensitive data (including PII and PHI). The encryption mechanisms will be determined based on the CMS requirements and standards. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.33 and TA.SP.5.

37. The selected Offeror must provide for database-level encryption at multiple levels (e.g., instance, tablespace, table and column). No PIMS-specific MECT 2.3 Checklist requirement has been identified.

38. The selected Offeror must provide a reusable architecture service for the encryption and decryption of application-shared secrets/keys. Encryption keys are a shared exchange, meaning both sides would share the key in order to handle the communication and reusable architecture service. The encryption keys will not be shared outside the scope of MMIS 2020 Platform. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

39. The selected Offeror must provide security warning banners, headers and footers, adhering to federal, state and other applicable standards that are prominently displayed on all screens and reports, and must be readily customizable by Department staff. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

40. The selected Offeror must provide the ability to apply format masks to sensitive data that is displayed on the screen (e.g., PHI, SSN). The corresponding CMS MECT 2.3 Checklist requirement number is TA.SP.14.

41. The selected Offeror will utilize a 2(+)-tier architecture with SOA, Web 2.0, XML capabilities, and Simple Object Access Protocol ("SOAP") and RESTful web services. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.BPM.4, TA.DC.9, and TA.SE.2.

42. The selected Offeror must store the information pertaining to the services available at particular endpoints in a machine-readable format in the service registry. The information must include the location of the service, routing information, failover protocols, and load balancing protocols in the service registry. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

43. The selected Offeror must provide the capability for a high volume of online and batch functions to run concurrently. The selected Offeror will coordinate module availabilities with the SI/DH for batch processes with prerequisites and dependencies from several disparate systems and schedulers. Dependencies may include:

    a. Time of calendar day;
    b. Use of system; and
    c. Contingent timing of batches.

No PIMS-specific MECT 2.3 Checklist requirement has been identified.

44. The selected Offeror must provide on-demand reporting on the status of batch processes. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

45. The selected Offeror must assist the Department in establishing technical standards and governance for the MMIS 2020 Platform to align technical integration among disparate systems, as needed. This includes supplying technical data, providing access to engineering expertise, and operating a test bed against which teams can test and resolve integration issues. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

46. The selected Offeror's solution must support the ability to load data and quality check data in a variety of approaches including the following:

    a. Bulk data extraction across selection criteria and loading across multiple output formats;
    b. Granular trickle-feed acquisition and delivery;
    c. Changed-data capture (ability to identify and extract modified data); and
    d. Event-based acquisition (time-based or data-value-based).

    No PIMS-specific MECT 2.3 Checklist requirement has been identified.

47. In collaboration with the ITC/QA Contractor, SI/DH Contractor, and MMIS 2020 Platform module contractors, the selected Offeror must conduct testing as systems and data are integrated into the SOA utilizing the ESB. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

48. The selected Offeror must coordinate with the SI/DH Contractor and ITC/QA Contractor to support testing across the MMIS 2020 Platform with regard to integration points between other modules and contractor-supported enterprise components. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

49. The selected Offeror must collaborate with the Department, the SI/DH Contractor, and the ITC/QA Contractor to plan inter-system testing across the MMIS 2020 Platform to include documenting objectives, entrance criteria, scheduling, testing strategy, test procedures, resource identification, and exit criteria. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

50. The selected Offeror must coordinate with the Department, the SI/DH Contractor, the ITC/QA Contractor to participate in the execution of inter-project testing, including setup of shared resources, setup of instrumentation, conduct of the test, and documentation of anomalies. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

51. The selected Offeror must use the automated tools to support PIMS Module testing. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

52. The selected Offeror must provide a development environment, a testing environment, and a training environment. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

53. The selected Offeror must coordinate with the SI/DH Contractor to achieve integration into the MMIS 2020 Platform. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

54. The selected Offeror must assist the Department in establishing the timing of cross-project "touch points," project-to-project timing dependencies, and other MMIS 2020 Platform Project milestones. This includes the communication and coordination of inbound and outbound data that flows through the solution. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

55. The selected Offeror must supply the ITC/QA Contractor all data conversion mapping for posting to the Artifact Library. The corresponding CMS MECT 2.3 Checklist requirement number is TA.DAM.3.

56. The selected Offeror must maintain the appropriate metadata of any data transmittion into the system and be able to identify originating system (data owner) and data format. The corresponding CMS MECT 2.3 Checklist requirement number is IA.DMS.2.

57. The selected Offeror must provide full, incremental, and transaction log backup and recovery capabilities on both a regular schedule and an ad-hoc basis, including:

    a. Redundant incremental off-site backups; and
    b. Regularly scheduled demonstrations of back-up and restore capabilities.

    No PIMS-specific MECT 2.3 Checklist requirement has been identified.

58. The selected Offeror must store logs in a location that is accessible by both the selected Offeror and authorized Department staff. The retention period of transaction logs must be in accordance with federal, Commonwealth, and Department standards. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

59. The selected Offeror must align the solution with the planned modularity and configurability of the MMIS 2020 Platform, providing flexibility for application components that utilize web services to allow seamless and flexible communication between components, and to support the removal of solutions and transfer of data as business needs evolve to plug-and-play into the SI/DH. The corresponding CMS MECT 2.3 Checklist requirement number is IA.DS.10.

60. The selected Offeror will collaborate with the Department, ITC/QA Contractor, and the SI/DH Contractor to design, develop, implement, and maintain the technical integrations and APIs used in the MMIS 2020 Platform Project. The corresponding CMS MECT 2.3 Checklist requirement number is TA.CM.4.

61. The selected Offeror must utilize Extensible Markup Language ("XML"), World Wide Web Consortium (" W3C") standards in the ESB message format, whenever possible, and must convert message formats and translate coded data within messages. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.BPM.4 and TA.DC.9.

62. The selected Offeror must leverage workflow and ESB orchestration to optimize data-related processes in the event-driven environment. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SOA.1 and TA.LG.2.

63. The selected Offeror must provide highly reusable parameterized web services, requiring minimal or no customization that will enhance the ability to:

    a. Rapidly deploy applications; and
    b. Integrate legacy applications.

    No PIMS-specific MECT 2.3 Checklist requirement has been identified.

64. The selected Offeror's solution must support the required inbound and outbound interfaces for the module either through the SI/DH or for direct, point-to-point interfaces between trading partners. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

65. The selected Offeror must provide that all inbound and outbound interfaces comply, as necessary, with National Information Exchange Model, NIST, HIPAA-compliant standards, and other applicable standards. The corresponding CMS MECT 2.3 Checklist requirement number is TA.DAM.2.

66. The selected Offeror's solution must support uninterrupted functionality during database backup windows (e.g., hot backup or dynamic backup). No PIMS-specific MECT 2.3 Checklist requirement has been identified.

67. The selected Offeror must provide the ability for concurrent users to simultaneously view the same record, documentation and template via the web interface. No PIMS-specific MECT 2.3 checklist requirement has been identified.

68. The selected Offeror's solution must allow reference data to be viewed, loaded, and edited by the authorized Department uses No PIMS-specific MECT 2.3 Checklist requirement has been identified.

69. The selected Offeror must utilize a configuration such that changes to modular data must remain in synchronization with the ODS. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

70. The selected Offeror must collaborate with the Commonwealth and across modules to establish the data architecture and processes for data management of the ODS. The corresponding CMS MECT 2.3 Checklist requirement numbers is IA.DMS.4.

71. The selected Offeror must reconcile all data elements found in the ODS. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

72. The selected Offeror must leverage all common code values maintained by the SI/DH Contractor. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

73. The selected Offeror must utilize standard industry code sets, using only the most current versions of these code sets or as approved by the Department. The corresponding CMS MECT 2.3 Checklist requirement number is S&C.IC.2.

74. The selected Offeror must support at least the following types of transformation:

    a. Simple transformations such as data-type conversions, string manipulations, and simple calculations;
    b. Moderate-complexity transformations, such as lookup and replace operations, aggregations, summarizations, deterministic matching, and management of slowly changing dimensions;
    c. Higher-order transformations, such as sophisticated parsing operations on free-form text and rich media facilities for developing custom transformations and extending packaged transformations; and,
    d. Facilities for developing custom transformations and extending packaged transformations.

    No PIMS-specific MECT 2.3 Checklist requirement has been identified.

75. The selected Offeror must utilize a Relational Database Management System to support OLTP, batch processing, mixed workloads, and business intelligence. The corresponding CMS MECT 2.3 Checklist requirement number is TA.BI.7.

76. The selected Offeror must provide advanced configurations for data caching, including support of client/application caching and support of server caching. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

77. The selected Offeror must provide the ability to function on a real-time basis. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

78. The selected Offeror must provide a normalized core data model or data object model, making proper use of primary, foreign keys, indexes, constraints and domain-based data types. The corresponding CMS MECT 2.3 Checklist requirement number is IA.LDM.5.

79. The selected Offeror must utilize Entity Relationship/Object Modeling Integration in order to synchronize logical, physical, and object models. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

80. The selected Offeror must provide built-in utilities to the Database Management Solution ("DBMS") to automate the normal day-to-day database administrator operations (e.g., automated index rebuilding, free space reclamation, and block reorganization). No PIMS-specific MECT 2.3 Checklist requirement has been identified.

81. The selected Offeror must support native geospatial data types. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

82. The selected Offeror must support various database connectivity protocols (e.g., Open Database Connectivity, Java Database Connectivity,and Object Linking and Embedding database protocol). No PIMS-specific MECT 2.3 Checklist requirement has been identified.

83. The selected Offeror must provide an underlying DBMS, so it is also available as a standalone query-able DBMS. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

84. The selected Offeror's solution must preserve committed transactions in a manner that ensure no greater than one (1) minute of committed transaction data is lost as the result of an unplanned interruption to services or a reduction in the quality of services. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

85. The selected Offeror must collaborate and contribute to project management activities, including status reporting, meetings, risk/issue management, and project planning as defined and managed by the ITC/QA Contractor and the Department. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

86. The selected Offeror must collaborate with the Department and the ITC/QA Contractor to manage the Change Management process. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

87. The selected Offeror must collaborate and contribute to release management and release planning activities (testing requirements, training impacts, promotion schedule) as defined and managed by the SI/DH Contractor, the ITC/QA Contractor and the Department. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

88. The selected Offeror must provide for the performance/latency of the connectivity to module system(s) such that the required performance (e.g., asynchronous and background messaging when a user action results in communications with other systems) is not adversely affected. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

89. The selected Offeror must establish processes to address future Commonwealth or federal regulations and requirements (e.g., Direct Secure Messaging for the exchange of PII and PHI between covered entities). The corresponding CMS MECT 2.3 Checklist requirement number is TA.SP.14.

90. The selected Offeror must send and accept batch and real-time representation of applicable HIPAA mandated and other standard health care transactions. The information exchanged will support a variety of formats, including X12, NCPDP, XML, and JSON formats. The corresponding CMS MECT 2.3 Checklist requirement numbers are IA.DS.11, IA.DS.5, TA.SP.16, and TA.SP.17.

91. The selected Offeror must support the ability for pre-generated performance standards related reports to be designed so that they can be rendered for online viewing in under five (5) seconds. The selected Offeror's solution must trigger an alert for performance outside of performance standards parameters and provide a link to the SLA-related reports online and accessible from a remote location. Additionally, performance data will be sent back to the SI/DH Contractor for inclusion in SI/DH MMIS 2020 Platform dashboards. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.BI.4, TA.FR.6, TA.PM.8, and TA.DC.7.

92. The selected Offeror must provide the ability to configure alerts, including:

    a. Alert thresholds;
    b. Alert notification channels; and
    c. Ability to turn alerts on or off for the module's performance standard monitoring capabilities.

    The corresponding CMS MECT 2.3 Checklist requirement number is TA.DC.7.

93. The selected Offeror must host the PIMS Module and meet the federal and Commonwealth standards (described in **Part I-9**) including required performance, security and data retention standards. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

94. The selected Offeror must provide a hosting solution that is sufficiently flexible in dealing with unavoidable circumstances, such as burst, cyclical, peak, and seasonal capacity demands or security and regulatory changes. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

95. The selected Offeror must provide a hosting environment for all system environments that is compliant with SSAE 16. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

96. The selected Offeror must utilize architecture with no single point of failure, supporting fault tolerance and failover of web, application, database servers, storage devices, and secondary devices such as load balancers, and supporting a high-availability enterprise. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

97. The selected Offeror must provide redundancy so that accessibility, reliability/fault tolerance, and performance are within defined performance standard parameters. No PIMS-specific MECT 2.3 checklist requirement has been identified.

98. The selected Offeror must enumerate the prioritized order of restoration for MMIS 2020 Platform modules in the event of a system-wide outage. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

99. The selected Offeror must sync planned outage windows to the greatest extent possible with all pertinent stakeholders and schedules that may affect or be affected by the MMIS 2020 Platform, including:

    a. the Commonwealth;
    b. Department maintenance schedule;
    c. MMIS 2020 Platform modules; and
    d. SI/DH Contractor.

    No PIMS-specific MECT 2.3 Checklist requirement has been identified.

100. The selected Offeror must communicate and coordinate with the Department in the event of an outage due to an emergency within fifteen (15) minutes of the identification of the outage. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

101. The selected Offeror must maintain proper power and cooling, including redundant power and cooling, to safeguard all hardware, software, and state-owned data. The corresponding CMS MECT 2.3 Checklist requirement number is TA.SP.61.

102. The selected Offeror must perform the following technical tasks, including:

a. Creating application server domains;
b. Deploying applications or components;
c. Monitoring and configuring the performance of the application server domain;
d. Diagnosing and troubleshooting problems;
e. Maintaining operating system to latest Department-approved version;
f. Maintaining current infrastructure documentation; and
g. Coordinating infrastructure changes with other contractors to minimize impact.

No PIMS-specific MECT 2.3 Checklist requirement has been identified.

103. The selected Offeror must support an orientation of business processes, business rules, data, and metadata management that allows a modular, componentized design approach that enhances interoperability across service modules and with external applications and data sources. The corresponding CMS MECT 2.3 Checklist requirement numbers are IA.DMS.2, IA.DS.9, and S&C.MS.2.

104. The selected Offeror must collaborate with MMIS 2020 Platform module contractors to maintain and synchronize all rules. If the PIMS Module has its own Business Rules Engine ("BRE"), the selected Offeror must export and support the load of these rules in the central location, on the SI/DH for the MMIS 2020 Platform. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.DM.1 and S&C.MS.10.

105. The selected Offeror must store PIMS Module specific rules in the PIMS Module for access by authorized user(s). The storage of business rules in the PIMS Module must support granular check-out and check-in rules and an audit trail of business rules changes. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

106. The selected Offeror must provide a rules engine which allows the rules to be tested against (de-identified) production data, such as claims/encounter processing in a non-production environment prior to deployment of the rules. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

107. The selected Offeror must provide the ability for the workflow engine to capture business processes using Business Process Model and Notation 2.0 or later, even if the engine uses a separate coding of the rules for execution. The corresponding CMS MECT 2.3 Checklist requirement number is S&C.MS.18.

108. The selected Offeror must streamline large sets of similarly structured rules with decision tables. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

109. The selected Offeror must provide for access to the most current rules during rule authoring and at execution time without recompiling code. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

110. The selected Offeror must provide the ability to rollback to prior versions of rules with minimal system impact. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

111. The selected Offeror must provide the ability for business rules to execute in a real time environment. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

112. The selected Offeror must provide the ability to maintain and display the history of each rule change in the rules engine. This history will show previous versions of the rule, a timestamp of when the change was made, a narrative box describing the change, and the identification of the user making the change. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

113. The selected Offeror must provide a rules editor that maintains the current version of standardized business rules' definitions in a language that business people can interpret and includes the ability to easily edit the rules. The module must transform the rules into system language for processing. The corresponding CMS MECT 2.3 Checklist requirement number is TA.DM.2.

114. The selected Offeror's informational technology solution must use production or inference rules to represent behaviors (e.g., IF THEN conditional logic). No PIMS-specific MECT 2.3 Checklist requirement has been identified.

115. The selected Offeror must be able to send work objects to other MMIS 2020 Platform modules via the DH, add received work objects to workflow queue, and return updates, including a closure of the work object back to the originating modules' workflow engine. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

116. The selected Offeror must support the saving of incomplete data sets for completion of the workflow at a later time. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

117. The selected Offeror must enable central workflow and transactional status alerts. The selected Offeror must centralize pending work items for the user in a "work queue." No PIMS-specific MECT 2.3 Checklist requirement has been identified.

118. The selected Offeror's solution must support the pushing of messages to intended workers without requiring them to specifically inquire for the data. The corresponding CMS MECT 2.3 Checklist requirement number is TA.SOA.2.

119. The selected Offeror's module windows and screens must be intuitive, easy to use, based on workflows, maintain the appropriate and relevant context, and offer multi-channel assistance. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.CS.10, TA.CS.14, and TA.CS.17.

120. The selected Offeror's module windows and screens must be compliant with Section 508 of the Rehabilitation Act of 1973 to meet the needs of diverse populations of users, including those with visual and hearing impairments, persons with low and moderate educational levels, and the elderly. Information on Section 508 can be accessed here: http://www.section508.gov. The corresponding CMS MECT 2.3 Checklist requirement number is TA.CS.18.

121. The selected Offeror must provide user experience personalization and customization capabilities for each user, including allowing users to specify precisely what they want. (e.g., choosing the information elements on a home page, choosing font size and display colors.) No PIMS-specific MECT 2.3 Checklist requirement has been identified.

122. The selected Offeror's solution must support the timeout of a user session after a specified period. The timeout period must be configurable by user type and module, minimally allowing different values for the public website and the internal website while meeting security rules. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.38, TA.SP.5, and TA.SP.54.

123. The selected Offeror's solution must support the ability of the website, wherever appropriate, to show progress via the use of Progress Bars. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

124. The selected Offeror must support session management capabilities to support user sessions and coordinated back-end application functionality. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

125. The selected Offeror must provide time-based content expiration and version management capabilities. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

126. The selected Offeror must provide the ability for a user to see, at configurable periods prior to session timeout, a message that warns them of the imminent timeout (e.g. a five [5] minute notice) and they must be able to click this message and keep their server session active. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

127. The selected Offeror's solution must support the most current versions of major browsers for devices that include the most popular operating system brands (i.e., Android, Macintosh, and Windows) without requiring specialized plug-ins or applets to function. The corresponding CMS MECT 2.3 Checklist requirement number is TA.CS.6.

128. The selected Offeror's solution must support the printing of items directly from the browser and allow internal users to queue items to print either locally or via batch. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

129. The selected Offeror must provide an accessibility testing solution that incorporates the use of assistive technologies. The solution must be validated through the use of Compliance Sheriff. The corresponding CMS MECT 2.3 Checklist requirement number is TA.CS.18.

130. The selected Offeror must provide screens for data entry with identified mandatory and optional data fields, including basic validations on data entry, including basic validations such as recognizing invalid characters or an incorrect number of characters. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.FR.1, TA.SP.1, and TA.SP.2.

131. The selected Offeror must collect and collate statistics on PIMS Module usage to support reporting requirements and continuous improvements in design. The corresponding CMS MECT 2.3 Checklist requirement number is TA.PM.6.

132. The selected Offeror must utilize web statistics that capture the entry screens, exit screens, IP addresses, application abandonment frequency/location, logon duration, session timeouts, time on each page, and keyword searches. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

133. The selected Offeror must provide a Capacity Planning approach that incorporates the use of a performance monitoring system for planning, sizing, and controlling capacity as needed. The corresponding CMS Checklist requirement number is TA.PM.5.

134. The selected Offeror must propose one (1) or more COTS monitoring tools to proactively monitor the performance, track progress, and facilitate decision making of key application components and services of the proposed solution and alert system administrators to instances of performance outside of acceptable thresholds as defined by pertinent performance standards. The corresponding CMS MECT 2.3 Checklist requirement number is TA.DC.7.

135. The selected Offeror must provide, configure, and operate COTS tool(s) to monitor Key Performance Indicators ("KPIs") metrics, including response time, resource availability, CPU utilization, and memory utilization thresholds via a dashboard. The selected Offeror must provide Department staff with on-demand access to utilize this tool. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.PM.7 and TA.PM.8.

136. The selected Offeror's solution must send alerts through e-mail, SMS, and CRM based on all monitored attributes. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

137. The selected Offeror must provide a performance dashboard(s) of a wide range of application services and network services, providing the ability to drill down to a level where the observations provide useful information and both real-time and snapshot views. The corresponding CMS MECT 2.3 Checklist requirement number is TA.BI.5.

138. The selected Offeror must maintain availability and user access to the module at all times, with the exception of planned downtime due to system upgrades or routine maintenance. The selected Offeror must communicate and coordinate all planned downtime and maintenance outages with the Department at least ten (10) business days in advance to allow for Department approval. The notification must include the date and time of the planned maintenance along with the anticipated time the module will be offline and unavailable. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

139. The selected Offeror must develop a standard maintenance page viewable during downtimes. The Department must have the ability to launch this page. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

140. The selected Offeror must utilize virtualization, where possible, in design and be prepared to create virtualized secured environments that are highly available, sustainable, extendible, and portable across hardware platforms. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

141. The selected Offeror must provide for the easy search and retrieval of historical data for all types of data. Data retrieved must include only the targeted files and documents with selection criteria to be set by the user. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

142. The selected Offeror must provide a presentation of searches that result in multiple pages of data in small groups of data with Next/Back paging capability. Page numbers must be displayed. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

143. The selected Offeror must provide flexible, adaptable technology to support the ongoing changes to business processes due to evolving federal and Department regulations and requirements. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

144. The selected Offeror must configure and implement the solution with the purpose of optimizing long-term maintenance and operations efforts (i.e., build for lowest cost long-term operational costs). No PIMS-specific MECT 2.3 Checklist requirement has been identified.

145. The selected Offeror must maintain adequate technical support and staffing to provide twenty-four (24) hour a day, seven (7) days a week, three hundred sixty-five (365) days a year hosting services. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

146. The selected Offeror's solution may be hosted or cloud-based, but offshore hosting is not acceptable; however, offshore development is permitted provided Department-specific data is not used. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

147. The selected Offeror must provide a graphical representation of reporting data as defined by the Department. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

148. The selected Offeror's solution must export reporting information into Excel or other formats as defined by the Commonwealth. The corresponding CMS MECT 2.3 Checklist requirement number is TA.FR.4.

G. Functional Requirements. This section details the functional requirements that the selected Offeror's PIMS Module must meet. Offerors must propose a solution that demonstrates its alignment with the detailed functional requirements.

1. The selected Offeror will provide a solution that will perform data analytics utilizing the MEDICAID data stored in the Department's EDW. The corresponding CMS MECT 2.3 Checklist requirement numbers are CM.PI1.1, PE.PI1.11, PE.PI1.13, PE.P12.14 and PE.P12.17.

2. The selected Offeror will provide analysis services capable of performing exploratory projects, based on the Department's need, in one or more of the following Data Analytics Domain:
    a. Life Sciences and Public Health;
    b. Social and Public Policy Analysis;
    c. Fraud, Waste, and Abuse;
    d. Risk Management (Insurance and Claims Management);
    e. Audit, Compliance, and Regulation; and,
    f. SUR for the detection of fraud, waste, and abuse

    No PIMS-specific MECT 2.3 Checklist requirement has been identified.

3. The selected Offeror must use advanced statistical analysis techniques such as nonlinear complex variate simulations, nonparametric regression, analysis of homogeneity of variance, covariance, multivariate cluster/outlier analyses or advanced applications of group theory used to map sets of observations including:
    a. Artificial Intelligence;
    b. Cognitive Computing;
    c. Data Mining;
    d. Micro and Macro Trending, Outlier Analysis;
    e. Machine Learning;

f. Open Data Platforms;
g. Policy Change through Outcome Analysis, including analyses incorporating varying elements of time trend analysis;
h. Crowd Sourcing and Social Media;
i. Text Mining; and
j. Geospatial Technology, Modeling, and Presentation Applications.

The corresponding CMS MECT 2.3 Checklist requirement number is PE.PI2.11.

4. The selected Offeror's module must have the functionality to host projects utilizing (computing and storage) Open Source and Commercial Data Analytics tool commonly used by Data Analytics/Scientist Community supported release or distributions (as applicable) of Windows, Linux or Unix. No PIMS-specific MECT 2.3 Checklist requirement has been identified.design, develop, implement and maintain monthly and ad-hoc profiles of providers, owners, agents, managing employees, recipients, and caregivers against state and federal databases. Discrepancies identified by the selected Offeror must be included on the Monthly Report. See **Part III-8.C Monthly Reports**. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

5. The selected Offeror must cooperate with the Department's MMIS IV&V Contractor as requested by producing items, including artifacts, system documentation, and reports to assist the Department in achieving and maintaining CMS certification. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

6. The selected Offeror must design, develop, implement, and maintain electronic Fraud, Waste and Abuse Case Management functionality within the PIMS Module. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

7. The selected Offeror must include all necessary data elements in the PIMS Module to support investigative reporting needs. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

8. The selected Offeror's PIMS Module must interface within the SI/DH CRM. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

9. The selected Offeror's PIMS Module must accommodate a phased-in implementation of the MMIS 2020 Platform. Once implemented, the system must be able to expand to include new functions without major impact on the system. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

10. The selected Offeror's PIMS Module must meet external and internal management reporting requirements. This requirement can be met by providing user-controlled sequence, frequency, and content specification for production reports, and by either providing a modern report and retrieval system for ad hoc report requests or the availability of an end-user report and retrieval functionality associated with the database product. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

11. The selected Offeror's PIMS Module must provide the following process controls:

a. Comprehensive edit controls which, for example, prevent incomplete or incorrect data from being processed.
b. Programmatic control of the process flow to prevent information from being processed in the wrong sequence.
c. Processing cycles completed in a logical, prescribed order.
d. Integrity of data entering the database, safeguarded through editing criteria.

No PIMS-specific MECT 2.3 Checklist requirement has been identified.

12. The selected Offeror's PIMS Module must allow for user friendly entry and organization of case notes and attachments in multiple formats including pdf, xlsx, and docx. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

13. The selected Offeror's PIMS Module must define all work steps for different case types. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

14. The selected Offeror's PIMS Module must assign a unique identification number automatically for each case and allow for manual assignment of unique identification numbers, with the ability to link unique identification numbers. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

15. The selected Offeror's PIMS Module must assign and re-assign cases automatically based on user-defined criteria, including workload balancing and be able to share and assign cases to multiple users. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

16. The selected Offeror's PIMS Module must route and record all work completed on a case. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

17. The selected Offeror's PIMS Module must schedule events related to the case and provide alerts based on pre-defined business rules to users. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

18. The selected Offeror's PIMS Module must crosswalk provider, recipient and caregiver Medicaid ID numbers; and provide search functionality to locate Medicaid ID numbers by unique identifier and numbers. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

19. The selected Offeror's PIMS Module must maintain the integrity of existing cases during conversion. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

20. The selected Offeror's PIMS Module must allow users, with appropriate role-based security, to update data fields and narrative sections; to include adding and updating a claim note, event description or comment on claims that are under review. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

21. The selected Offeror's PIMS Module must utilize Department templates for all correspondence and ensure all newly created correspondence and documents receive Department approval prior to their use. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

22. The selected Offeror's PIMS Module must have the ability to send data for letter generation to the OBM Module. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

23. The selected Offeror's PIMS Module must link all documentation (e.g. imaged documents, reports, letters, file notes, and spreadsheets) to the case; and retain all pertinent electronic and imaged documentation for evidence. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

24. The selected Offeror's PIMS Module must have the ability to retrieve and store Electronic Health Records. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

25. The selected Offeror's PIMS Module must provide the functionality to print letters locally at the workstation. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

26. The selected Offeror's PIMS Module must allow the upload and download of case tracking information and documents by users, with delete capability across the system. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

27. The selected Offeror's PIMS Module must allow MA providers and MCOs to electronically submit documentation through the SI/DH provider or partner portal and link submitted documentation to a case. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

28. The selected Offeror must manage the size and scalability of document uploads and downloads. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

29. The selected Offeror's PIMS Module must have retention and purging functionality, according to Commonwealth guidelines, with an overall solution for document control. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

30. The selected Offeror's PIMS Module must have functionality to find, view, and update all case records. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

31. The selected Offeror's PIMS Module must be able to add or delete claims that are included in any case record created. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

32. The selected Offeror's PIMS Module must record, track, trend, and report on all information related to the hearings and appeals process for providers and recipients, including case docket numbers, hearing dates, administrative law judge name, final findings, reconsideration, filings with Commonwealth court, etc. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

33. The selected Offeror's PIMS Module must record provider corrective action plans including, due date, reminders, receipt, acceptance, non-acceptance, revisions, and non-compliance. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

34. The selected Offeror's PIMS Module must provide automatic notification for post-corrective action review, according to the Commonwealth-defined time period. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

35. The selected Offeror's PIMS Module must store settlement agreements on the case, status, payments and status dates of progress on the settlement. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

36. The selected Offeror's PIMS Module must analyze staff workload and performance, including:
    a. Number of cases reviewed;
    b. Number of claims and encounters included in the universe;
    c. Total dollars reimbursed for cases included in the universe;
    d. Number of actual claims reviewed in the sample;
    e. Total dollars reimbursed for cases included in the universe; and,
    f. Total dollars identified as overpayments for claims reviewed included in sample size.

    The information must be provided via reports in any frequency designated by the Commonwealth (e.g., by quarter, calendar year, or fiscal year) and by any type of requester (e.g., by individual reviewer, by provider type, by section delivery system, or collectively for the entire unit).

    No PIMS-specific MECT 2.3 Checklist requirement has been identified.

37. The selected Offeror's PIMS Module must include data elements necessary to support the following fraud, waste, and abuse reporting capabilities, including:
    a. Overpayments and underpayments identified as a result of data mining.
    b. Percent of cases opened with overpayments and underpayments identified as a result of data mining.
    c. Number of referrals made to the Office of Attorney General ("OAG"), Medicaid Fraud Control Section ("MFCS"), number of Cease and Desist Orders received from MFCS (including non-Bureau of Program Integrity cases) and of those, the number of closed cases in a specified time, number of accepted and declined referrals, number of closed cases and the disposition.
    d. Dollar value of provider or caregiver referrals made to the OAG/MFCS.
    e. Number of OAG/MFCS referrals to BPI.
    f. Number, type, and modality of referrals and complaints made to and accepted by BPI. Number of complaints received that resulted in a disposition.
    g. Total dollars recovered from all Medicaid integrity activities (settlements and judgments, overpayments, and other collections, MFCS investigations, other civil and criminal law enforcement, and tips).
    h. Generate reports by all data fields with sorting and filtering capabilities.

i. Use standard report naming conventions, as defined by the Commonwealth.
j. Number of recipient referrals made to the PA Office of Inspector General, dollar value of referral and final disposition.

The corresponding CMS MECT 2.3 Checklist requirement numbers are PE.PI2.1, PE.PI2.5, and PE.PI2.13.

38. The selected Offeror's PIMS Module must include all active, closed preliminary, pending and MFCS cases and any other cases that need to be retained; based on Commonwealth's record retention guidelines. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

39. The selected Offeror must provide an automated process to receive, track, view and report on Monthly Hospital Utilization Review Committee, Adverse Determination Summary Reports (required by Medicaid Regulation §1163.80 and Code of Federal Regulations §482.21), including report of non-compliant hospitals. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

40. The selected Offeror's PIMS Module must track and report on the provider enrollment process between Bureau of Fee-for-Service Programs ("BFFSP"), Bureau of Program Integrity ("BPI"), and Office of General Counsel ("OGC") when a provider application is forwarded to BPI for review and recommendation due to a report of disciplinary, licensing, criminal action, or adverse finding resulting from a background check. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

41. The selected Offeror's PIMS Module must conduct, track, and report on pre-payment program integrity reviews defined by the Commonwealth, to include the following criteria:
    a. Specific recipients;
    b. Specific providers;
    c. Claim or service type;
    d. Claims/encounters or a series of claims and encounters that match suspicious billing patterns or that indicate suspicious service provision;
    e. Procedure(s) or diagnosis code(s);
    f. Disposition of case; and,
    g. Dollar value of approved versus denied claims and encounters.

    The corresponding CMS MECT 2.3 Checklist requirement number is PE.PI1.17.

42. The selected Offeror must report the number of Service Questionnaire's (termed Explanation of Benefits ("EOBs") by the Department) generated by the MMIS 2020 Fee For Service Platform Module and returned by the recipient. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

43. The selected Offeror must provide comprehensive tracking functionality and automation opportunities by program and source integration to track and support fraud, waste, and abuse prevention, including:
    a. Gross adjustment recoupments;
    b. Provider payment holds and suspensions, restitutions, self-disclosures, ownership interests, and pre-payment review;
    c. TPL recoveries;

d. Fraud and abuse recoveries (provider, recipient, and caregiver);
e. Provider payments with flexibility down to the provider/service location level; and,
f. Federally-assisted and state-only program recipients separately from other categories of assistance.

No PIMS-specific MECT 2.3 Checklist requirement has been identified.

44. The selected Offeror's PIMS Module must identify, track, and generate an audit log of claims, encounters, recipients, providers, and caregivers in the Departments MMIS 2020 Platform system based on the Department review. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

45. The selected Offeror's PIMS Module must flag the recipient, provider, and caregiver suspected of participation in a health care fraud scheme and address risk level (moratoria, felony) at re-enrollment, re-validation, conclusion of payment suspension, and other scenarios as defined by the Commonwealth. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

46. The selected Offeror's PIMS Module must have the ability to generate data for EOBs to a sampling of Medicaid recipients each month and ad hoc data for targeted sampling, or operate an alternate means approved by the Commonwealth to sample recipients for fraud, waste, and abuse control. The EOB must be in the recipient's designated language or translated and authenticated to the alternative language. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

47. The selected Offeror must ensure all PIMS Module reports are accessible and printable by users. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

48. The selected Offeror must develop, distribute, and evaluate data on demand for summary questionnaires, related to PI investigations; for transmission to the Outbound Mail module via the SI/DH. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

49. The selected Offeror must allow access to PIMS Module users only after permission is granted by the Department. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

50. The selected Offeror's PIMS Module must maintain the date, time, and author of any action taken on a case. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

51. The selected Offeror's PIMS Module must automatically generate data for mailings including, letters, questionnaires, and information requests for transmission to the Outbound Mail module via the DH. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

52. The selected Offeror's PIMS Module must automatically send follow up mailings based on time parameters determined by the Department. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

53. The selected Offeror's PIMS Module must identify cases for follow up review based on time parameters determined by the Department. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

54. The selected Offeror's PIMS Module must scan and associate all incoming correspondence and payments to the appropriate case file. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

55. The selected Offeror's PIMS Module must interface with all MMIS 2020 Platform modules via the SI/DH to send, receive, capture and report on all data sets within the MMIS. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

56. The selected Offeror must provide flexible, adaptable technology to support the ongoing changes to business processes due to evolving federal and Commonwealth regulations. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

57. The selected Offeror's PIMS Module must provide automation in the following areas:
    a. Integrate a registry for home health and caregiver services that includes cross-agency information sharing.
    b. Interface in real-time, or near real-time with relevant federal and Commonwealth databases, including numerous BPI proprietary, and all additional databases. Database examples include: Access; Hearings and Appeals (Provider, Recipient); Adjustment and Financial; OAG/MFCS; OIG; Recipient Restriction; Complaints Log; HCSIS (waivers); FFS case management-TRUcare; Harmony (Dept. Aging-state options, service plan delivery, service orders); Referral (Provider, Recipient); IEB (Independent Enrollment Broker); OMNIA (LOCAs); McKesson CERMe (guideline for home health/rehab/inpatient/DME/prior authorization); RAC and UPIC contractor; Labor and Industry (L&I) Employment data set; State Corporation Bureau.
    c. Provide an automated matching process (if available) for the following:

        i. U.S. Department of Health and Human Services-Office of Inspector General's (HHS-OIG) List of Excluded Individuals and Entities (LEIE);
        ii. Excluded Parties List System (EPLS) on the System for Award Management (SAM);
        iii. National Plan and Provider Enumeration System upon enrollment and reenrollment; and,
        iv. TIBCO –TIBCO is the company/vendor that is in charge of data exchange files with CMS.

    d. Provide system automation to check other databases as identified by the Commonwealth to include:
        i. State-Licensing Board;
        ii. Health-Facility Licensure;
        iii. Insurance;
        iv. Agriculture;
        v. Transportation;
        vi. Labor & Industry;
        vii. Corrections;
        viii. Revenue;
        ix. Prothonotary; and,
        x. Or any licensing, credentialing, or enumerating agency.

No PIMS-specific MECT 2.3 Checklist requirement has been identified.

58. The selected Offeror's PIMS Module must provide the functionality for auto-generation of letter data to be sent to the Outbound Mail module through the SI/DH for letters to be sent to providers, recipients, OIM/CAO, etc. as defined by the Commonwealth. No PIMS-specific MECT 2.3 Checklist requirement has been identified.

59. The selected Offeror must support the use of the Management and Administrative Reporting System ("MARS"). No PA-specific MECT 2.3 Checklist requirement has been identified.

60. The selected Offeror must identify and prepare data, as it is created/received, that will need to be shared by the Data Hub to other stakeholders. No PA-specific MECT 2.3 Checklist requirement has been identified.

61. The selected Offeror's solution must provide the capability to create, open and close care management records. No PA-specific MECT 2.3 Checklist requirement has been identified.

H. PIMS System, Cyber and HIPAA Security Plan. The selected Offeror will design, develop, implement, and maintain PIMS System, Cyber and HIPAA Security Plan ("SCHSP"). The initial PIMS SCHSP must be delivered forty-seven (47) business days after the purchase order effective date. The plan must detail how the selected Offeror will maintain compliance with Commonwealth Information Technology Policies in **Section I-31.A** of this RFP. The PIMS SCHSP must detail how cyber security measures and HIPAA security measures are built into the proposed solution. Include in the PIMS SCHSP how the measures will keep Pennsylvania's Medicaid data secure from cyber data breaches and unauthorized HIPAA violations.

The selected Offeror must describe how its PIMS SCHSP monitors for and prevents cyber breaches, identifies cyber breaches, rectifies cyber breaches that occur, and reports HIPAA violations. The selected Offeror must describe the frequency of review and update of the PIMS SCHSP and the testing frequency and process.

The Offeror must provide detailed information regarding its PIMS SCHSP.

1. Describe the security measures that are built into proposed solutions to prevent system and data breaches.
2. Describe preventative measures, such as policies and procedures, taken to reduce the risk of system cyber-attacks and HIPAA violations.
3. Provide details of how your solution's cyber security and risk mitigation plan prevents cyber data breaches, monitors and identifies cyber data breaches, and rectifies cyber data breaches that occur.
4. Describe the frequency of reviews and updates of the cyber security and risk mitigation plan and the testing process and testing frequency.
5. Use of PII and PHI and a description of the types of data that will be collected.
6. Sources of PII/PHI, populations, and transfer and disclosure mechanisms.
7. Details about the entities with which the collected information will be shared.
8. Privacy and security standards for business partners, other third parties and the agreements that bind these entities.
9. Incident handling procedures.

10. Privacy and security awareness programs and materials for the Offeror's workforce.
11. A statement that the system meets HIPAA requirements for transactions and code sets, privacy and security, and when required, NPI. This statement is in addition to the completion of all the HIPAA-related checklist criteria.

The selected Offeror must detail in the PIMS SCHSP how it will enforce security within the PIMS Module and the selected Offeror's organization including physical security of hardware, interactions between other MMIS 2020 Platform modules and the Department, identification of individuals who have privileged access, and how data to and from external sources is controlled.

The selected Offeror must report all system security breaches including Cyber intrusions to the Department within fifteen (15) minutes of incident identification regardless of the known scope of the incident. The selected Offeror must report misuse of IT resources and loss or theft of equipment (USB drives, laptops, smartphone, etc.) that may contain MMIS 2020 Platform data, via email, to the Department within one hour of the incident. The selected Offeror is required to follow incident-handling procedures to document the full scope of the incident, containment, eradication, and recovery as appropriate to the situation for all incidents. Failure to report any security issues or breach incidents as noted and provide sufficient response to any security issue/breach is subject to liquidated damages

Deliverable: PIMS System, Cyber and HIPAA Security Plan

The Offeror must describe its approach to the development and execution of the PIMS System, Cyber and HIPAA Security Plan. The selected Offeror must deliver the PIMS System, Cyber and HIPAA Security Plan sixty-five (65) calendar days after the purchase order effective date of the contract and must update the Plan annually.

I. Tier 2 Technical Support. The selected Offeror must provide SMEs who can assist stakeholders with PIMS-related issues for Tier 2 Technical Support. Stakeholders will communicate PIMS-related issues to the Tier 1 Support Center by phone, web form, or email. When the Tier 1 Support Center is unable to resolve an PIMS Module-related issue, it will create and route a trouble ticket to the selected Offeror through a CRM tool for Tier 2 assistance. The CRM tool will create a trouble ticket to track the activities taken to resolve the PIMS Module issue. Upon successful completion of the issue, the selected Offeror will complete the trouble ticket showing the corrective actions taken and will route back to the Tier 1 Support Center via CRM. The selected Offeror will collaborate with the ITC/QA Contractor and the Tier 1 Support Center Contractor to design and develop the Tier 2 escalation process and the CRM workflow, including the trouble ticket template.

The selected Offeror must, at a minimum:

1. Coordinate resolution of trouble tickets for PIMS functions sent via CRM from the Tier 1 Support Center;
2. Facilitate resolution of PIMS issues with users and document action in trouble ticket;
3. Return completed trouble ticket via CRM to the Tier 1 Support Center;
4. Escalate PIMS trouble tickets that cannot be resolved to Tier 3 via CRM for resolution;
5. Collaborate with ITC/QA contractor on documenting the knowledge base of information to allow the Tier 1 Support Center to answer common PIMS questions.
6. Acknowledge 99% or greater of all inquiries from the Tier 1 Support Center within one (1) hour of receipt; and,
7. 99% or greater of all inquiries from the Tier 1 Support Center must have a resolution, plan of action or escalation to a defect within three (3) business days.

The Offeror must describe its approach to the development and execution of the Tier 2 – Technical Support.

J. Input and Output File Updates. The selected Offeror must use a solution that processes input file updates accurately and makes all file uploads available within sixty (60) minutes (or depending on the file, at an agreed upon time identified in the project schedules). Likewise, the selected Offeror's solution must provide for the production and delivery of all output files within sixty (60) minutes of sending (or depending on the file, at an agreed upon time identified in the project schedules).

All input and output file protocols and procedures must align and comply with Chapter 11 of the State Medicaid Manual on Medicaid Management Information Systems.

K. Reuse. In accordance with CMS directive, the Department is seeking a PIMS solution that will maximize reuse opportunities for other states and local governments or that has been used by other states and can be reused by the Department. Please explain how your solution will allow reuse by other states in their solution, which may include cloud hosting, open source development and share customization. If you have reused your module in the past with other states in their MMIS, please identify the state and what was reused. See State Medicaid Director Letter #18-005 Mechanized Claims Processing and Information Retrieval Systems – Reuse at https://www.medicaid.gov/federal-policy-guidance/downloads/smd18005.pdf.

The Offeror must describe its approach to the development and execution of Reuse.

I-8. Reports and Program Control. The selected Offeror must work with the Department to define weekly, monthly, quarterly and annual reporting requirements during JAD sessions. The selected Offeror is responsible for the accuracy of calculations and completeness of data used as input. The selected Offeror must make all defined reports available online and in the required format by scheduled time as defined and mutually agreed upon.

A. Operations Report. As the MMIS 2020 Platform Dashboard is being developed by the ITC/QA and SI/DH Contractors, the selected Offeror must produce inputs to the Dashboard that detail PIMS operations. The selected Offeror must develop an Operations Report that includes:

1. Operations Production Status with agreed upon metrics.
2. Service Level Agreement Reporting.
3. Other operational metrics as required by the Department.

B. Weekly Status Reports. The selected Offeror must submit an electronic weekly status report aligned to the PIMS-MWP in a format approved by the Department. The selected Offeror must submit weekly reports for the previous week to the Department no later than 12pm on the first business day of the following week. The reports will cover the previous week's reporting period (Sunday through Saturday). At a minimum, weekly status report must contain the following:

1. Updated Project Plan schedule with upcoming milestones and overall percentage complete.
2. A dashboard that shows the overall status of the project.
3. The plans for activities scheduled for the next week.
4. The status of Deliverables as defined in **Part III, Section III-6. A.**
5. Time ahead or behind schedule for applicable tasks.
6. New risks identified in the previous week.

The Offeror must describe its approach and execution of the weekly status reports. The Offeror may propose additional or more frequent reports and report items based on its experience with IT projects of this size and scope. The Offeror must provide a sample weekly status report with its Technical Submittal.

C. Monthly Status Reports. The selected Offeror must submit an electronic monthly status report aligned to the PIMS-MWP in a format approved by the Department. The selected Offeror must submit monthly reports for the previous month to the Department no later than 8 a.m. on the fifth business day of the subsequent month. The reports will cover the previous month's reporting period (1st calendar day through last calendar day of the month). At a minimum, monthly status report must contain the following:

1. A description of the completion status of the Project in terms of the approved Project Plan incorporating an Earned Value Analysis for schedule and cost.
2. KPIs, including Cost Performance Index ("CPI") and Schedule Performance Index ("SPI"), with explanations if CPI or SPI are beyond thresholds.
3. Updated project schedule with upcoming milestones and overall percentage complete.
4. A dashboard that shows the overall status of the project.
5. The plans for activities scheduled for the next month.
6. The status of Deliverables as defined in **Part III, Section III-6.A.**
7. Time ahead or behind schedule for applicable tasks.
8. Updated issue management report including the issues from the IV&V Contractor's Post-Implementation Assessment Review.
9. A risk analysis of actual and perceived problems along with their suggested mitigations.
10. Strategic changes to the Project Plan, if any.
11. Any organizational changes that may have taken place or will take place. Changes in key personnel must be approved by the Department in advance.
12. Key activities completed during reporting period.

The Offeror must describe its design, development, implementation, and maintenance of the monthly status reports. The Offeror may propose additional or more frequent reports and report items based on its experience with IT projects of this size and scope. The Offeror must provide a sample monthly status report with its Lot 1 Technical Submittal.

D. Meetings. During the course of the contract, the selected Offeror must attend, or lead meetings; as requested by the Department. At the Department's discretion, these meetings will take place in the Harrisburg, Pennsylvania area or be conducted via conference calls.

The selected Offeror must attend MMIS 2020 Platform meetings as directed and support these meetings by providing reports, participating in brainstorming and planning activities, providing consultation and technical assistance, and helping to resolve issues.

For meetings lead by the selected Offeror, the selected Offeror must produce meeting materials, which include schedules, written status reports, draft and final minutes, decision registers, agendas, recaps and other meeting materials. The selected Offeror must provide meeting materials as follows:

1. Distribute agendas at least two (2) business days prior to meetings.
2. Submit meeting minutes to the Department for approval within two (2) business days of meeting being held.
3. Review available project artifacts prior to any meeting.
4. Meeting materials are subject to recording in the MMIS 2020 Platform artifact library.

At a minimum, the selected Offeror must participate as directed in the following meetings:

1. **PIMS Kick-off Meeting.** The selected Offeror must facilitate a kick-off meeting within sixty (60) calendar days of the effective date of the contract for the MMIS 2020 Platform stakeholders confirming project scope and objectives, summary of the project, project schedule, methodology, the roles, responsibilities and expectation of the team, and milestones of the PIMS Module.

2. **Change Control Board Meeting.** The ITC/QA Contractor will facilitate the CCB Meetings that includes the Department, the selected Offeror, and the other MMIS 2020 Platform module and legacy system contractors. The selected Offeror must participate in the CCB and will be notified by the Department for required support as needed.

   The CCB reviews defects and requested changes for each module or functional area and ensures that DHS and the contractors have a mutual understanding of what is to be delivered, when it is to be delivered, and the cost impact in effort hours, if applicable. The CCB serves as a clearinghouse for all defects and changes, including changes to scope and cost. The CCB reports to the MMIS 2020 Platform Steering Team. If a change control item must be elevated above the CCB for resolution, it will be sent by the CCB to the Steering Team for decision. The CCB will meet on a frequency and at a time mutually acceptable to all stakeholders.

   The CCB is comprised of Department resources from multiple program offices and the contractors who have the authority to make decisions related to the defect or status of a change order, its financial impact, and its importance. The core membership of the CCB will invite SMEs and stakeholders to CCB meetings as needed. During the transition from legacy system to the MMIS 2020 Platform, the legacy contractor may also be invited to attend.

3. **Release Planning Meeting.** Release Planning is the logical output of the CCB. Release Planning involves the scheduling of change orders ("CO") agreed upon by the CCB and the impact to Department and MMIS Business Operations. During the transition from legacy system to MMIS 2020 Platform, release planning must account for changes to existing modules or functionalities. Release planning must also continue during the M&O phase of the MMIS. The selected Offeror must attend the Release Planning Meeting and will be notified by the Department for required support as needed.

   Under the strategic guidance of the Department, the ITC/QA Contractor will facilitate the Release Planning Meetings that includes the Department, the legacy system contractor, and MMIS 2020 Platform module contractors. The ITC/QA Contractor will produce a proposed system CO release schedule and documentation of its impact to MMIS Business Operations and the EDW. The Release Planning Meetings will convene on a frequency and at a time mutually acceptable to all stakeholders.

   Release Planning is comprised of Department resources from multiple program offices and the contractors who have the authority to make decisions related to the release. The Department resources may invite subject matter experts and stakeholders to the meetings as needed. During the transition from legacy system to MMIS 2020, the legacy system contractor may also be invited to attend.

4. **QA/QC Meetings.** Under the strategic guidance of the Department, the ITC/QA Contractor will facilitate and document in writing all project meetings that are necessitated as part of the QA/QC scope of work. The selected Offeror must participate in the QA/QC Meetings and will be notified by the Department for required support as needed.

5. **Requirements Gathering related meetings.** Under the strategic guidance of the Department, the ITC/QA Contractor will facilitate, and document requirements gathering and JAD sessions, as defined in **Part III-6.A.5 Requirements Management Plan** for the PIMS Module. The selected Offeror must attend all Requirements Gathering related meetings for the PIMS Module and other MMIS 2020 Platform Modules Requirements Gathering related meetings as needed.

6. **Status Meetings**. The selected Offeror must participate in status meetings with the Department. Under the strategic guidance of the Department, the meeting will follow an agenda and allow the selected Offeror to report to the Department on the projects' schedules, risks, issues, decisions, action items, and accomplishments, at a minimum.

The Offeror must describe its approach to facilitating and participating in meetings. The Offeror may propose additional meetings based on their experience with IT projects of this size and scope. DHS may require the selected Offeror to attend and facilitate other meetings at its discretion.

I-9. Performance Standards. The Commonwealth has developed a set of minimum Performance Standards defined below, which the selected Offeror must meet, or exceed in order to be in good standing. The Department may, at its discretion, assess liquidated damages. Where an assessment is defined as an "up to" amount, the dollar value will be set at the discretion of the Department. The selected Offeror's performance will be reviewed and assessed on a monthly basis. The DHS Contract Administrator will give written notice of each failure to meet a performance standard to the selected Offeror. If Department does not assess liquidated damages in a particular instance, the Department is not precluded from pursuing other or future assessments relating to those performance metrics and their associated damages.

Table 4. PIMS Module Performance Standards

Category	Criteria	If Non-Compliant, Amount Owed
PIMS – 1 Personnel	**Key Personnel:** PIMS Executive Account Director PIMS Project Manager PIMS Testing Manager PIMS Functional Lead PIMS SUR Specialist	Failure to notify DHS Contract Administrator of voluntary diversion within thirty (30) calendar days may result in the Department assessing liquidated damages of up to $2,500. Failure to Interim fill a Key Personnel vacancy within thirty (30) calendar days and/or permanently fill a vacancy within ninety (90) calendar days may result in a penalty of up to $2,000 per day for each day vacancy.
PIMS – 2 System availability	Access to all production MMIS 2020 Platform activities are available for all MMIS users at all times except during planned downtime.	Any unscheduled downtime whether consecutive or intermittent cannot exceed one (1) hour per calendar month in total. • Unscheduled downtime in excess of one (1) hour but fewer than five (5) hours in one (1) month may result in the Department assessing up to $250 for each partial or full hour in liquidated damages. • Unscheduled downtime exceeding five (5) hours per month but fewer than twelve (12) hours may result in the Department assessing up to $500 for each partial or full hour in liquidated damages. • Unscheduled downtime exceeding twelve (12) hours per month may result in the Department assessing up to $1,000 for each partial or full hour in liquidated damages.
PIMS – 3 System availability	All test and training environments will be available 6 a.m. – 6 p.m. Monday through Friday and as agreed to during testing and training windows.	Any unscheduled downtime whether consecutive or intermittent cannot exceed one (1) hour per calendar month in total. • Unscheduled downtime in excess of one (1) hour but fewer than eight (8) hours in one (1) month may result in the Department assessing up to $500 in liquidated damages. • Unscheduled downtime exceeding eight (8) hours per month may result in assessing up to $1,000 in liquidated damages.
PIMS – 4 Interactive Response Time	Ninety-eight percent (98%) of all interactive transactions will have a responses time of two (2) seconds or less as measured from the receipt of transactions to the response back to the sender. Response for this Performance Standard is based on the average time between the receipt of a transaction and response/acknowledgment of the transaction.	Interactive Response Time for each transaction will be recorded daily from midnight to midnight each day. The sum of transactions exceeding the two (2) second Interactive Response Time will be divided by the total number of transactions for each twenty-four (24) hour period. Should the resulting percentage equals more than two percent (2%), the Department may assess up to $1,000 in liquidated damages.

Category	Criteria	If Non-Compliant, Amount Owed
PIMS – 5 Outbound Response	All outbound files received from the SI/DH must be transmitted back to the SI/DH within four (4) hours.	All outbound files will be measured in a calendar month. The Department may assess up to $2,500 in liquidated damages for each file when response time exceeds the allowable response time by one (1) hour or more,
PIMS – 6 Disaster Recovery	Conduct and pass a 24-Hour Recovery Point Objective and a 36-Hour Recovery Time Objective test of the DR Plan biannually	Failure to pass the biannual 24-Hour Recovery Point Objective or the 36-Hour Recovery Time Objective may result in the Department assessing up to $1,000 in liquidated damages; for each failure.
PIMS – 7 Disaster Recovery	On the occurrence of a disaster, the selected Offeror must meet the 24-hour Recovery Point Objective and the 36-hour Recovery Time Objective when executing the DR plan.	Failure to meet the 24-hour Point Objective may result in the Department assessing up to $10,000 in liquidated damages. Failure to meet the 36-hour Recovery Time Objective may result in the Department assessing up to $10,000 in liquidated damages.
PIMS – 8 Audits	Pass all audits without incurring monetary fines to include those conducted by the Commonwealth, CMS, and annual SOC 3 audits.	The Department may assess liquidated damages equal to the costs incurred and monetary fine to address any audit findings.
PIMS – 9 Compliance	All software utilized within the PIMS Module must be a version compatible with the SI/DH, unless otherwise approved by the Department. Waived for the first six (6) months of each module's M&O.	The Department may assess liquidated damages in the amount of up to $1,000 $2,500 per month when PIMS software is not compatible with the SI/DH. Compatible is define as the SI/DH and PIMS Module cannot function because of version mismatch.
PIMS – 10 Compliance	Adhere to and remain current with applicable State and Federal laws, rules, regulations, guidelines, policies, and procedures relating to information systems, information systems security and privacy, physical security, PHI confidentiality and privacy, Americans with Disabilities Act and Section 508 of the Rehabilitation Act.	The Department may assess liquidated damages of up to $2,500 plus any incurred cost to remediation for each non-compliance condition it identifies during the course of normal day to day operations, as the result of a finding in an audit, or as reported in a monthly report.
PIMS – 11 Auditing /Archiving	Maintain audit log data online for a minimum of one hundred and twenty (120) calendar days. Waived for the first one hundred and twenty (120) calendar days of M&O.	The Department may assess liquidated damages of up to $1,000 per month for noncompliance.
PIMS – 12 Auditing /Archiving	Maintain all original inbound and outbound transactional data for a minimum of sixty (60) calendar days. Waived for the first sixty (60) calendar days of M&O.	The Department may assess liquidated damages of up to $1,000 per month for noncompliance.

Category	Criteria	If Non-Compliant, Amount Owed
PIMS – 13 Auditing /Archiving	Maintain system reports and extracts online for a minimum of one hundred and eighty (180) calendar days. Waived for the first one hundred and eighty (180) calendar days of M&O.	The Department may assess liquidated damages of up to 1,000 per month for noncompliance.
PIMS – 14 Reporting	Standard, recurring reports, including CMS required reports and Medicaid Chapter 11, must contain accurate data and made available by the date and time specified by the Department. • Daily reports - due by 8 a.m. of the next business day. • Weekly reports - due by 12 p.m. of the first business day of the following week. • Monthly reports - due by 8 a.m. the 5th business day of the following month. • Quarterly Reports - due by 8 a.m. the 1st business day the third week of the first month following the end of the quarter. • Annual reports - due by 8 a.m. the 1st business day of the second month of the following year. • All other reports not defined above will be due as mutually agree upon during JADs.	The Department will review report accuracy and delivery on a monthly basis. •Any report containing data the Department determines as incorrect may result in the Department assessing liquidated damages in the amount of up to $250 for each incorrect report. • Each report delivered after the time specified and due date may result in the Department assessing liquidated damages in the amount of up to $250 for each late report.
PIMS – 15 Updates	Upload all input files from internal and external sources and make available at date and time schedules as mutually agreed to by the Department and the selected Offeror during the DDI of each module prior to M&O.	File uploads delayed by more than sixty (60) minutes after the agreed upon time frame will result in a penalty as follows: •Up to ten (10) files delayed in one (1) month may result in an assessment of up to $1,000. •Eleven (11) or more files delayed in one (1) month may result in an assessment of up to $2,000. Files uploads not completed accurately may result in an assessment of up to $1,000 per incident.
PIMS – 16 Updates	Accurately produce and deliver all output files at agreed upon date and time schedules.	File uploads delayed past the scheduled time by more than sixty (60) minutes may result in the Department assessing liquidated damages as follows: •Up to ten (10) files delayed past the scheduled time in one (1) month may result in liquidated damages of up to $1,000 •Eleven (11) or more files delayed past the scheduled time in one (1) month may result in liquidated damages of up to $2,000
PIMS – 17 Updates	Download all output files at agreed upon date and time schedules as mutually agreed to by the Department and the selected Offeror during the DDI of each module prior to M&O.	Output files delayed past the scheduled time by more than sixty (60) minutes may result in the Department assessing liquidated damages as follows: •Up to ten (10) files delayed past the scheduled time in one (1) month may result in liquidated damages of up to $500. •Eleven (11) or more files delayed past the scheduled in one (1) month may result in liquidated damages of up to $1,000.

Category	Criteria	If Non-Compliant, Amount Owed
PIMS – 18 Security	All system security breaches must be reported to the DHS Contract Administrator within fifteen (15) minutes of incident identification regardless of the known scope of the incident. Misuse of IT resources, loss or theft of equipment (USB drives, laptops, smartphone etc.) that may contain MMIS 2020 Platform data must be reported via email to the DHS Contract Administrator or designee within one (1) hour of the incident. The selected Offeror must follow incident handling procedures for all incidents to include scope of incident, containment, eradication and recovery as appropriate to the situation.	Failure to report incident or provide sufficient response to any security issue or breach may result in the Department assessing liquidated damages in the amount of up to $10,000 per security breach or incident.
PIMS – 19 Defect Management	A CAP must include the proposed timeline for correcting the issues conforming to **Part I, Section III-6.C PIMS Defect Management Plan** for approval by the Department. DHS may change the severity level of any system event or issue after considering the effect on the provider community, population served, and continued system operations. When reconciliation is required to correct the downstream influence of a defect, the selected Offeror must provide a plan within two (2) business days. The reconciliation plan will detail how the affected issues will be corrected for the Department's review and approval. In instances where claims are affected, the report must include number of claims affected, original amount paid, adjusted amount of payout or take back, affected providers, and other elements required for the Department's review and approval. Upon Department's approval, the correction will occur within the time frames on **Part III, Section I-6.6 PIMS Defect Management Plan**.	DHS will monitor all reported system issues and associated timeframes. Failure to meet any assigned timeframes for Critical, Significant and Moderate defects may result in the Department assessing liquidated damages in the amount of up to $2,000 for each issue. Additional liquidated damages will be assessed at up to $1,000 every seven (7) calendar days until correction is implemented. Minor defects may result in the Department assessing liquidated damages in the amount of up to $2,500 per incident if agreed-upon resolution time is not met. Failure to deliver a CAP within given timeframe may result in liquidated damages of up to $750 per calendar day for each calendar day delayed. Failure to implement an approved reconciliation plan within approved timeframe may result in liquidated damages of up to $750 per calendar day for each calendar day delayed.
PA-20 Response Time	Response time requirements are classified in four (4) categories. Each real-time service will be assigned a priority during the requirements and design process. The selected Offeror is responsible for response times only within its end points. Once assigned a priority, responses must meet the following response time requirements: Category 1: equal to a sub-second, 99% of the time Category 2: equal to a sub-second, 98% of the time Category 3: less than or equal to two (2) seconds, 98% of the time Category 4: less than or equal to twenty (20) seconds, 90% of the time	For each category's hourly average that exceeds the threshold response time in a calendar month, the Department may assess up to $2,500 in liquidated damages for each category.
PA-21 Quality – Notice Output Files	Create and deliver output data of PA/PE approval and denial notices to the SI/DH with the correct system and user populated data as defined and agreed upon by the Department.	Failure to create and deliver output data of PA/PE approval and denial notices to the SI/DH with the correct system and user populated data may result in the Department assessing liquidated damages of up to $100 per notice of output data with one or more errors.

Category	Criteria	If Non-Compliant, Amount Owed
PIMS – 22 Maintenance	All scheduled maintenance requests must be requested a minimum of ten (10) business days prior to the maintenance occuring.	Failure to notify the Department at least ten (10) business days prior to scheduled maintenance may result in the Department assessing liquidated damages of up to $1,000 for each day for which notice is late.
PIMS – 23 Tier 2 Response	Acknowledge 99% of all inquiries must acknowledge all inquiries from the Tier 1 Support Center within one (1) hour of receipt.	Failure to acknowledge inquires 99% or greater in any calendar month may result in the Department assessing liquidated damages of $500 per month.
PIMS – 24 Tier 2 Resolution	98% or greater of all inquiries must have a resolution, plan of action or escalation to a defect within three (3) business days.	Failure to resolve 99% of all inquiries within three (3) business days may result in the Department assessing liquidated damages of $1,000 per month.
PIMS – 25 Deliverables	Delivery of acceptable developed materials (either approved or conditionally approved) as determined solely within the discretion of the Department, including acceptable updates to developed materials, by the date and time specified by the Department.	A late deliverable may result in the Department accessing liquidated damages in an amount of up to $500 per calendar day up to 5% of the monthly fixed fee invoice.

A. For any deficiency, including ones relating to the performance metrics, the selected Offeror will prepare and submit a CAP for any observation or finding contained in a notice of deficiency. Unless another time period has been specified for submission, the selected Offeror must submit the CAP to the Department within ten (10) business days of notification of the deficiency or such longer time as may be agreed to by the Department.

B. The selected Offeror must include in the CAP:

1. Brief description of the findings;
2. Specific steps the selected Offeror will take to correct the situation or reasons why it believes corrective action is not necessary;
3. Name(s) and title(s) of responsible staff person(s);
4. Timetable for performance of the corrective action steps;
5. Monitoring that will be performed to ensure that corrective action steps were implemented; and
6. Signature of the selected Offeror's Executive Account Director.

C. The selected Offeror must implement the corrective action plan within the timeframe agreed to by the parties for that particular corrective action plan. Failure to implement a corrective action plan, in the manner agreed to, may result in further action by the Department, including a finding of default.

D. In the event the Department determines a deficiency to be a serious non-compliance with the selected Offeror's obligations under the contract, the Department may find the selected Offeror in default.

I-10. Objections and Additions to Standard Contract Terms and Conditions. The Offeror will identify which, if any, of the terms and conditions it would like to negotiate and what additional terms and conditions the Offeror would like to add to the standard contract terms and conditions as part of its Lot 1 Technical Submittal, not via the Question and Answer process. The Offeror's failure to make a submission under this paragraph will result in its waiving its right to do so later, but the Department may consider late objections and requests for additions if to do so, in the Department's sole discretion, would be in the best interest of the Commonwealth. The Department may, in its sole discretion, accept

or reject any requested changes to the standard contract terms and conditions. The Offeror will not request changes to the other provisions of the RFP, nor will the Offeror request to completely substitute its own terms and conditions. All terms and conditions must appear in one integrated contract. The Department will not accept references to the Offeror's, or any other, online guides or online terms and conditions contained in any proposal.

Regardless of any objections set out in its proposal, the Offeror must submit its proposal, including the cost proposal, based on the terms and conditions set out in the Standard Terms and Conditions**.** The Department will reject any proposal that is conditioned on the negotiation of the terms and conditions set out in the Standard Terms and Conditions or to other provisions of the RFP as specifically identified above.

DRAFT TECHNICAL SUBMITTAL:
LOT 2: THIRD PARTY LIABILITY ("TPL") SERVICES

II-11. Statement of the Project. State in succinct terms your understanding of the problem presented, and the service required by Lot 2 of this RFP. The Offeror's response must demonstrate that the Offeror fully understands the scope of services to be provided, the Offeror's responsibilities, and how the Offeror will effectively manage the contract. The statement of the problem must discuss specific issues and risks associated with the TPL Services and must include proposed solutions for each. The Offeror must demonstrate how they would develop and maintain relationships with the other MMIS 2020 Platform module's contractors for the MMIS 2020 Platform.

II-12. Management Summary. Include a narrative description of the proposed effort and a list of the items to be delivered or services to be provided. Include a description of the proposed collaboration with the SI/DH Contractor, the ITC/QA Contractor, the IV&V Contractor, the Tier 1 Support Center Contractor, Legacy MMIS contractor and other MMIS 2020 Platform module contractors. The summary will condense and highlight the contents of the Lot 2 Technical Submittal in a manner that allows a broad understanding of the entire Lot 2 Technical Submittal.

I-13. Qualifications.

A. Company Overview. The Offeror must describe the corporate history and relevant experience of the Offeror and any subcontractors. The Offeror must detail information on the ownership of the company (names and percent of ownership), the date the company was established, the date the company began operations, the physical location of the company and the current size of the company. The Offeror must provide a corporate organizational chart.

The Offeror must describe its corporate identity, legal status, including the name, address, telephone number, and email address for the legal entity that is submitting the proposal. In addition, the Offeror must provide the name of the principal officers, a description of its major services and any specific licenses and accreditations held by the Offeror.

If an Offeror is proposing to use the services or products of a subsidiary or affiliated firm, the Offeror must describe the business arrangement with that entity and the scope of the services the entity will provide.

If the experience of any proposed subcontractor is being used to meet the qualifications and requirements of Lot 2 of this RFP, the Offeror must provide the same information as listed above for the subcontractor. This information must be presented separately within this section, clearly identifying the subcontractor's experience and name.

References. The Offeror must provide a list of at least three (3) relevant contacts within the past four (4) years to serve as corporate references. The references must be outside clients (non-Pennsylvania DHS). This list will include the following for each reference:

1. Name of customer
2. Type of contract
3. Contract description, including type of service provided
4. Total contract value
5. Contracting Officer's name and telephone number
6. Role of subcontractors (if any)
7. Time period in which service was provided.

The Offeror must submit Corporate Reference Questionnaire, directly to the contacts listed. The references should return the completed questionnaires in sealed envelopes to the Offeror. The Offeror must include these sealed references with its Lot 2 hardcopy Technical Submittal.

The Offeror must disclose any contract or agreement cancellations, or terminations within five (5) years preceding the issuance of this RFP. If a contract or agreement was canceled or terminated for lack of performance, the Offeror must provide details on the customer's allegations, the Offeror's position relevant to the allegations, and the final resolution of the cancellation or the termination. The Offeror must include each customer's Company or entity name, Address, Contact name, Phone number, and Email address.

The Department may disqualify an Offeror based on a failure to disclose such a cancelled or terminated contract or agreement. If the Department learns about such a failure to disclose after a contract is awarded, the Department may terminate the contract.

B. Prior Experience. The Offeror must include experience with modular implementations, particularly TPL Module implementations that were similar in size and complexity as the Pennsylvania's MMIS 2020 Platform Project. Experience includes implementation activities, operations, project management activities, CMS Medicaid Enterprise Certification, knowledge of MMIS, CMS Conditions and Standards, MITA, and MECT checklists, Health Care Exchanges, and supporting the transition from a legacy MMIS or healthcare systems to modern modular systems.

Highlight any modular MMIS or healthcare-related experience that your organization performed within the last four (4) years.

Experience shown must be work done by individuals who will be assigned to this project as well as that of your company. Referenced studies or projects must be identified, and the name of the customer shown, including the name, address, and telephone number of the responsible official of the customer, company, or agency who may be contacted.

C. Offeror Personnel. Include the number of executive and professional personnel, analysts, auditors, researchers, consultants and other staff who will be engaged in the work. Show where these personnel will be physically located during the time they are engaged in the work. For key personnel, include the employee's name and, through a resume or similar document, the key personnel's education and experience. Indicate the responsibilities each individual will have and how long each has been with your company. Identify by name any subcontractors you intend to use and the services they will perform.

A minimum of three (3) client references for Key Personnel must be identified. All client references for Key Personnel must be outside clients (non-Pennsylvania DHS) who can provide information on the individual's experience and competence to perform project tasks similar to those requested in this RFP. Key Personnel may be a member of the Offeror's organization, or any subcontractor included in the Offeror's proposal.

The Offeror must submit, Personnel Reference Questionnaire, directly to the contacts listed. The references should return completed questionnaires in sealed envelopes to the Offeror. The Offeror must include these sealed references with its Lot 2 hardcopy Technical Submittal.

Submitted resumes are not to include personal information that will or will be likely to require redaction prior to release of the proposal under the Right-to-Know Law, including but not limited to home addresses and phone numbers, Social Security Numbers, Drivers' License numbers or numbers from state identification cards issued in lieu of a Drivers' License, and financial account numbers. If the Commonwealth requires any of this information for security verification or other purposes, the information will be requested separately and as necessary.

The Department has identified four (4) key personnel:

TPL Executive Account Director
TPL Project Manager
TPL Testing Manager
TPL Functional Lead

Table 5 provides the minimum qualifications and high-level responsibilities for each key personnel. This table also provides the minimum onsite requirements for each key personnel for the phases prior to M&O and the M&O phase. The phases prior to M&O are: 1) Initiation and Planning; 2) Requirements, Design, and Development; 3) Integration, Test, and Implementation. Final onsite percentages will be finalized during contract negotiations. The percent of time onsite during M&O will be as needed determined by future enhancements or other MMIS 2020 Platform changes.

Table 5: TPL Key Personnel Qualifications

ROLE NAME	RESPONSIBILITIES	QUALIFICATIONS	MINIMUM % ONSITE PRIOR TO M&O	MINIMUM % ONSITE DURING M&O
TPL Executive Account Director	1. Provide overall leadership, coordination, and implementation of the TPL solution. 2. Communicate with Commonwealth executives and other MMIS module contractors, as needed. 3. Function as the primary point of contact with the DHS MMIS 2020 Platform Executive Review Board, MMIS 2020 Platform Steering Committee and the MMIS 2020 Platform Project Team for activities related to contract administration, overall project management and scheduling, correspondence between the Department and the selected Offeror, dispute resolution, and status reporting to the Department. 4. Oversee Disaster Recovery. 5. Responsible for approving the invoices submitted to the Department.	1. Ability to commit selected Offeror resources as needed to successfully perform work. 2. Ability to identify and resolve project-related issues and risks requiring escalation within the selected Offeror organization. 3. Ability to resolve project-related issues and risks requiring action by subcontractors. 4. Minimum of ten (10) years of experience working on and/or leading large, complex system implementation projects for similar clients. 5. Knowledge of the Health and Human Services ("HHS") industry.	25	10

ROLE NAME	RESPONSIBILITIES	QUALIFICATIONS	MINIMUM % ONSITE PRIOR TO M&O	MINIMUM % ONSITE DURING M&O
TPL Project Manager	1. Provide day-to-day management and be the principal liaison for the TPL Executive Account Director, DHS MMIS 2020 Platform Project Manager, Department staff, and other MMIS 2020 module contractors 2. Guide the project by using project management processes, organizing the project, and managing team work activities consistent with the approved TPL work plan. 3. Schedule and report activities. 4. Coordinate use of personnel resources. 5. Point of contact for issue identification and resolution. 6. Facilitate implementation of the TPL Module. 7. Responsible for all project deliverables. 8. Responsible for CMS Certification. 9. Responsible for QA/QC. 10. Provide oversight for Tier 2 Support	1. Minimum of five (5) years of experience managing large, complex system development, and with implementation and operation projects of a scale similar to the MMIS 2020 Platform project. 2. Preferably at least five (5) years of experience managing design and development of healthcare information systems or MMIS. 3. Experience leading teams of more than ten (10) staff, including staff from diverse organizations to successfully implement and operate technology-based solutions.	50	As Needed
TPL Testing Manager	1. Coordinate testing efforts for the TPL Module to support implementation, continuity of operations within PROMIS*e*™, and overall MMIS function. 2. Develop the Test Plan for the TPL and integration with PROMIS*e*™ and other MMIS 2020 Platform modules. 3. Oversee test case and test script development and approval for TPL integration testing efforts. 4. Facilitate the TPL test environment setup. 5. Coordinate defect management efforts during TPL integration testing efforts 6. Work in cooperation with the SI/DH Contractor, ITC/QA Contractor, and other MMIS 2020 Platform module contractors.	1. Minimum of six (6) years of experience with planning and executing all phases of system testing – unit testing, system testing, integration testing, user acceptance testing, regression testing, performance testing. 2. Experience with and expertise in selection and use of automated test tools and other testing-related tools. 3. Experience managing test teams comprising individuals from multiple organizations.	25	As Needed

ROLE NAME	RESPONSIBILITIES	QUALIFICATIONS	MINIMUM % ONSITE PRIOR TO M&O	MINIMUM % ONSITE DURING M&O
	7. Participate in Disaster Recovery testing.			
TPL Functional Lead	1. Serve as the TPL SME to the Commonwealth and other MMIS 2020 Platform contractors. 2. Coordinate Configuration Management activities 3. 3. Develop, revise, refresh, and deliver TPL training materials to the ITC/QA Contractor for the TPL Management activities. 4. Oversees TPL Module training. 5. Oversee Tier 2 support.	1. Minimum of five (5) years of experience as a business/functional SME within an HHS, health system or IT environment.	50	As Needed

Staffing Requirements. The selected Offeror must supply staff who will provide TPL services. The selected Offeror must be able to work cooperatively with Commonwealth staff and other individuals and entities during the MMIS 2020 Platform Project. The selected Offeror must coordinate and receive direction from designated Department staff.

The selected Offeror may acquire specialized expertise using subcontracts and must identify any proposed subcontractors in response to **Part II, Section II-13.D. Subcontractors.**

The selected Offeror may not assign Key Personnel to more than one role or to any other position under the TPL contract.

For all other personnel, describe job title, position descriptions, responsibilities, and qualifications.

Due to the ever-changing landscape of MMIS 2020 Platform Project and its complexity, the Department needs to have consistency when dealing with the selected Offeror's staff and other contractors. The selected Offeror must maintain a core team of qualified staff who are able to support the aspects of the DHS MMIS 2020 Platform as detailed in Lot 2 of this RFP.

In the case that it is necessary to identify a resource who will not be 100% dedicated to the MMIS 2020 Platform contract, the Offeror must indicate the percent of time that the personnel will be assigned during DDI activities and the percent of time staff will be assigned during M&O.

Key Personnel Diversions or Replacement. Once Key Personnel are approved by DHS, the selected Offeror may not divert or replace personnel without the prior approval of the DHS Contract Administrator. The selected Offeror must provide notice of a proposed diversion or replacement to the DHS Contract Administrator at least thirty (30) calendar days in advance of the change and provide the name, qualifications, and background check (if required) of the person who will replace the diverted personnel. The DHS Contract Administrator will notify the selected Offeror within ten (10) business days of the diversion notice whether the proposed diversion is acceptable and if the replacement is approved.

"Divert" or "diversion" is defined as the transfer of personnel by the selected Offerors or its subcontractor to another assignment within the control of either the Offeror or subcontractor. Advance notification and approval does not include changes in Key Personnel due to resignations, death, disability, or dismissal for cause or dismissal as a result of the termination of a subcontract or any other causes that are beyond the control of the selected Offeror or its subcontractor. DHS must approve all replacement personnel.

The DHS Contract Administrator may request that the selected Offeror remove a person from this project at any time. In the event that a person is removed, the selected Offeror will have ten (10) business days to fill the vacancy with a person acceptable in terms of experience and skills, subject to the DHS Administrator's approval. DHS may require the removal of an assigned resource to the TPL contract at any time.

Key personnel status will be reviewed monthly as part of the Monthly Status Report - see **Section II-18.C.** of this RFP.

D. Subcontractors. Provide a subcontracting plan for all subcontractors, including SDB and SB subcontractors, who will be assigned to the TPL contract. The selected Offeror is prohibited from subcontracting or outsourcing any part of this Project without the written approval from the Commonwealth. For each subcontractor included in your subcontracting plan, you must provide:

1. Name of subcontractor;
2. Address of subcontractor;
3. Number of years worked with the subcontractor;
4. Number of employees by job category to work on this project;
5. Description of services to be performed;
6. What percentage of time the staff will be dedicated to this project;
7. Geographical location of staff; and
8. Resumes (for key personnel).

The Offeror's subcontractor information must include (through a resume or a similar document) the employees' names, education, and experience in the services outlined in Lot 2 of this RFP. Information provided will also indicate the responsibilities each individual will have in this Project and how long each has been with subcontractor's company.

II-14. Training. The ITC/QA Contractor is responsible for the MMIS 2020 Platform training; however, the selected Offeror will provide the ITC/QA Contractor with system and technical documentation to support the creation and development of training materials for end users. The selected Offeror must use the train the trainer approach to train the ITC/QA Contractor for initial training and for follow up training on enhancements and modifications to the TPL Module. Training will be a collaborative process; the ITC/QA Contractor is the lead trainer working collaboratively with the selected Offeror, the SI/DH contractor and other MMIS 2020 Platform Contractors. The selected Offeror will provide the ITC/QA Contractor with follow up training materials to support enhancements to the TPL Module. The selected Offeror, with the ITC/QA Contractor, will conduct training of each module's functionality, user interfaces, technical components, interfaces, reporting, and other operational requirements. The selected Offeror must provide and maintain its own training environment.

The selected Offeror will focus training requirements on technical end users and the ITC/QA Contractor will focus training requirements to the MMIS 2020 Platform stakeholders. The selected Offeror must design, develop and implement a comprehensive training plan with training materials to provide technical training to the Department and

MMIS 2020 Platform module contractors on TPL Module components and functionality. The training must communicate an overview of the solution, which includes technical framework, integration touchpoints, governance processes, new system components, business processes, services, implementation requirements, and other project requirements. The ITC/QA Contractor will lead training activities on CRM functionality for the MMIS 2020 Platform module contractors and stakeholders.

The Offeror must describe its training solution, the training schedule, materials, and a sample of the training plan in its Lot 2 Technical Submittal.

I-15. Financial Capability. Describe your company's financial stability and economic capability to perform the contract requirements. Provide your company's financial statements for the past two (2) fiscal years. If your company is a publicly traded company, please provide a link to your financial records on your company website in lieu of providing hardcopies. Financial statements must include the company's Balance Sheet and Income Statement or Profit/Loss Statements. Also include a Dun & Bradstreet comprehensive report, if available. The Commonwealth may request additional information it deems necessary to evaluate an Offeror's financial capability as part of its contractor responsibility determination.

I-16. Work Plan. Describe in narrative form your technical plan for accomplishing the work. Use the task descriptions, deliverables, and reports and project control activities in **Part II, Lot 2** as your reference point. Modifications of the task descriptions are permitted; however, reasons for changes must be fully explained. Indicate the number of person hours allocated to each task. Include a Program Evaluation and Review Technique or similar type display, time related, showing each event. If more than one approach is apparent, comment on why you chose this approach. Where appropriate, the selected Offeror must use automation to facilitate completion of tasks. Describe the relationship between primary staff described in **Part III, Section II-13.C Offeror Personnel** and the specific tasks, assignments, and deliverables proposed to accomplish the scope of work. Indicate the number of staff hours allocated to each task.

The Department will provide strategic leadership and regulatory oversight. Describe how your approach will establish standards that maintain fidelity to the MMIS 2020 Platform Project objectives while minimizing disruptions. Describe how communications and work flow between your team and the MMIS 2020 Platform stakeholders will occur.

Describe your management approach, including how you will implement the proposed work plan. Where possible, the Offeror must provide specific examples of methodologies or approaches, including monitoring approaches, it will use to fulfill the Lot 2 technical submittal requirements and examples of similar experience and approach on comparable projects. The Offeror must describe the management and monitoring controls it will use to achieve the required quality of contract services and all performance requirements. The Offeror must also describe the approach to internally monitor and evaluate the effectiveness of meeting the contract requirements.

Items to be addressed in the work plan approach are included in the Tasks section below:

Tasks:

A. Program Management. The Department will provide strategic oversight for the MMIS 2020 Platform Project, including oversight of all contractors. The selected Offeror has primary responsibility for the services under a

resulting contract for the lifecycle of the TPL Module. Under the strategic guidance of the Department, the ITC/QA contractor will be the primary project management office for the MMIS 2020 Platform Project.

Throughout the life of the TPL Module contract, the selected Offeror must use project management techniques that include a comprehensive project plan that is designed, developed, implemented, monitored, tracked and maintained. The selected Offeror must develop status reports and project plan updates as defined in **Part III, Section II-18 Reports and Program Control.**

The selected Offeror must design, develop, implement and maintain the TPL Master Work Plan ("TPL-MWP") for the successful completion of services within scope, budget, and schedule throughout the term of the TPL Module contract. The work plan must adhere to industry best practices for project management such as Information Technology Infrastructure Library ("ITIL") or Project Management Body of Knowledge ("PMBOK®"). Offerors must describe the standard that it will use and its rationale for choosing that project management tool.

The selected Offeror must have a TPL-MWP that will act as a confirmation of project scope, MECL phases, implementation objectives, and result in the product being delivered on time and meeting all requirements specified in Lot 2 of the RFP.

The selected Offeror must develop the TPL-MWP that, at a minimum, includes the following deliverables:

1. TPL Charter and Project Roles
2. TPL Defect Management Plan
3. TPL Change Management Plan
4. TPL Release Management Plan
5. TPL Business Rules Engine Management Plan
6. TPL Quality Management Plan
7. TPL Test Plan
8. TPL Rollback Plan
9. TPL CMS Certification Plan
10. TPL Data Management Strategy Plan
11. TPL Closeout Plan
12. TPL Maintenance and Operations Plan
13. TPL Technical Infrastructure Document
14. TPL System Design Document
15. TPL Turnover Plan

Upon approval by the Department, the selected Offeror must execute and monitor the TPL-MWP. As changes are approved through the Change Management process, the selected Offeror must update plans and provide the Department with a summary of the changes as part of its reporting requirements. Offerors may recommend an alternative to this reporting requirement and provide a rationale for their recommendation. The selected Offeror must immediately alert the Department to any risk to the project identified as the result of the change.

Deliverable: TPL-MWP

The Offeror must describe its approach to designing, developing, implementing, and maintaining the TPL-MWP with recommended timelines for completion of the components. Additionally, the Offeror must describe how it will coordinate and work with MMIS 2020 Platform stakeholders to execute and monitor the TPL-MWP.

The selected Offeror's specific roles in designing, developing, implementing and maintaining the following components of the TPL-MWP are addressed below.

B. TPL Charter and Project Roles. The selected Offeror will design, develop, implement, and maintain the TPL Charter and Project Roles to document and maintain end-product scope. The selected Offeror must deliver the initial TPL Charter and Project Roles for the Department's approval within twenty-two (22) business days after the purchase order effective date and update as needed throughout the MMIS 2020 Platform lifecycle. At a minimum, the TPL Charter and Project Roles will address:

1. TPL Charter

a. Project leadership and key stakeholders
b. Overview of the project
c. Project approach
d. Scope
e. High-level schedule
f. Assumptions
g. Contstraints and risks
h. Responsibility matrix

2. TPL Project Roles

a. **Project Plan.** Under the strategic guidance of the Department, the ITC/QA Contractor will design, develop, implement and maintain the Integrated Master Schedule ("IMS") that includes each MMIS 2020 Platform module. The IMS will serve as the MMIS 2020 Platform baseline schedule, including the transition from the legacy system. Development of and modifications to the TPL project plan occurring throughout the MMIS 2020 Platform lifecycle must be approved by the Department. The Department requires that the TPL project plan is both business and technically oriented with a focus on the technical aspects of the TPL Module. The selected Offeror must coordinate and share the TPL Module project plan with the ITC/QA Contractor's IMS for distribution to the SI/DH Contractor, and other MMIS 2020 Platform module contractors. The selected Offeror must document its project role in the TPL Charter and Project Roles deliverables. The selected Offeror must maintain a detailed project plan and include in the weekly report as defined in **Part II, Section I-18 Reports and Project Control**.

b. **Communications**. Under the strategic guidance of the Department, the ITC/QA Contractor will design, develop, implement, and maintain the Master Communications Plan for the MMIS 2020 Platform. The Master Communications Plan will address communications to all stakeholders, MMIS 2020 Platform contractors, and the legacy system contractor. The ITC/QA Contractor will develop a standard template that the selected Offeror must complete for the TPL Module communications. Modifications to the TPL Module communications occurring throughout the MMIS 2020 Platform lifecycle must be approved by the Department. The Department requires that the TPL Module communications is both business and technically oriented with a focus on the technical aspects of the TPL module. The selected Offeror must coordinate and share the plan with the ITC/QA Contractor for distribution to the SI/DH Contractor and other MMIS 2020 Platform module contractors. The selected Offeror must document in the TPL Charter and Project Roles deliverables its project role in the Master Communications Plan for the MMIS 2020 Platform.

c. **Risks and Issues.** Under the strategic guidance of the Department, the ITC/QA Contractor will design, develop, implement, and maintain the Risks and Issues Management Plan for the MMIS 2020 Platform.

The Risks and Issues Management Plan will include issue identification, tracking, risk analysis, mitigation recommendations, reporting risk information to the Department and other MMIS 2020 Platform Stakeholders, and resolution. The ITC/QA Contractor must account for the transition from the legacy system to the MMIS 2020 Platform in the Risks and Issues Management Plan. The selected Offeror must develop, maintain, and share the TPL Module Risks and Issues with the ITC/QA Contractor for distribution to the SI/DH Contractor, and other MMIS 2020 Platform module contractors. At a minimum, the TPL Module Risks and Issues must include, risk identification, issue identification, tracking, analysis, mitigation recommendations, reporting, and both interim and final resolutions. The Department anticipates risks and issues are both business and technically oriented with a focus on the technical aspects of the TPL module. The selected Offeror must document in the TPL Charter and Project Roles deliverables its project role in the communication of risks and issues to the ITC/QA Contractor for inclusion in the MMIS 2020 Platform Risks and Issues Management Plan.

d. **Requirements Management**. Under the strategic guidance of the Department, the ITC/QA Contractor will design, develop, implement, and maintain the Requirements Management Plan for the MMIS 2020 Platform. The ITC/QA Contractor will at a minimum gather, organize, prioritize, and document business requirements for the lifecycle of the MMIS 2020 Platform, including enhancements made during the M&O phase for the TPL Module. The process must also identify the requirements for the EDW.

   The ITC/QA Contractor will design, develop, implement, and maintain a detailed requirements collection process to document and verify all requirements have been captured for the TPL Module. The ITC/QA Contractor will develop and use a process that includes an analysis of business processes and needs, and translates these processes and needs into formal requirements.

   The Department has gathered initial high-level business requirements for the TPL Module. The requirements are grouped by business functional area and were traced to the CMS certification checklists. The ITC/QA Contractor will use methods to collect requirements that include work sessions, surveys, interviews, policy and regulatory analysis, business rule reviews, facilitated Joint Application Desing ("JAD") sessions and any other means necessary to identify all requirements. The selected offeror is required to provide technical assistance throughout the requirements gathering processes.

   The ITC/QA Contractor will consolidate the final requirements approved by the Department into a Business Requirements Document ("BRD"), and will cross walk the requirements in the BRD to the CMS certification checklist and the TPL's module's Lot 2 RFP requirements. The selected Offeror will collaborate and assist to ensure all requirements are captured.

   The ITC/QA Contractor will complete a Business Gap Analysis to determine if the business requirements meet or exceed what is required for CMS certification, federal and state regulations, and the Department's desired functionality. The selected Offeror will collaborate and assist to enusre the analysis is complete and meets CMS Certification requirements.

   The ITC/QA Contractor will complete the Requirements Traceability Matrix ("RTM") and the selected Offeror will collaborate with the ITC/QA Contractor to verfy the RTM.

   The BRD and the RTM become the initial baseline for the design phase and a reference point throughout the SDLC for determining whether the final product meets the approved requirements. The RTM must, for each identified requirement, contain the source of the requirement, the applicable CMS checklist items, the implementation point, and reference to the test case or script that validates the proper implementation of the requirement. The selected Offeror will collaborate with the ITC/QA contractor to validate the RTM.

Once the Department approves the BRD, the BRD becomes the blueprint for the selected Offeror to build the General System Design ("GSD") document, Systems Requirements Design ("SRD") and Business Design Documents ("BDD"). COTS products are not required to design and develop a GSD or SRD; however, a BDD is required. The selected Offeror will deliver the GSD, SRD, if required, and a BDD to the ITC/QA Contractor for review with the SI/DH and other impacted MMIS 2020 Module contractors. The ITC/QA Contractor will submit all documents to the Department for final approval.

When the GSD, SRD, if required, and BDD are approved by the Department, the ITC/QA Contractor will conduct a Technical Gap Analysis to confirm that the technical solutions developed by the module contractors meet the business requirements. The selected Offeror will collaborate and verify the Technincal Gap Analysis meets the business requirements. If the technical gap analysis reveals deficiencies, the selected Offeror will work with the ITC/QA Contractor to rewrite the GSD. The Department will approve the GSD, and the selected Offeror will commence building the TPL Module.

The selected Offeror must document in the TPL Charter and Project Roles deliverable its project role in the Requirements Management Plan for the MMIS 2020 Platform.

e. **Project Documentation**. Under the strategic guidance of the Department, the ITC/QA Contractor will design, develop, implement, and maintain the MMIS 2020 Platform Documentation Management Plan. including the management of the content of the MMIS 2020 Platform Artifact Library, where all MMIS 2020 Platform documents will be stored. The ITC/QA Contractor will develop a standard template or style guide that the selected Offeror must follow when creating TPL Module documentation. The ITC/QA Contractor will establish and maintain revision control for all artifacts. The TPL selected Offeror must use the ITC/QA supplied tempates to create the followingdocuments:
    1) Flow diagrams and reference materials, including system flow to and from the SI/DH.
    2) Design documents, including interface and architecture.
    3) Data documents, including development, and management of defined data entities, attributes, data models and relationships that convey the meaning and use of Medicaid data and information.
    4) List of application servers and usage.
    5) List of web servers and usage.
    6) Network IP and port details.
    7) Environment variables.
    8) Test Plan.
    9) Training Materials.
    10) Hyperlinks.
    11) Document links.
    12) Organization charts.
    13) Contact details.
    14) Tier 2 Technical support procedures.
    15) Other documents requested by the Department.

    The selected Offeror must document in the TPL Charter and Project Roles deliverable its role in the preparing TPL Module docuementation in collaboration with the ITC/QA Contractor.

f. **Implementation Plan.** Under the strategic guidance of the Department, the ITC/QA Contractor will design, develop, implement, and maintain the MMIS 2020 Platform Implementation Plans to move MMIS 2020 modules and functionality from design, development, implementation, and testing to operations..The plan will provide for the transition from the legacy system to the TPL Module.

The selected Offeror will collaborate with the ITC/QA Contractor in preparing the TPL Implementation plan. At a minimum, the Implementation Plan will include:

1) Description of intended functionalities and their impact on implemented MMIS 2020 Platform modules
2) BDD, BRD, GSD and SRD, if not a COTS product, Business and Technical Gap Analysis
3) Configuration Plan
4) Deployment strategies
5) Rollback Plan
6) Legacy system and installed modules impact
7) Transition Plan from Legacy functionality to the OBM Module
8) Functionality comparison template comparing Legacy functionality to the OBM Module
9) Test Result Review
10) "Go live" checklist
11) Logistics and meeting management
12) Issue reporting and resolution process
13) Defect reporting and resolution process
14) User support, including training Updates to the MMIS 2020 comprehensive user manual

The ITC/QA Contractor will develop a "go live" checklist to document at a minimum, that the system can accept all transaction formats required under HIPAA, accept proprietary forms and formats designated by DHS, produce required EDW extracts, generate reports for users, and operate as designed to meet business needs. The selected Offeror will collaborative with the ITC/QA Contractor to develop, document, and use the "go live" checklist. The Department must approve the "go live" checklist. The selected Offeror must document in the TPL Charter and Project Roles its project role in the preparing the Implementation Plan in collaboration with the ITC/QA Contractor.

g. **Data Conversion Plan.** Under the strategic guidance of the Department, the SI/DH Contractor will design, develop, implement and maintain the MMIS 2020 Platform Data Conversion Plans to move MMIS 2020 modules and functionality from design, development, implementation and testing to operations. The ITC/QA Contractor will evaluate the Data Conversion Plan, identify any gaps, and make recommendations to close gaps. The plan will provide for the transition from the legacy system to the TPL Module.

The selected Offeror will collaborate with the SI/DH Contractor in preparing the Data Conversion plan. At a minimum, the SI/DH Contractor will include in the MMIS 2020 Platform Module Data Conversion Plan:

1) A data management strategy that will support integration, optimization, quality, stewardship, standards, and governance of data.
2) A description of appropriate skill sets, processes, technologies/tools, and any naming conventions followed.
3) Approach to conversion, cleansing and migration.
4) Approach to risk management for data conversion effort.
5) Approach for testing migration or converted data.
6) Approach to reporting the number of records successfully converted vs. errors or exceptions.
7) Approach for cleansing data to prepare it for loading to the proposed solution that is refined as necessary.
8) Approach to resolving data conversion errors and issues.
9) Approach for supporting the Department validation of converted data.
10) Tasks, timelines, and responsible parties for all conversion and migration tasks.

11) Entrance and exit criteria for each phase of the effort.

Deliverable: TPL Charter and Project Roles

The Offeror must describe its approach to the design, development, implementation, and maintenance of the TPL Charter and Project Roles.

C. TPL Defect Management Plan. The selected Offeror must identify and resolve defects identified during testing as well as during production after implementation pertaining to the TPL Module.

The Department and the ITC/QA Contractor are responsible for overall defect management for the MMIS 2020 Platform and will develop the MMIS 2020 Platform Defect Management Plan to identify, track, monitor, and report defects identified during testing and production to the Department and other MMIS 2020 Platform Stakeholders. The ITC/QA Contractor will develop standards for defect identification, tracking, monitoring, and reporting. The selected Offeror may offer recommendations to enhance the standards.

The selected Offeror will leverage the MMIS 2020 Platform CRM tool, developed by the SI/DH Contractor, to report and track issues and defects. The Department and the ITC/QA Contractor will manage the Change Control Board ("CCB") which is responsible for defect management through the lifecycle of the MMIS 2020 Platform Project. The selected Offeror must participate in the CCB.

The Department will determine the severity and priority of defects and will use defect resolution in accordance with the protocols in the chart below. The Severity Level and Definition columns will be used pre-M&O and the remaining columns will be determined for User Acceptance Testing ("UAT"). During M&O all columns will be used.

Severity Level	Definition	Response Time	Corrective Action Plan	Work-around Time	Final Resolution	Reconciliation Plan
Critical	MMIS 2020 Platform Portals or MMIS 2020 Platform module(s) are unavailable creating an inoperable state. Users unable to perform routine job functions that are mission critical. Qualifying condition examples include: • Inability to adjudicate claims • Failure or Inability to process financial cycle(s) •Failure to provide complete eligibility responses greater than 80% of the time. •Any Commonwealth defined mission critical condition.	15 Minutes	1.5 hours	2 hours	1 calendar day	3 calendar days

Severity Level	Definition	Response Time	Corrective Action Plan	Work-around Time	Final Resolution	Reconciliation Plan
Significant	MMIS 2020 Platform Portals or MMIS 2020 Platform module(s) are creating a serious system functionality loss that requires workarounds. Users are partially incapable of completing their normal functions. Qualifying condition examples include: •Incorrect claims adjudication • Limited access to module(s) • Inability to meet established timeframes for production data imports, exports and loading. • Issue affects large group of users with complicated workaround. • Provider or state staff unable to access remittance advice reports or 835 files less than 3 months old.	1.5 hours	3 hours	4 hours	2 calendar days	7 calendar days
Moderate	MMIS 2020 Platform Portals or MMIS 2020 Platform module(s) are creating a limited loss of functionality. Moderate system issues where workarounds exist but, on a whole, do not affect production. Qualifying condition examples include: • Report is not available but can be generated manually • Issue affects small subgroup of users with uncomplicated workaround • Mouse hover feature not triggering text display	1 calendar day	5 calendar days	10 calendar days	30 calendar days	40 calendar days

Severity Level	Definition	Response Time	Corrective Action Plan	Work-around Time	Final Resolution	Reconciliation Plan
Minor	Inconsequential loss of functionality. Impact to user is slight to unknown. Effect on MMIS 2020 Platform system functions negligible to no impact. Issue cosmetic in nature such as spelling error or branding issue. Qualifying condition examples include: • Report incorrectly named • Minor page layout issue • Help page missing or incomplete	7 calendar days	30 calendar days	n/a	90 calendar days or as mutually agreed upon	As mutually agreed upon

Deliverables:
1. TPL Defect Management Plan
2. TPL Defect Management Report

The selected Offeror must deliver the initial TPL Defect Management Plan and the initial TPL Defect Management Report within thirty-three (33) business days of the purchase order effective date; and must update weekly to provide that the project is on schedule and meets CMS Certification requirements. The TPL Defect Management Plan will be reviewed monthly as part of the Monthly Status Report (see **Section II-18.C** of this RFP).

The Offeror must describe its approach to the design, development, implementation, and maintenance of the Defect Management Plan.

D. TPL Change Management Plan. The selected Offeror must participate in the CCB, as needed; and react to requested changes to the TPL Module by providing design documents, estimates, and timelines. The Department and the ITC/QA Contractor manage the CCB and review requested changes for the MMIS 2020 Platform Project. The Department has final approval authority on the priority and scheduling of all changes. Refer to **Section II-18.E** for information about the CCB meeting.

The selected Offeror is responsible for changes to the TPL Module and must recommend changes to the CCB for approval.

The selected Offeror must design, develop, implement, and maintain the TPL Change Management Plan as a participant of the CCB. The selected Offeror will deliver the initial TPL Change Management Plan within thirty-six (36) business days after the purchase order effective date for the Department's approval; and will update weekly throughout the MMIS 2020 Platform project. The plan must contain a methodology for determining and reporting the level of effort, hours, resources, and scheduling and cost of the change.

Deliverable: TPL Change Management Plan

The Offeror must describe its approach to the design, development, implementation, and maintenance of the TPL Change Management Plan.

E. TPL Release Management Plan. Under the strategic guidance of the Department, the ITC/QA Contractor is responsible for developing and executing the MMIS 2020 Platform Release Management Plan. The ITC/QA Contractor will develop a standard template to capture information from the MMIS 2020 Platform and legacy system contractors when developing the MMIS 2020 Platform Release Management Plan. The selected Offeror may have an opportunity to offer recommendations to enhance the template.

The Department will set release timelines in coordination with the MMIS 2020 Platform Project contractors and the legacy system contractor. During the transition from the legacy system to the MMIS 2020 Platform, the Department anticipates that the release schedule will be based on the MMIS 2020 Platform Timeline.

After the full transition to the MMIS 2020 Platform (during M&O), the release schedule will be determined by other factors, such as state and federal mandates, enhancements and module updates or replacements. During M&O the ITC/QA Contractor will be responsible for developing and executing Release Management Plans. The selected Offeror will continue to collaborate and support the ITC/QA Contractor in future releases.

The ITC/QA Contractor will lead release planning meetings, which will be attended by the Department, the legacy system contractor, and MMIS 2020 Platform module contractors. The selected Offeror must participate in the Release Planning Meetings – see **Section II-18.E. Meetings** of this RFP. The Department will provide final approval before a release can be implemented into production.

The Department requires that the MMIS 2020 Platform Release Management Plan is business oriented whereas the release management plans developed by the MMIS 2020 Platform module contractors, including the TPL Release Management Plan, will be both business and technically oriented with a focus on the technical aspects of the release. Regardless, the selected Offeror must coordinate the TPL Release Management Plan with legacy and other MMIS 2020 Platform contractors.

The selected Offeror will design, develop, implement, and maintain the TPL Release Management Plan using the MMIS 2020 Platform Release Management Plan. The selected Offeror will deliver the initial TPL Release Management Plan within forty (40) business days after the purchase order effective date; and will update no later than twenty-nine (29) business days prior to each module or functionality release. The selected Offeror must coordinate the TPL Release Management Plan with the ITC/QA Contractor and the legacy system and MMIS 2020 Platform contractors to maintain ongoing operations of the Department's program and facilitate a seamless transition to the MMIS 2020 Platform with the ultimate goal of achieving CMS certification.

Deliverable: TPL Release Management Plan

The Offeror must describe its approach to the design, development, implementation, and maintenance of the TPL Release Management Plan.

F. TPL Business Rules Engine Management Plan. The selected Offeror will design, develop, implement, and maintain a TPL Business Rule Engine Management Plan that describes its approach to tracking and controlling changes of the TPL Module business rules. All business rules which interact with other MMIS 2020 modules must

be provided to the SI/DH Business Rules Engine. The selected Offeror must submit the initial TPL Business Rules Engine Management Plan within forty-three (43) business days after the purchaser order effective date and review the plan monthly and update with changes. The plan must include a description including how the selected Offeror manages business rule changes to the TPL Module.

Deliverable: TPL Business Rules Engine Management Plan

The Offeror must describe its approach to the design, development, implementation, and maintenance of the TPL Business Rules Engine Management Plan

G. TPL Quality Management Plan. The MMIS 2020 Platform is subject to IV&V oversight. The list of artifacts for CMS Certification subject to IV&V oversight can be found at: https://www.medicaid.gov/medicaid/data-and-systems/mect/index.html.

The ITC/QA Contractor will provide Quality Management ("QM") services. The following items are subject to quality assurance ("QA") review: system security plan, test plans, COOP and DR plans, data conversion plans, and rollback plans. Under the strategic leadership of the Department, and with feedback from the MMIS 2020 Platform module contractors, the ITC/QA Contractor will develop MMIS 2020 Platform standards, such as those for defect identification, tracking, monitoring, and reporting. The ITC/QA Contractor is responsible for the application of standards through quality control ("QC") measures.

In addition to IV&V Contractor oversight and the QM measures described above, each MMIS 2020 Platform module contractor must have QM processes for their modules and services.

The selected Offeror will design, develop, implement, and maintain a TPL QM Plan to maintain quality practices for the lifecycle of the TPL Module. The selected Offeror will deliver the initial TPL QM Plan within seventy-fifty-four (54) business days after the purchase order effective date. The selected Offeror will develop a TPL QM Plan that includes quality assurance of processes, and quality control to provide fidelity to MMIS 2020 Platform standards. The selected Offeror must include in its TPL QM Plan, at a minimum:

1. Overview of QM activities and tasks to be performed;
2. Processes and procedures for conducting QA/QC activities, including procedures for documenting, resolving, and reporting issues and risks identified during QA/QC activities, or problems that may be identified by the Department;
3. Performance monitoring reviews, measures, and reports;
4. Roles and responsibilities of the selected Offeror and Subcontractors, if applicable, in performing QA/QC activities; and,
5. QC procedures for modules' fidelity to standards developed by the selected Offeror such as data exchanges, telecommunications set up ("VPN", etc.), interfaces, and single sign-on requirements.

Deliverable: TPL Quality Management Plan

The Offeror must describe its approach to the design, development, implementation, and maintenance of the TPL Quality Management Plan.

H. TPL Test Plan. In the Testing Phase of the SDLC, the ITC/QA Contractor, selected Offeror, and MMIS 2020 Platform module and legacy system contractors have varying roles dependent upon the level and objective of the

test being conducted. While the Department must approve all test results, tests are led by different entities, and test artifacts are subject to QA and IV&V review. Accordingly, the selected Offeror and all MMIS 2020 Platform module contractors must cooperate with the Department to develop a comprehensive testing plan that provides for each component meeting or exceeding the functional, technical, security, and performance requirements, including bi-directional traceability to requirements and design prior to its implementation. Note: the scope of testing refers to testing of modules or functionality prior to release during the lifecycle of the MMIS 2020 Platform.

The selected Offeror and module contractors must update the module or functionality being tested as well as the testing environment as the result of defects identified. The selected Offeror must communicate testing status to the Department and appropriate stakeholders throughout this phase.

MMIS 2020 Platform testing must be conducted in accordance with industry best practices. For this RFP, the Department has chosen the Guide to the Software Engineering Body of Knowledge Version 3.0 (SWEBOK®) as its reference; however, Offerors may choose a different reference. Offerors must identify their reference and provide a rationale for the standard they choose.

The minimum levels of MMIS 2020 Platform testing are defined below along with the test lead, participation, and QA requirements. Offerors may recommend additional levels or strategies for the Department to consider.

1. **Unit Testing**: Unit testing verifies the functioning of a single module in isolation, including the TPL Module, or other functionality that is tested. Unit testing is self-led by the selected Offeror and subject to QA, where applicable. For example, COTS products are exempt; however, custom code is not.

2. **Integration Testing**: Integration testing verifies the interactions between the TPL Module and the SI/DH. The SI/DH Contractor leads this level of testing in collaboration with the selected Offeror.

3. **System Testing**: System testing tests downstream and end-to-end module-to-module functionality between the TPL Module and the SI/DH. System testing includes assessing non-functional system requirements including security, speed, accuracy, and reliability; and assessing functionality to external interfaces to other applications, utilities, hardware devices, operating environments, providers, business partners, and other stakeholders. The SI/DH Contractor will submit to the Department, the results of security vulnerability testing, and the results are subject to QA.

The levels of MMIS 2020 Platform testing contain various objectives. Offerors may recommend additional objectives or strategies for the Department to consider. The objectives below are the minimum to be conducted:

1. UAT
2. Installation User Testing (Operational Readiness)
3. Regression Testing
4. Performance Testing
5. Stress Testing
6. Back-to-Back Testing
7. Recovery Testing
8. Interface Testing
9. Usability and Human Computer Interaction Testing

The selected Offeror, in collaboration with the ITC/QA Contractor and SI/DH Contractor, must develop test plans that measure and test the MMIS 2020 Platform's ability to function as designed and meet the Department's business needs. The selected Offeror must deliver each TPL Test Plan thirty-three (33) business days prior to the testing of each TPL Module upgrade. Test Cases and scripts must include positive and negative scenarios. The

negative scenarios must include stress testing the system with bad or invalid data to validate that it is rejected correctly. Test scripts must provide step-by-step instructions for executing test cases, including the expected results.

The selected Offeror must provide and maintain its own testing environment; however, the SI/DH Contractor will provide and maintain a testing environment for the SI/DH that allows the MMIS 2020 Platform modules, including the TPL Module, to use for the appropriate level of test. The selected Offeror, in collaboration with the SI/DH Contractor, will provide the various system environments needed to perform the required testing and training activities for the MMIS 2020 Platform, including UAT. The environments must include an integrated test environment to accommodate testing the successful implementations of modules and technical integration activities. The integrated test environment must allow for end-to-end testing and be capable of a mirror of the production system.

The selected Offeror, in collaboration with the SI/DH Contractor, must develop test plans and test summary reports in accordance with industry standards. Plans must outline various parameters, resources, methods, and criteria to fully test the system. The selected Offeror must track defects in the CRM tool.

The SI/DH Contractor and the selected Offeror will create and maintain the logical environments for development and testing, which includes UAT. The selected Offeror must cooperate with the IV&V Contractor, who is responsible for evaluating the test results of all contractors.

The selected Offeror, in collaboration with the SI/DH Contractor, must report the results of testing to the MMIS 2020 Platform module and legacy system contractors, and the Department. The report must identify successes, failures, defects and deviations of the expected results. The report must also identify risks, issues and dependencies that could prevent successful implementation. The selected Offeror, in collaboration with the SI/DH Contractor, must provide recommendations for corrective action. The Department will approve the test deliverables and results.

Deliverables:

1. TPL Integration Test Plan
2. TPL System Test Plan

The Offeror must describe its approach to the design, development, implementation, and maintenance of the TPL Test Plan.

I. TPL Rollback Plan. The selected Offeror must design, develop, implement, and maintain the TPL Rollback Plan. Every module must have a rollback plan to halt or restore the system to its original, pre-conversion condition because of an issue or defect found during implementation or post-implementation. The selected Offeror must develop a rollback plan related to the TPL Module and functionality. The ITC/QA Contractor is responsible for the QA of individual rollback plans.

The ITC/QA Contractor is responsible for developing a standard template that the selected Offeror must follow when creating its individual rollback plan. The selected Offeror may offer recommendations to enhance the template. The selected Offeror will provide its TPL Rollback Plan to the ITC/QA Contractor.

The ITC/QA Contractor will compile the TPL Rollback Plan as part of the MMIS 2020 Master Rollback Plan. The Master Rollback Plan must contain checkpoints for the Department's review where a decision will be made to execute or rollback the release. The plan must include factors and risks to be considered in making the decision.

The selected Offeror will deliver the initial TPL Rollback Plan sixty-five (65) business days prior to the implementation of each module and update the TPL Rollback Plan eight(8) business days prior to the actual module implementation for the Department's approval.

Deliverable: TPL Rollback Plan

The Offeror must describe its approach to the design, development, implementation, and maintenance of the TPL Rollback Plan.

J. TPL CMS Certification Plan. The ITC/QA Contractor will develop a plan for CMS certification of the MMIS 2020 Platform. The selected Offeror will deliver the initial TPL CMS Certification Plan within one hundred twenty-nine (129) business days after the purchase order effective date and update twenty-two (22) business days after a module is onboarded. The Department will use the MMIS module checklists for certification found at https://www.medicaid.gov/medicaid/data-and-systems/mect/index.html. The selected Offeror will work with the ITC/QA Contractor to complete the evidence columns of the checklists for review by CMS for the TPL Module. The selected Offeror must complete certification activities from a technical perspective for the TPL Module and complete MECT checklists prior to gate reviews.

The selected Offeror must collaborate with the ITC/QA Contractor, IV&V Contractor, and the Commonwealth, to obtain CMS Certification.

The selected Offeror, in collaboration with the SI/DH Contractor and the ITC/QA Contractor, must design, develop, implement, and maintain the TPL CMS Certification Plan that includes processes and procedures to manage certification requirements throughout the MMIS 2020 Platform lifecycle.

The Plan must include:

1. Completing the certification checklists and artifacts.
2. Completing certification deliverables.
3. Validating solution functionality against the checklist.
4. Creating traceable deliverables to the checklist.
5. Document and artifact delivery to the MMIS 2020 Platform Artifact Library.

The selected Offeror will participate in CMS Certification activities, as needed by the Department, including:

1. Cooperating with the SI/DH, IV&V and ITC/QA Contractors
2. Completing applicable certification checklists
3. Creating any necessary artifacts for certification
4. Responding to CMS queries before, during, and after site visits in collaboration with the Department.

Deliverables:

1. TPL CMS Certification Plan
2. Completed Certification Checklists
3. Artifacts required by the Department or CMS

The Offeror must describe its approach to the design, development, implementation, and maintenance of the TPL CMS Certification Plan.

K. TPL Data Management Strategy Plan. The selected Offeror must design, develop, implement, and maintain the TPL Data Management Strategy Plan. The TPL Data Management Strategy Plan must include the following concepts: Data Integrity (data cannot be modified undetectably), Data Availability (access is not inappropriately blocked or denied), Data Authenticity (validation of transactions), Data Security (encryption and Department approved security protocols and processes), Non-repudiation of Data (parties to a transaction cannot deny their participation in the transaction). The selected Offeror must demonstrate through data analysis that the implementation outcomes have been validated and are accurate. The methodology of the data analysis must be described in the data management security plan. The selected Offeror will deliver the initial TPL Data Management Strategy Plan within forty-three (43) business days after the purchase order effective date and review the plan monthly and update with changes.

Deliverable: TPL Data Management Strategy Plan

The Offeror must describe its approach to the design, development, implementation, and maintenance of the TPL Data Management Strategy Plan.

L. TPL Closeout Plan. The selected Offeror must design, develop, implement, and maintain the TPL Closeout Plan. The selected Offeror will deliver the initial TPL Closeout Plan within twenty-two (22) business days after the implementation of the TPL Module. When the TPL Module is implemented, the selected Offeror must certify, in writing, to the Department that all SDLC activities have been completed per the implementation plan and all risks, issues, and action items are closed for the TPL Module in collaboration with the SI/DH Contractor, ITC/QA Contractor, and IV&V Contractor.

The Department will evaluate the Closeout Plan documentation from the selected Offeror. Upon acceptance, the Department will prepare an acceptance letter addressed to the selected Offeror indicating that the module was accepted as fully operational.

The acceptance criteria include:

- Deliverables and documentation that have been submitted and accepted by the Department
- No critical or significant defects are open
- No change orders identified as required for CMS certification are open

The IV&V Contractor must prepare a post-implementation assessment and problem resolution report. The report will include identification of all problems and corresponding resolutions found during the implementation; any operational items that could be impacted; and recommendations on improving the rollout process until the final report (after final certification of all modules). Within ten (10) business days after the IV&V Contractor issues the Post Implementation Assessment after each implementation, the selected Offeror will submit an Issue Resolution Plan identifying a resolution plan for any items that are contained in the IV&V Contractor's Post Implementation Assessment Report. The Closeout Plan will be reviewed monthly as part of the Monthly Status Report (see **Section II-18.C** of this RFP).

The selected Offeror must review the Post-Implementation Assessment report and develop issue resolution plans, and strategies and recommendations for future rollouts to prevent recurrences M&O as they relate to the TPL Module.

Deliverables:

1. TPL Closeout Plan

2. Issue resolution plan resulting from the Post-Implementation Assessment report
3. Written certification from the selected Offeror

The Offeror must describe its approach to the design, development, implementation, and maintenance of the TPL Closeout Plan.

M. TPL Maintenance and Operations Plan. The selected Offeror must design, develop, implement, and maintain the TPL M&O Plan. The selected Offeror will deliver the initial TPL M&O Plan thirty-three (33) business days before the implementation of the TPL Module and will review monthly thereafter. The objective of the M&O phase of SDLC is to stabilize and maintain the deployed solution. The selected Offeror must provide operational and maintenance support of the selected Offeror's solution, including any customer service support and system, product, or application upgrades such as operational performance metrics, performance standards, and service level agreements, as needed..

During M&O, the selected Offeror must monitor the day-to-day TPL Module operations.

At a minimum, the selected Offeror must:

1. Maintain current versions and licenses for all software, hardware, or other infrastructure.
2. Maintain backwards compatible versions of software.
3. Perform necessary upgrades to COTS products and components, if applicable.
4. Perform routine preventative maintenance.
5. Collaborate with the ITC/QA Contractor, other MMIS 2020 Platform module contractors, and the Department to create a standard schedule for maintenance activities.
6. Provide support for production both during work hours and outside of normal business hours, and coordinate with the Department for the level of expected support (e.g. what communication methods will be used outside of normal business hours and the expected response time).
7. Collaborate with other MMIS 2020 Platform contractors to perform defect triage, determining the severity of defects, responsibility, and resolution timeline.
8. Initiate work order to change or enhance the TPL module.

Deliverable: TPL Maintenance and Operations Plan

The Offeror must describe its approach to the design, development, implementation, and maintenance of the TPL Maintenance and Operations Plan.

N. TPL Technical Infrastructure Document. The selected Offeror must design, develop, implement, and maintain a Technical Infrastructure Document that describes all the hardware, system software, and tools necessary for each of the environments proposed, which includes:

1. A comprehensive system assets inventory (hardware, software, services, processes, configuration, etc.) preferably maintained and managed through a centralized Configuration Management Database ("CMDB") developed and hosted by the SI/DH Contractor.
2. A detailed product currency and license inventory preferably maintained and managed through a centralized CMDB, including:

a) List of all software licenses, current installations version, latest version (for each particular product), and next target installation version, such as upgraded Oracle to 11.2.0.4 version although the latest version is 12.c,
b) Software end-of-life; and,
c) Software end-of-support.

3. Network connectivity diagrams, including:
   a) Entire network diagram representing physical and logical links between nodes including servers, load balancers, firewalls, and,
   b) Secure boundary representation diagrams.
4. Network configuration inventory, preferably maintained and managed through a centralized CMDB, including:
   a) IP management (subnets, Virtual Local Area Networks ("VLANs"), IP assignment inventory, etc.);
   b) Network ports in use;
   c) Network protocols in use;
   d) Secure tunnels; and,
   e) Certificates.
5. Data flow diagrams, including:
   a) Node to node traffic (from data source to data destination), including all data repositories and pass-through systems involved; and,
   b) Between various logical elements of a particular unique solution or application (e.g. link between front-end and back-end elements).
6. Approach to capacity planning.

The selected Offeror must submit the TPL Technical Infrastructure Document to the Department for approval due one hundred (100) business days after the purchase order effective date and must update weekly thereafter.

Deliverable: TPL Technical Infrastructure Document

The Offeror must describe its approach to the design, development, implementation, and maintenance of the TPL Technical Infrastructure Document.

O. TPL System Design Document. The selected Offeror must design, develop, implement, and maintain the TPL System Design Document ("SDD"). An SDD is not necessary for COTS products, but an interface design document (including APIs) is required. The TPL SDD must include:

1. A list of all local and off-site facilities.
2. A network schematic showing all network components and technical security controls.
3. A description of each component, including basic functions and the business areas supported.
4. An enterprise system diagram, including all components, identifying all logic flow, data flow, systems functions, and their associated data storage.
5. A bi-directional traceability to requirements and test plan.

Deliverable: TPL System Design Document

The selected Offeror must submit its TPL SDD to the Department eighty (80) business days after the purchaser order effective date and update the eleven (11) business days after the GSD is approved by the Department for each MMIS 2020 Platform module.

The Offeror must describe its approach to the design, development, implementation, and maintenance of the System Design Document.

P. TPL Turnover Plan. Turnover is defined as those activities that the selected Offeror must perform at the end of the contract term, to turnover service delivery to a successor Offeror or to Commonwealth resources. During the turnover period, the selected Offeror must actively and cooperatively participate with the Department and its incoming contractor, if any. Offerors must submit a draft outgoing turnover plan with its Lot 2 Technical Submittal. The Offeror awarded a contract under Lot 2 of this RFP must provide the Department MMIS 2020 Project Manager and incoming contractor with all data, content, files, instructions, processes, and all other items deemed appropriate by DHS to successfully transition services and work effort. The selected Offeror must provide data in a format that is considered an industry-standard and approved by the Department MMIS 2020 Project Manager or designee.

The outgoing turnover plan must include at a minimum:

1. Data turnover tasks;
2. Custom interface turnover tasks;
3. Reusable code turnover tasks;
4. Documentation regarding files, interfaces, and work flows not considered to be part of the COTS proprietary documentation tasks; and,
5. A timeline with milestones for the TPL Turnover to include planning, execution, and implementation approval.

Additionally, the selected Offeror must develop an outgoing turnover plan when requested by the DHS MMIS 2020 Project Manager or designee. The outgoing transition plan must be reviewed and approved by the DHS MMIS 2020 Project Manager and stakeholders. Once approved by the DHS MMIS 2020 Project Manager, the selected Offeror must complete all activities included in the outgoing turnover plan within nine (9) months.

Deliverable: TPL Turnover Plan

The Offeror must describe their approach to the design, development, implementation, and maintenance of the TPL Turnover Plan.

II-17. Requirements

A. Disaster Recovery. The selected Offeror must develop and document a DR plan for approval by the Commonwealth that integrates with the Commonwealth's enterprise DR standards and timing objectives for electronic records and files relating to the TPL Module. The DR plan must comply with the following standards:

1. 24-hour Recovery Point Objective.
2. 36-hour Recovery Time Objective.
3. Encryption for data at rest.

In addition, the selected Offeror must:

1. Participate in and provide support for Commonwealth-led DR testing. In the event of a failed test, the selected Offeror must submit a Corrective Action Plan ("CAP") for review and approval. Once approved, the selected Offeror must retest the DR plan utilizing the approved CAP.

2. Review and test the DR Plan six (6) months after the purchase order effective date and every six (6) months thereafter, and provide the results to the Commonwealth.
3. .
4. Restore the TPL Module in the event of a system-wide outage, provide technical assistance to restore the MMIS 2020 Platform based on the Department's prioritized order of module restoration.

The DR plan must include at a minimum:

1. A procedure to return to limited twenty-five percent (**25%**) operation within twenty-four (24) hours of the DR event.
2. The ability to return to full operation within three (3) calendar days of the DR event.
3. A plan to confirm that the post-disaster software version is the same as before the disaster.
4. A procedure to confirm that pre-disaster data is not lost or corrupted.
5. A complete backup of all non-software data sets at the end of each production business day.
    a. The selected Offeror's datacenter architecture must consist of multiple geographically disbursed datacenters. Any datacenters being used in a back-up function must be at least fifty (50) miles apart from the associated primary location for the service. The selected Offeror must list the address of all datacenter locations from which the selected Offeror will provide the services. The plan must identify the backup sites.
    b. If the resultant backup media (for example, tapes and disks) are utilized, they must be removed to an external secure site. Back-up media must be cycled on a weekly basis.
    c. Upon the installation of any software (new or upgraded), a complete backup (copy) of the software must be made with the resultant backup media removed to an external secure site.
6. Servers must be designed to employ a method of redundancy for operational integrity and production.
7. All workstations attached to the network must have sufficient processing capability to be used interchangeably and must backup one another until repair or replacement can be affected.
8. The selected Offeror must utilize appropriate methods to achieve datacenter sustainability, such as realizing a low Power Usage Effectiveness ratio.
9. Servers must be connected to an Uninterrupted Power Supply system, which will condition incoming power to the server and provide sufficient processing time for the server to be correctly shutdown in the event of a power failure.
10. In the event of damage of a sufficient magnitude to the primary operational site, a second company location must be modified to accommodate the system.
11. The DR plan must include a description of the chain of communication and command, by level, in the case of a systems or power failure.
12. The selected Offeror must have a Business Continuity Plan to maintain business operations via a semi-automated or manual mode to mitigate complete disruption of services until systems have been restored to normal operating capacities.
13. In a datacenter environment that hosts both Commonwealth and non-Commonwealth clients, the selected Offeror must provide segregation of Commonwealth data and computing resources from other clients' data and computing resources. The selected Offeror is required to provide system and data segregation between different agency application environments.
14. Each datacenter must have the capability to provide DR for other datacenters for identified critical applications.

Deliverable: TPL DR Plan.

The selected Offeror must deliver the TPL DR Plan forty-three (43) business days days prior to the TPL Module implementation and must update annually. The TPL DR Plan will be reviewed with the monthly status report – see **Section II-18.C** of this RFP. The Offeror must describe how, by whom, and when its TPL DR

plan will be tested. The Offeror must describe how its TPL DR test plans support compliance with the required system availability as described in**, Section II-19. Performance Standards** of this RFP**.** The Offeror must also describe its approach to backing up the infrastructure to provide for continuity of operations.

B. Emergency Preparedness. To support continuity of operations during an emergency, including a pandemic or an event that causes major disruption in business or system operations, the Commonwealth needs a strategy for maintaining operations for an extended period of time. The strategy ensures that essential contractors that provide critical business services to the Commonwealth have planned for such an emergency and put contingencies in place to provide needed goods and services.

1. Describe how you anticipate such a crisis will impact your operations.
2. Describe your emergency response continuity of operations plan ("COOP"). Attach a copy of your plan, or at a minimum, summarize how your plan addresses the following aspects of preparedness:
   a. Employee training (describe your organization's training plan, and how frequently your plan will be shared with employees).
   b. Identification of essential business functions and key employees within your organization necessary to carry them out.
   c. Contingency plans for:
      i. How your organization will handle staffing issues when a portion of key employees are incapacitated.
      ii. How employees in your organization will carry out the essential functions if crisis control measures prevent them from coming to the primary workplace.
   d. How your organization will communicate with staff and suppliers when primary communications systems are overloaded or otherwise fail, including key contacts and chain of communications ("including suppliers").
   e. How and when your emergency plan will be tested, and if the plan will be tested by a third-party. Include a plan for corrective actions should the testing fail.

Deliverable: TPL COOP

The selected Offeror must deliver the TPL COOP forty-three (43) business days prior to the TPL Module implementation and must update the Plan annually.

C. Records Management. The selected Offeror must comply with records management requirements as defined in Management Directive 210.5 available at: http://www.oa.pa.gov/Policies/md/Pages/Management_AdministrativeSupport(205-260).aspx.

The selected Offeror will retain records until a time the Department determines that they qualify for disposition.

D. TPL Module Requirements Categories. Detailed requirements have been organized into three (3) categories: General, Technical and Functional. The selected Offeror's proposed solutions must demonstrate its alignment with the TPL Module detailed requirements. Offerors must respond to each individual requirement.

The requirements listed below represent the requirements for the TPL Module. Under the Department's strategic guidance, the ITC/QA Contractor will lead requirements gathering-related meetings including JAD sessions in collaboration with the selected Offeror, the SI/DH Contractor and other appropriate

MMIS 2020 Platform module contractors to finalize the TPL Module requirements. The results of the requirements collection will be consolidated into a BRD, and the requirements in the BRD will be cross walked to the CMS certification checklist and the TPL Module's RFP requirements.

The ITC/QA Contractor will complete a Business Gap Analysis to ensure the business requirements meet or exceed what is required for CMS certification, CMS and State regulations, and the Department's desired functionality. Offerors may propose additional requirements for consideration to achieve CMS certification.

E. General Requirements. The selected Offeror must meet the following general requirements for the TPL Module:

1. Provide a package of fully functional business processes that support the MMIS 2020 Platform requirements.
2. Provide a module for TPL that is independent and separate from other MMIS 2020 Platform modules or external solutions with the exception of shared data.
3. Provide a module that meets all CMS Medicaid Enterprise Certification Toolkit ("MECT") checklist requirements related to the TPL Module and that will achieve CMS certification.
4. Implement and operate, in the United States, your modular solution through software, data, and interoperable interfaces.
5. Provide, maintain, and host the necessary databases to run the COTS/MOTS package, custom product, or SaaS for the module.
6. Provide a product base of standard reports to operate, control, manage, and monitor the operations of the module's business processes.
7. Provide for customization of reports included in the module and additional reports defined by the Department to meet critical business needs.
8. Provide the capability for users to produce ad hoc reports based on the data processed and generated by the module.
9. Provide a configurable automated rules engine in the module for defining processing.
10. The selected Offeror must maintain code lists and reference files needed only by the selected Offeror's application. Data used by multiple modules will be housed in the ODS.
11. Maintain the code to its module and provide release updates that contain enhancements to the software. When practical, coordinate module enhancements through software updates with other states licensed to use its module.
12. Collaborate with the SI/DH Contractor, other module contractors, IV&V Contractor, ITC/QA Contractor, and the Commonwealth to ensure MMIS 2020 Platform success.
13. Collaborate with the SI/DH and module contractors to develop a module that accommodates phased-in TPL services consistent with the Department's overall MMIS 2020 Platform implementation plan.
14. Achieve and maintain HIPAA and CMS compliance in the TPL Module.
15. Collaborate with the SI/DH Contractor, other module contractors, IV&V Contractor, ITC/QA Contractor and the Department to complete data conversion for the TPL Module from the Legacy system.
16. Host a minimum of ten (10) years of MCA data converted from the legacy system via the SI/DH.

The corresponding CMS MECT 2.3 Checklist requirement numbers are OM.CL4.37, OM.CL1.15, IA.DMS.5, and S&C.MS.14, TA.FR.7 and TA.FR.8.

F. Technical Requirements. The selected Offeror must meet the following technical requirements for the TPL Module. CMS supplied MECT Version 2.3. The MECT checklist requirements support MMIS 2020 Platform certification processes and can be accessed at https://www.medicaid.gov/medicaid/data-and-systems/mect/index.html The corresponding MECT 2.3 Checklist requirement numbers have been included as applicable. Not all requirements will have an identified TPL-specific MECT 2.3 Checklist requirement.

1. The selected Offeror must utilize the guidance provided in the CMS's Minimum Acceptable Risk Standards for Exchanges, Version 2.0, and is responsible for providing a solution that meets all industry, state, and federal security standards. The selected Offeror must maintain, and make available at any time, security policies and procedures for each contractor and subcontractor module and location. At a minimum, the selected Offeror must provide for the security of the TPL Module in compliance with the following federal regulations and publications:

   a. 45 CFR § 95.621(f) ADP System Security Requirements and Review Process;
   b. Standards defined in Federal Information Processing Standards ("FIPS") issued by the National Institute of Standards and Technology ("NIST");
   c. NIST Special Publication 800-111 Storage Encryption Technologies for End User Devices;
   d. NIST Cryptographic Module Validation Program (https://csrc.nist.gov/Projects/cryptographic-module-validation-program);
   e. FIPS PUB 112 Password Usage Procedure;
   f. FIPS PUB 186-4 Digital Signature Standard, Published July 2013;
   g. 5 U.S.C. § 552a(o)(1)(F), (H) and (I) Records maintained on individuals;
   h. IRS Pub 1075;
   i. Privacy Act of 1974 at 5 U.S.C. 552a;
   j. Computer Matching and Privacy Protection Act of 1988 ("CMPPA");
   k. Federal Information Security Management ("FISMA");
   l. SSA Information System Security Guidelines for Federal, State, and Local Agencies;
   m. Child Online Privacy Protection Act ;
   n. Title XIX Confidentiality Rules;
   o. HIPAA;
   p. Administrative Simplification (HIPAA and ACA), including transactions and code sets, privacy, and security provisions;
   q. Federal security and privacy standards adopted by the DHHS Services for Exchanges;
   r. NIST 800-53 Assessing Security and Privacy Controls in Federal Information Systems and Organizations;
   s. Public Law 114-255 21st Century Cures Act Section 5006;
   t. Title XXI of the SSA;
   u. HITECH; and
   v. CRF Title 45 Part 164 Security and Privacy.

   The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.13, TA.SP.15, TA.SP.18, TA.SP.27, TA.SP.28, TA.SP.3, TA.SP.37, TA.SP.38, TA.SP.42, TA.SP.53, TA.SP.57, TA.SP.58, TA.SP.74, TA.SP.76, TA.SP.77, and IA.DS.21.

2. The selected Offeror must comply with all applicable Department and OIT security policies, including the following:

   a. Department security policies and standards: http://www.dhs.pa.gov/provider/busandtechstandards/secdomain/index.htm#.Vypl3HosimU

b. Department privacy policies and standards: http://www.dhs.pa.gov/provider/busandtechstandards/privdomain/index.htm#.VypmF3osimU
c. Commonwealth Security ITPs: http://www.oa.pa.gov/Policies/Pages/itp.aspx
    i. ITP_SEC031- Encryption Standards for Data in Transit;
    ii. ITP_SEC020- Encryption Standards for Data at Rest;
    iii. ITP_SEC016- Commonwealth of Pennsylvania – Information Security Officer Policy;
    iv. ITP_SEC014- Identity Protection and Access Management (IPAM) Architectural Standard – Identity Management Technology Standards;
    v. ITP_SEC013- Identity Protection and Access Management (IPAM) Architectural – Identity Management Services;
    vi. ITP-SEC-007- Minimum Standards for IDs and Passwords; and
    vii. Department encryption policies and standards: http://www.dhs.pa.gov/cs/groups/webcontent/documents/communication/p_031963.pdf

The corresponding CMS MECT 2.3 Checklist requirement number is TA.SP.38.

3. The selected Offeror must adhere to all pertinent federal security mandates, regulations, and standards including the following:
    a. 18 U.S.C. § 641: Public Money, Property or Records;
    b. 18 U.S.C. § 1905: Disclosure of Confidential Information;
    c. 21 CFR Parts 1-1499: Food and Drugs;
    d. 42 CFR Subchapter C: Medical Assistance Programs
    e. 42 CFR Subpart F: Safeguarding Information on Applicants and Beneficiaries
    f. 45 CFR Parts 160, 162.1301 and 164: Standards for Privacy of Individually Identifiable Health Information;
    g. American Recovery and Reinvestment Act of 2009 ("ARRA");
    h. Emergency Medical Treatment & Labor Act;
    i. Freedom of Information Act ("FOIA");
    j. OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems;
    k. The Deficit Reduction Act of 2005;
    l. The Patient Protection and Affordable Care Act of 2010 ("ACA"); and
    m. The Sarbanes-Oxley Act of 2002; and ISO 27001 and ISO 27002

    The corresponding CMS MECT 2.3 Checklist requirement numbers are S&C.ISC.6 and PL.RDM1.3..

4. The selected Offeror must implement a security architecture aligned with current MITA Security and Privacy model and other applicable architecture documents. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SOA.1 and TA.DAM.2

5. The selected Offeror's services and infrastructure must adhere to best practices and to Web Services security specifications and standards, as appropriate, including:
    a. Messaging
        i. Confidentiality & Integrity: WS-Security, SSL/TLS, XML Encryption;
        ii. Authentication: WS-Security Tokens, SSL/TLS X.509 Certificates, XML Signature;
    b. Resource

i. Authorization: Extensible Access Control Markup Language ("XACML"), extensible Rights Markup Language, Role Based Access Control, Attribute Based Access Control;
ii. Privacy: Enterprise Privacy Authorization Language, XACML;

c. Trust
i. Establishment: WS-Trust, XML Key Management, X.509;
ii. Trust Proxying: Security Assertion Markup Language, WS-Trust; Federation: WS-Federation, Shibboleth;

d. Security Properties
i. Policy: WS-Policy; Security Policy: WS-Security Policy; and
ii. Availability: WS-Reliability Messaging, WS-Reliability.

The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.BPM.4 and TA.DC.9.

6. The selected Offeror must provide for the effective integration of modular solutions, including COTS solutions, without requiring MMIS 2020 Platform contractors to make significant modifications to the inherent capabilities of their modules, including business rules engine and workflow. If a COTS solution does not provide a required function and a Department standard product preference exists, the selected Offeror must utilize the Department's solutions, standards or both. The corresponding CMS MECT 2.3 Checklist requirement number is TA.DAM.3.

7. The selected Offeror must adhere to Atomicity, Consistency, Isolation, Durability ("ACID") for the handling of transaction rollbacks, validity, and referential integrity checks,. No TPL-specific MECT 2.3 Checklist requirement has been identified.

8. The selected Offeror must support secure single sign-on**,** roles-based access by integrating with the Department's Identity and Access Management ("IDAM") Single Sign-on solution, CA SiteMinder. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.11, TA.SP.22, TA.SP.5, TA.SP.50, and TA.SP.51.

9. The selected Offeror must leverage the security roles defined by the Department. No TPL-specific MECT 2.3 Checklist requirement has been identified.

10. The selected Offeror must support access and role changes in real-time. No TPL-specific MECT 2.3 Checklist requirement has been identified.

11. The selected Offeror must provide a solution that is configurable to add users to multiple user groups. If conflicting access levels occur due to a user being in multiple user groups, the lowest access level will take precedence for a particular action. The corresponding CMS MECT 2.3 Checklist requirement number is TA.SP.51.

12. The selected Offeror must support the unique authentication credentials for each user gaining access to the system and must not support "group" or "corporate" logins. No TPL-specific checklist requirement has been identified.

13. The selected Offeror must provide the ability for a user to manually initiate a secure logout of the system from the external-facing portal. No TPL-specific checklist requirement has been identified.

14. The selected Offeror must support fine-grained access control, such as field-level access control, based on a user's role and privileges. No TPL-specific MECT 2.3 Checklist requirement has been identified.

15. The selected Offeror must provide the ability to define and implement fine-grained exclusion controls on a per-user basis. No TPL-specific MECT 2.3 Checklist requirement has been identified.

16. The selected Offeror will grant access to and from the DH using a unique user identifier (user ID) and user profile, combined with a strong password - following appropriate IDAM policy. The selected Offeror must be able to trace and audit any transaction or change to data by the module, down to the user ID level. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.24, TA.SP.70, IA.DS.18, and S&C.MS.4.

17. The selected Offeror must create, delete, modify, and assign role-based security to grant view and modify access to individual windows, reports, data elements, and field levels. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.BI.9, TA.SP.11, TA.SP.25, TA.SP.26, TA.SP.32, and TA.SP.50.

18. The selected Offeror must provide the capability to permit or restrict access to sensitive documents, generated forms, and other content based on a user's assigned security roles. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.BI.9, TA.SP.22, TA.SP.25, and TA.SP.32.

19. The selected Offeror must support authentication mechanisms for batch or web-based interfaces for data exchange with the federal government and other business partners. The corresponding CMS MECT 2.3 Checklist requirement number is S&C.IC.6

20. The selected Offeror must accommodate secure communications between Commonwealth business partners and the Commonwealth via multiple communication methods including email, text, and web portal, as defined by the Commonwealth. The corresponding CMS MECT 2.3 Checklist requirement number is TA.DC.10.

21. The selected Offeror must maintain policies and procedures for Commonwealth-mandated background checks and staffing controls, allowing the selected Offeror’s personnel access to Commonwealth-owned confidential information and to restricted areas within the selected Offeror’s host environment. Background checks are to be conducted annually and at the expense of the selected Offeror. No TPL-specific MECT 2.3 Checklist requirement has been identified.

22. The selected Offeror must provide audit logs as requested by the Department in a best of practice format or made compatible for integration to an advanced log correlator. The corresponding CMS MECT 2.3 Checklist requirement number is IA.DS.18

23. The selected Offeror must maintain a separate audit trail file for all transactions processed by the system, in a format that is logical and meaningful. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.39, IA.DS.18, and TA.LG.1.

24. The selected Offeror must capture root information on all changes to critical records and data fields (e.g., Identification Number and Name) that occur and publish this information to the ODS, including identification of the responsible system user and date and time of the change. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.27, TA.SP.37, and TA.SP.39.

25. The selected Offeror must have security audit trail reporting capabilities for a variety of criteria including security, level, locale, IP address, user ID, modification made and date/time. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.37, TA.SP.39, and IA.DS.18.

26. The selected Offeror must utilize automated utilities to review an appropriate subset of audit logs of system activity at least once weekly for unusual, unexpected, or suspicious behavior. The selected Offeror will inspect administrator groups on demand, and at least once every fourteen (14) calendar days, to detect the creation of any unauthorized administrator accounts. The selected Offeror will conduct manual reviews of system audit randomly on demand and must conduct at least once every thirty (30) calendar days. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.18 and TA.LG.1.

27. The selected Offeror must audit user login habits, restrict access, and notify the Department when anomalies are detected. The selected Offeror will produce reports of detected anomalies. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.38 and TA.SP.52.

28. The selected Offeror must generate and maintain audit logging that records user and system access to data to the data level. In addition, the selected Offeror must meet the audit log requirements mandated by all pertinent Department, Commonwealth, and federal guidelines, policies and standards. The corresponding CMS MECT 2.3 Checklist requirement number is IA.DS.18.

29. The selected Offeror must commission annual third-party auditing and security reviews of the TPL Module, including the SOC 3 report audit, and provide a copy of all audits, including dates they were conducted; to the Department. Audits must be conducted by an independent, third-party auditor. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.18 and IA.DS.18.

30. The selected Offeror must adhere to security and audit controls applying to storage, backup, retrieval, and viewing of archive data records including:
    a. Secure and encrypted storage;

b. Encrypted backups; and
c. Audit trails.

The corresponding CMS MECT 2.3 Checklist requirement number is IA.DS.18.

31. The selected Offeror must support file-based encryption of flat or XML files received from the SI/DH. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.BPM.4 and TA.DC.9.

32. The selected Offeror must support audit controls for hardware, software, and procedural mechanisms that record and examine activity in information systems that contain or use electronic Protected Health Information. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.10, TA.SP.18, TA.SP.36, TA.SP.7, and TA.SP.9.

33. The selected Offeror must provide for the configurable ability to encrypt both data at rest and data in motion. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.34 and TA.SP.72.

34. The selected Offeror must require message-level encryption (signed, encrypted messages) between system tier boundaries to mitigate against the risk of any one tier being compromised by malicious intent. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.34, TA.SP.41, and TA.SP.6.

35. The selected Offeror must provide transport-level encryption of data submitted from client to server devices using Secure Sockets Layer encryption over HTTP. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.14, TA.SP.35, TA.SP.6, TA.SP.7, TA.SP.70, and TA.SP.72.

36. The selected Offeror must provide encryption capabilities to secure the sensitive data (PII and PHI) stored. The encryption mechanisms will be determined based on the CMS requirements and standards. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.33 and TA.SP.5.

37. The selected Offeror must provide for database-level encryption at multiple levels (e.g., instance, tablespace, table and column). No TPL-specific MECT 2.3 Checklist requirement has been identified.

38. The selected Offeror must provide a reusable architecture service for the encryption and decryption of application-shared secrets/keys. No TPL-specific MECT 2.3 Checklist requirement has been identified.

39. The selected Offeror must provide security warning banners, headers and footers, adhering to federal, state and other applicable standards that are prominently displayed on all screens and reports, and must be readily customizable by Department staff. No TPL-specific MECT 2.3 Checklist requirement has been identified.

40. The selected Offeror must provide the ability to apply format masks to sensitive data that is displayed on the screen, including PHI and SSN. The corresponding CMS MECT 2.3 Checklist requirement number is TA.SP.14.

41. The selected Offeror will utilize a 2(+)-tier architecture with SOA, Web 2.0, XML capabilities, and SOAP and RESTful web services. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.BPM.4, TA.DC.9, and TA.SE.2.

42. The selected Offeror must store the information pertaining to the services available at particular endpoints in a machine-readable format in the service registry. The information must include the location of the service, routing information, failover protocols, and load balancing protocols in the service registry. No TPL-specific MECT 2.3 Checklist requirement has been identified.

43. The selected Offeror must provide the capability for a high volume of online and batch functions to run concurrently. The selected Offeror will coordinate module availabilities with the SI for batch processes with prerequisites and dependencies from several disparate systems and schedulers. Dependencies may include:
    a. Time of calendar day;
    b. Use of system; and
    c. Contingent timing of batches.

    No TPL-specific MECT 2.3 Checklist requirement has been identified.

44. The selected Offeror must provide on-demand reporting on the status of batch processes. No TPL-specific MECT 2.3 Checklist requirement has been identified.

45. The selected Offeror must assist the Department in establishing technical standards and governance for the MMIS 2020 Platform to align technical integration among disparate systems, as needed. This includes supplying technical data, providing access to engineering expertise, and operating a test bed against which teams can test and resolve integration issues. No TPL-specific MECT 2.3 Checklist requirement has been identified.

46. The selected Offeror's solution must support the ability to load data and quality check data in a variety of approaches including the following:
    a. Bulk data extraction and loading;
    b. Granular trickle-feed acquisition and delivery;
    c. Changed-data capture (ability to identify and extract modified data); and
    d. Event-based acquisition (time-based or data-value-based).

    No TPL-specific MECT 2.3 Checklist requirement has been identified.

47. In collaboration with the ITC/QA Contractor, SI/DH Contractor and MMIS 2020 Platform module contractors, the selected Offeror must conduct testing as systems and data are integrated into the SOA utilizing the ESB. No TPL-specific MECT 2.3 Checklist requirement has been identified.

48. The selected Offeror must coordinate with the SI/DH Contractor and ITC/QA Contractor to support testing across the MMIS 2020 Platform with regard to integration points between other modules and contractor-supported enterprise components. No TPL-specific MECT 2.3 Checklist requirement has been identified.

49. The selected Offeror must collaborate with the Department, the SI/DH Contractor and the ITC/QA Contractor to plan inter-system testing across the MMIS 2020 Platform Project to include documenting objectives, entrance criteria, scheduling, testing strategy, test procedures, resource identification, and exit criteria. No TPL-specific MECT 2.3 Checklist requirement has been identified.

50. The selected Offeror must coordinate with the Department, the SI/DH Contractor, The ITC/QA Contractor to participate in the execution of inter-project testing, including setup of shared resources, setup of instrumentation, conduct of the test, and documentation of anomalies. No TPL-specific MECT 2.3 Checklist requirement has been identified.

51. The selected Offeror must use automated tools to support TPL Module testing. No TPL-specific MECT 2.3 Checklist requirement has been identified.

52. The selected Offeror must provide a development environment, testing environment, and a training environment. No TPL-specific MECT 2.3 Checklist requirement has been identified.

53. The selected Offeror must coordinate with the SI/DH Contractor to achieve integration into the MMIS 2020 Platform. No TPL-specific MECT 2.3 Checklist requirement has been identified.

54. The selected Offeror must assist the Department in establishing the timing of cross-project "touch points," project-to-project timing dependencies, and other MMIS 2020 Platform project milestones. This includes the communication and coordination of inbound and outbound data that flows through the solution. No TPL-specific MECT 2.3 Checklist requirement has been identified.

55. The selected Offeror must supply the ITC/QA contractor all data conversion mapping for posting to the Artifact Library. The corresponding CMS MECT 2.3 Checklist requirement number is TA.DAM.3.

56. The selected Offeror must provide that any data transmitted into the system will maintain the appropriate metadata to be able to identify originating system (data owner) and data format. The corresponding CMS MECT 2.3 Checklist requirement number is IA.DMS.2

57. The selected Offeror must provide full, incremental, and transaction log backup and recovery capabilities

on both a regular schedule and an ad-hoc basis, including:

a. Redundant incremental off-site backups; and
b. Regularly scheduled demonstrations of back-up/restore capabilities.

No TPL-specific MECT 2.3 Checklist requirement has been identified.

58. The selected Offeror must store logs in a location that is accessible by both the selected Offeror and authorized Department staff. The retention period of transaction logs must be in accordance with federal, Commonwealth, and Department standards. No TPL-specific MECT 2.3 Checklist requirement has been identified.

59. The selected Offeror must align the solution with the planned modularity and configurability of the MMIS 2020 Platform, providing flexibility for application components that utilize web services to allow seamless and flexible communication between components and to support the removal of solutions and transfer of data as business needs evolve to plug-and-play into the DH. The corresponding CMS MECT 2.3 Checklist requirement number is IA.DS.10.

60. The selected Offeror will collaborate with the Department, ITC/QA Contractor and the SI/DH Contractor to design, develop, implement, and maintain the technical integrations and APIs used in the MMIS 2020 Platform Project. The corresponding CMS MECT 2.3 Checklist requirement number is TA.CM.4.

61. The selected Offeror must utilize XML W3C standards in the ESB message format, whenever possible, and must convert message formats and translate coded data within messages. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.BPM.4 and TA.DC.9.

62. The selected Offeror must leverage workflow and ESB orchestration to optimize data-related processes in the event-driven environment. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SOA.1 and TA.LG.2.

63. The selected Offeror must provide highly reusable, parameterized web services, requiring minimal or no customization that will enhance the ability to:
    a. Rapidly deploy applications; and
    b. Integrate legacy applications.

    No TPL-specific MECT 2.3 Checklist requirement has been identified.

64. The selected Offeror's solution must support the required inbound and outbound interfaces for the module through the SI/DH. No TPL-specific MECT 2.3 Checklist requirement has been identified.

65. The selected Offeror must provide that all inbound and outbound interfaces comply, as necessary, with National Information Exchange Model, NIST, HIPAA-compliant standards and other applicable standards. The corresponding CMS MECT 2.3 Checklist requirement number is TA.DAM.2

66. The selected Offeror's solution must support uninterrupted functionality during database backup windows including hot-backup or dynamic backup. No TPL-specific MECT 2.3 Checklist requirement has been identified.

67. The selected Offeror must provide the ability for concurrent users to simultaneously view the same record, documentation and template via the web interface. No TPL-specific MECT 2.3 Checklist requirement has been identified.

68. The selected Offeror's solution must allow reference data to be viewed, loaded and edited by the authorized Department users. No TPL-specific MECT 2.3 Checklist requirement has been identified.

69. The selected Offeror must utilize a configuration such that changes to modular data must remain in synchronization with the ODS. No TPL-specific MECT 2.3 Checklist requirement has been identified.

70. The selected Offeror must collaborate with the SI/DH and across modules to establish the data architecture and processes for data management of the ODS. The corresponding CMS MECT 2.3 Checklist requirement numbers is IA.DMS.4.

71. The selected Offeror must reconcile all data elements found in the ODS. The corresponding CMS MECT 2.3 Checklist requirement number is TA.DAM.7.

72. The selected Offeror must leverage all common code values maintained by the SI/DH Contractor. No TPL-specific MECT 2.3 Checklist requirement has been identified.

73. The selected Offeror must utilize standard industry code sets, using only the most current versions of these code sets or as approved by the Department. No TPL-specific MECT 2.3 Checklist requirement has been identified.

74. The selected Offeror must support at least the following types of transformation:
    a. Simple transformations such as data-type conversions, string manipulations and simple calculations;
    b. Moderate-complexity transformations such as lookup and replace operations, aggregations, summarizations, deterministic matching, and management of slowly changing dimensions;
    c. Higher-order transformations, such as sophisticated parsing operations on free-form text and rich media facilities for developing custom transformations and extending packaged transformations; and,
    d. Facilities for developing custom transformations and extending packaged transformations.

    No TPL-specific MECT 2.3 Checklist requirement has been identified.

75. The selected Offeror must utilize a Relational Database Management System to support OLTP, batch processing, mixed workloads and business intelligence. The corresponding CMS MECT 2.3 Checklist requirement number is TA.BI.7.

76. The selected Offeror must provide advanced configurations for data caching including support of client/application caching and support of server caching. No TPL-specific MECT 2.3 Checklist requirement has been identified.

77. The selected Offeror must provide the ability to operate on a real-time basis. TPL-specific MECT 2.3 Checklist requirement has been identified.

78. The selected Offeror must provide a normalized core data model or data object model, making proper use of primary, foreign keys, indexes, constraints and domain-based data types. The corresponding CMS MECT 2.3 Checklist requirement number is IA.LDM.5

79. The selected Offeror must utilize Entity Relationship/Object Modeling Integration in order to synchronize logical, physical and object models. No TPL-specific MECT 2.3 Checklist requirement has been identified.

80. The selected Offeror must provide built-in utilities to the Database Management Solution ("DBMS") to automate the normal day-to-day database administrator operations (e.g., automated index rebuilding, free space reclamation, and block reorganization). No TPL-specific MECT 2.3 Checklist requirement has been identified.

81. The selected Offeror must support native geospatial data types. No TPL-specific MECT 2.3 Checklist requirement has been identified.

82. The selected Offeror must support various database connectivity protocols including Open Database Connectivity, Java Database Connectivity, and Object Linking and Embedding database protocol. No TPL-specific MECT 2.3 Checklist requirement has been identified.

83. The selected Offeror must provide an underlying DBMS, so it is also available as a standalone query-able DBMS. No TPL-specific MECT 2.3 Checklist requirement has been identified.

84. The selected Offeror's solution must preserve committed transactions in a manner so no greater than one (1) minute of committed transaction data is lost as the result of an unplanned interruption to services or a reduction in the quality of services. No TPL-specific MECT 2.3 Checklist requirement has been identified.

85. The selected Offeror must collaborate and contribute to project management activities including status reporting, meetings, risk/issue management, and project planning as defined and managed by the ITC/QA Contractor and the Department. No TPL-specific MECT 2.3 Checklist requirement has been identified.

86. The selected Offeror must collaborate with the Department and the ITC/QA Contractor to manage the Change Management process. No TPL-specific MECT 2.3 Checklist requirement has been identified.

87. The selected Offeror must collaborate and contribute to release management and release planning activities (testing requirements, training impacts, promotion schedule) as defined and managed by the SI/DH Contractor, the ITC/QA Contractor and the Department. No TPL-specific MECT 2.3 Checklist requirement has been identified.

88. The selected Offeror must provide for the performance/latency of the connectivity to module system(s) such that the required performance (e.g., asynchronous and background messaging when a user action results in communications with other systems) is not adversely affected. No TPL-specific MECT 2.3 Checklist requirement has been identified.

89. The selected Offeror must establish processes to address future Commonwealth or federal regulations and requirements (e.g., Direct Secure Messaging for the exchange of PII and PHI between covered entities). The corresponding CMS MECT 2.3 Checklist requirement number is TA.SP.14.

90. The selected Offeror must send and accept batch and real-time representation of applicable HIPAA mandated and other standard health care transactions. The information exchanged will support a variety of formats, including X12, NCPDP, XML, and JSON formats. The corresponding CMS MECT 2.3 Checklist requirement numbers are IA.DS.11, TA.SP.16, and TA.SP.17.

91. The selected Offeror must support the ability for pre-generated performance standards related reports to be designed so that they can be rendered for online viewing in under five (5) seconds. The Offeror's module must trigger an alert for performance outside of performance standards parameters and provide a link to the SLA-related reports online and accessible from a remote location. Additionally, performance data will be sent back to the SI/DH Contractor for inclusion in SI/DH MMIS 2020 Platform dashboards. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.BI.4, TA.FR.6, TA.PM.8, and TA.DC.7.

92. The selected Offeror must provide the ability to configure alerts, including:
    a. Alert thresholds;
    b. Alert notification channels; and
    c. Ability to turn alerts on or off the module's performance monitoring capabilities.

    The corresponding CMS MECT 2.3 Checklist requirement number is TA.DC.7.

93. The selected Offeror must host the TPL Module and meet federal and Commonwealth standards (described in **Part I-31**) including required performance, security and data retention standards. No TPL-specific MECT 2.3 Checklist requirement has been identified.

94. The selected Offeror must provide a hosting solution that is sufficiently flexible in dealing with unavoidable circumstances, such as burst, cyclical, peak, and seasonal capacity demands or security and regulatory changes. No TPL-specific MECT 2.3 Checklist requirement has been identified.

95. The selected Offeror must provide a hosting environment for all system environments that is compliant with SOC 3. No TPL-specific MECT 2.3 Checklist requirement has been identified.

96. The selected Offeror must utilize architecture with no single point of failure, supporting fault tolerance and failover of web, application, database servers, storage devices, and secondary devices such as load balancers, and supporting a high-availability enterprise. No TPL-specific MECT 2.3 Checklist requirement has been identified.

97. The selected Offeror must provide redundancy so that accessibility, reliability/fault tolerance and performance are within defined SLA parameters. No TPL-specific MECT 2.3 Checklist requirement has been identified.

98. The selected Offeror must enumerate the prioritized order of restoration for MMIS 2020 Platform modules in the event of a system-wide outage. No TPL-specific MECT 2.3 Checklist requirement has been identified.

99. The selected Offeror must sync planned outage windows to the greatest extent possible with all pertinent stakeholders and schedules that may affect or be affected by the MMIS 2020 Platform, including:
    a. The Commonwealth;
    b. Department maintenance schedule;
    c. MMIS 2020 Platform modules; and
    d. SI/DH Contractor.

    No TPL-specific MECT 2.3 Checklist requirement has been identified.

100. The selected Offeror must communicate and coordinate with the Department in the event of an outage due to an emergency within fifteen (15) minutes of the identification of the outage. No TPL-specific MECT 2.3 Checklist requirement has been identified.

101. The selected Offeror must maintain proper power and cooling, including redundant power and cooling, to safeguard all hardware, software, and state-owned data. The corresponding CMS MECT 2.3 Checklist requirement number is TA.SP.61.

102. The selected Offeror must perform technical tasks, including:
    a. Creating application server domains;
    b. Deploying applications or components;
    c. Monitoring and configuring the performance of the application server domain;
    d. Diagnosing and troubleshooting problems;
    e. Maintain operating system to latest Department-approved version;
    f. Maintain current infrastructure documentation; and

g. Coordinate infrastructure changes with other contractors to minimize impact.

No TPL-specific MECT 2.3 Checklist requirement has been identified.

103. The selected Offeror must support an orientation of business processes, business rules, data, and metadata management that allows a modular, componentized design approach that enhances interoperability across service modules and with external applications and data sources. The corresponding CMS MECT 2.3 Checklist requirement numbers are IA.DMS.2, IA.DS.9, and S&C.MS.2.

104. The selected Offeror must collaborate with MMIS 2020 Platform module contractors to maintain and synchronize all rules. If the TPL Module has its own Business Rules Engine ("BRE"), the selected Offeror must export and support the load of these rules in the central location on the SI/DH for the MMIS 2020 Platform. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.DM.1 and S&C.MS.10.

105. The selected Offeror must store TPL Module specific rules in the TPL Module for access by authorized user(s). The storage of business rules in the TPL Module must support granular check-out and check-in rules and an audit trail of business rules changes. No TPL-specific MECT 2.3 Checklist requirement has been identified.

106. The selected Offeror must provide a rules engine which allows the rules to be tested against (de-identified) production data, such as encounter processing data, in a non-production environment prior to deployment of the rules. No TPL-specific MECT 2.3 Checklist requirement has been identified.

107. The selected Offeror must provide the ability for the workflow engine to capture business processes using Business Process Model and Notation 2.0 or later, even if the engine uses a separate coding of the rules for execution. The corresponding CMS MECT 2.3 Checklist requirement number is S&C.MS.18.

108. The selected Offeror must streamline large sets of similarly structured rules with decision tables. No TPL-specific MECT 2.3 Checklist requirement has been identified.

109. The selected Offeror must provide for access to the most current rules during rule authoring and at execution time without recompiling code. No TPL-specific MECT 2.3 Checklist requirement has been identified.

110. The selected Offeror must provide the ability to rollback to prior versions of rules with minimal system impact. No TPL-specific MECT 2.3 Checklist requirement has been identified.

111. The selected Offeror must provide the ability for business rules execute in a real-time environment. No TPL-specific MECT 2.3 Checklist requirement has been identified.

112. The selected Offeror must provide the ability to maintain and display the history of each rule change in the rules engine. This history will show previous versions of the rule, a timestamp of when the change was made, a narrative box describing the change, and the identification of the user making the change. No TPL-specific MECT 2.3 Checklist requirement has been identified.

113. The selected Offeror must provide a rules editor that maintains the current version of standardized business rules' definitions in a language that business people can interpret and includes the ability to easily edit the rules. The module must transform the rules into system language for processing. The corresponding CMS MECT 2.3 Checklist requirement number is TA.DM.2.

114. The selected Offeror's informational technology solution must use production or inference rules to represent behaviors (e.g., IF THEN conditional logic). No TPL-specific MECT 2.3 Checklist requirement has been identified.

115. The selected Offeror must be able to send work objects to other MMIS 2020 Platform modules via the DH, add received work objects to workflow queue, and return updates, including a closure of the work object back to the originating modules' workflow engine. No TPL-specific MECT 2.3 Checklist requirement has been identified.

116. The selected Offeror must support the saving of incomplete data sets for completion of the workflow at a later time. No TPL-specific MECT 2.3 Checklist requirement has been identified.

117. The selected Offeror must enable central workflow and transactional status alerts. The selected Offeror must centralize pending work items for the user in a "work queue." No TPL-specific MECT 2.3 Checklist requirement has been identified.

118. The selected Offeror's solution must support the pushing of messages to intended workers without requiring them to inquire specifically for the data. The corresponding CMS MECT 2.3 Checklist requirement number is TA.SOA.2.

119. The selected Offeror's module windows and screens must be intuitive, easy to use, based on workflows, maintain the appropriate and relevant context, and offer multi-channel assistance. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.CS.10, TA.CS.14, and TA.CS.17.

120. The selected Offeror's module windows and screens must be compliant with Section 508 of the Rehabilitation Act of 1973 to meet the needs of diverse populations of users, including those with visual and hearing impairments, persons with low and moderate educational levels, and the elderly. Information on Section 508 can be accessed here: http://www.section508.gov. The corresponding CMS MECT 2.3 Checklist requirement number is TA.CS.18.

121. The selected Offeror must provide user experience personalization and customization capabilities for each user, including allowing users to specify precisely what they want, including choosing the font size, display colors, and information elements on a home page. No TPL-specific MECT 2.3 Checklist requirement has been identified.

122. The selected Offeror's solution must support the timeout of a user session after a specified period. The timeout period must be configurable by user type and module, minimally allowing different values for the public website and the internal website while meeting security rules. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.SP.38, TA.SP.5, and TA.SP.54.

123. The selected Offeror's solution must support the ability of the website, wherever appropriate, to show progress through the use of Progress Bars. No TPL-specific MECT 2.3 Checklist requirement has been identified.

124. The selected Offeror must support session management capabilities to support user sessions and coordinated back-end application functionality. No TPL-specific MECT 2.3 Checklist requirement has been identified.

125. The selected Offeror must provide time-based content expiration and version management capabilities. No TPL-specific MECT 2.3 Checklist requirement has been identified.

126. The selected Offeror must provide the ability for a user to see, at configurable periods prior to session timeout, a message that warns them of the imminent timeout such as a five [5] minute notice, and they must be able to click this message and keep their server session active. No TPL-specific MECT 2.3 Checklist requirement has been identified.

127. The selected Offeror's solution must support most current versions of major browsers for devices that include the most popular operating system brands (i.e., Android, Macintosh, and Windows) without requiring specialized plug-ins or applets to function. The corresponding CMS MECT 2.3 Checklist requirement number is TA.CS.6.

128. The selected Offeror's solution must support the printing of items directly from the browser and allow internal users to queue items to print either locally or via batch. No TPL-specific MECT 2.3 Checklist requirement has been identified.

129. The selected Offeror must provide an accessibility testing solution that incorporates the use of assistive technologies. The solution must be validated through the use of Compliance Sheriff. The corresponding CMS MECT 2.3 Checklist requirement number is TA.CS.18.

130. The selected Offeror must provide screens for data entry with identified mandatory and optional data fields, including basic validations on data entry such as recognizing invalid characters or an incorrect number of

characters. The corresponding CMS MECT 2.3 Checklist requirement numbers are TA.FR.1, TA.SP.1, and TA.SP.2.

131. The selected Offeror must collect and collate statistics on TPL Module usage to support reporting requirements and continuous improvements in design. The corresponding CMS MECT 2.3 Checklist requirement number is TA.PM.6.

132. The selected Offeror must utilize web statistics that capture the entry screens, exit screens, IP addresses, application abandonment frequency/location, logon duration, session timeouts, time on each page, and keyword searches. No TPL-specific MECT 2.3 Checklist requirement has been identified.

133. The selected Offeror must provide a Capacity Planning approach that incorporates the use of a performance monitoring system for planning, sizing, and controlling capacity as needed. The corresponding CMS MECT 2.3 Checklist requirement number is TA.PM.5.

134. The selected Offeror must propose one (1) or more COTS monitoring tools to proactively monitor the performance, track progress, and facilitate decision making of key application components and services of the proposed solution and alert system administrators to instances of performance outside of acceptable thresholds as defined by pertinent service level agreements. The corresponding CMS MECT 2.3 Checklist requirement number is TA.DC.7.

135. The selected Offeror must provide, configure, and operate COTS tool(s) to monitor Key Performance Indicators ("KPIs") metrics and diagnostic information, including response time, resource availability, CPU utilization, error detection, network connectivity interruptions, database servers going offline, and memory utilization thresholds via a dashboard. The selected Offeror must provide Department staff with on-demand access to utilize this tool. The corresponding CMS MECT Checklist requirement numbers are TA.PM.7 and TA.PM.8.

136. The selected Offeror's solution must send alerts through email, SMS, and CRM based on all monitored attributes. No TPL-specific MECT 2.3 Checklist requirement has been identified.

137. The selected Offeror must provide a performance dashboard(s) of a wide range of application services and network services providing the ability to drill down to a level where the observations provide useful information and both real-time and snapshot views. The corresponding CMS MECT 2.3 Checklist requirement number is TA.BI.5.

138. The selected Offeror must maintain availability and user access to the module twenty-four (24) hours a day, seven (7) days a week, three hundred sixty-five (365) days a year, with the exception of planned downtime due to system upgrades or routine maintenance. The selected Offeror must communicate and coordinate all planned downtime and maintenance outages with the Department at least ten (10) business days in advance for Department approval. The notification must include the date and time of the planned maintenance along

with the anticipated time the module will be offline and unavailable. No TPL-specific MECT 2.3 Checklist requirement has been identified.

139. The selected Offeror must develop a standard maintenance page viewable during downtimes. The Department must have the ability to launch this page. No TPL-specific MECT 2.3 Checklist requirement has been identified.

140. The selected Offeror must utilize virtualization, where possible, in design and be prepared to create virtualized secured environments that are highly available, sustainable, extendible, and portable across hardware platforms. No MCA-specific MECT 2.3 Checklist requirement has been identified.

141. The selected Offeror must provide for the search and retrieval of historical data for all types of data. Data retrieved must include only the targeted files and documents. No TPL-specific MECT 2.3 Checklist requirement has been identified.

142. The selected Offeror must provide a presentation of searches that result in multiple pages of data in small groups of data with Next/Back paging capability. Page numbers must be displayed. No TPL-specific MECT 2.3 Checklist requirement has been identified.

143. The selected Offeror must provide flexible, adaptable technology to support the ongoing changes to business processes due to evolving federal and Department regulations and requirements. No TPL-specific MECT 2.3 Checklist requirement has been identified.

144. The selected Offeror must configure and implement the solution with the purpose of optimizing long-term maintenance and operations efforts (i.e., build for lowest cost long-term operational costs). No TPL-specific MECT 2.3 Checklist requirement has been identified.

145. The selected Offeror must maintain adequate technical support and staffing to provide twenty-four (24) hour a day, seven (7) days a week, three hundred sixty-five (365) days a year hosting services. The selected Offeror's solutions may be hosted or cloud-based, but offshore hosting is not acceptable. No TPL-specific MECT 2.3 Checklist requirement has been identified.

146. The selected Offeror's solution may be hosted or cloud-based, but offshore hosting is not acceptable; however, offshore development is permitted provided Department-specific data is not used. No TPL-specific MECT 2.3 Checklist requirement has been identified.

147. The selected Offeror must provide a graphical representation of reporting data as defined by the Department. No TPL-specific MECT 2.3 Checklist requirement has been identified.

148. The selected Offeror's solution must export reporting information into Excel or other formats as defined by the Department. The corresponding CMS MECT 2.3 Checklist requirement number is TA.FR.4.

G. Functional Requirements. This section details the functional requirements that the selected Offeror's TPL Module must meet. Offerors must propose a solution that demonstrates its alignment with the detailed functional requirements.

1. The selected Offeror must operate and maintain the TPL Module processing functionality related to the MMIS 2020 Platform to support the needs of the Department and the requirements of federal and state regulations. No TPL-specific MECT 2.3 Checklist requirement has been identified.

2. The selected Offeror's module must provide TPL services in accordance with all applicable federal and state laws, regulations, and policies, including any changes to law, regulations, or policies. The corresponding CMS MECT 2.3 Checklist requirement number is S&C.ISC.7.

3. The selected Offeror's module must validate the consistency of TPL data across all modules (e.g., TPL, Pharmacy, MCO, Provider and Eligibility) and provide real-time updates as they are received. The module must reconcile data between internal modules on a predetermined schedule and maintain synchronicity of all data. The corresponding CMS MECT 2.3 Checklist requirement number is FM.TPL1.7.

4. The selected Offeror's module must utilize a web-based platform that supports a paperless environment where all documentation received and generated is stored. The Offeror must describe how its solution meets this need. No TPL-specific MECT 2.3 Checklist requirement has been identified.

5. The selected Offeror's module must be scalable to meet future Departmental business needs. No TPL-specific MECT 2.3 Checklist requirement has been identified.

6. The selected Offeror's module must provide an audit trail of changes by user and date. The corresponding CMS MECT 2.3 Checklist requirement numbers are FM.DSS.11.3, OM.TPL1.4, and PL.RDM1.12.

7. The selected Offeror's module must accept imaged files of paper documents and convert to a specific format. The Offeror must explain the maximum file size of an imaged document the proposed module can accept. No TPL-specific MECT 2.3 Checklist requirement has been identified.

8. The selected Offeror's module must accept data, messages, and files from trading partners. Data, messages, and files will be accepted by the DH, scanned for viruses, and sent to the TPL Module. Partners include:
    a. MCOs;
    b. Insurance carriers;
    c. Department agencies (e.g., Department of Revenue, Department of Military and Veterans Affairs, ~~Bureau of Child Support Enforcement (PACSES),~~ Department of Health);
    d. Other State Governmental agencies;

e. Federal agencies (CMS, US Postal Service to standardize address information);
f. Medicare carriers/intermediaries; and,
g. Coordination of Benefits contractors.

No TPL-specific MECT 2.3 Checklist requirement has been identified.

9. The selected Offeror's module must accept narratives on all recovery records and create system-generated narratives based on TPL activities. The module must support a process ensuring that narratives are sortable by date, time, user, and other unique identifiers. No TPL-specific MECT 2.3 Checklist requirement has been identified.

10. The selected Offeror must support all data conversion from TPL systems. No TPL-specific MECT 2.3 Checklist requirement has been identified.

11. The selected Offeror must maximize the opportunities for recovery by offering industry best practices and recommendations. The corresponding CMS MECT 2.3 Checklist requirement number is S&C.ISC.10.

12. The selected Offeror's module must provide on-line, real-time access to TPL and TPL-related data. No TPL-specific MECT 2.3 Checklist requirement has been identified.

13. The selected Offeror's module must allow the type of TPL recovery to be identified in the claim's history file. No TPL-specific MECT 2.3 Checklist requirement has been identified.

14. The selected Offeror's module must provide the ability to sort, filter, and display all TPL-related data elements. No TPL-specific MECT 2.3 Checklist requirement has been identified.

15. The selected Offeror's module must accept, process, and maintain the following data inputs from the SI/DH including:

    a. Recipient TPL resource data stored in CIS;
    b. Cost avoidance matrix;
    c. TPL-related claim record;
    d. Parameters used to identify potential recovery claims;
    e. Monthly file from Department of Revenue regarding probate estates;
    f. Deceased recipient data from CIS;
    g. Encounter data from MCOs;
    h. Weekly file of COBRA claims (mandatory pay and chase);
    i. TPL vendor files of unduplicated claims;
    j. Reconciliation file for COBRA claims billed by TPL vendor;
    k. Reconciliation file from TPL vendor;
    l. Coverage codes;
    m. Improved analytics and accuracy of encounter data;

n. Capture accurate encounter and claims data; including a process to request a file via the DI/SH for unsubmitted encounter data from the MOCs for selected recipients.
o. CIS purged data (virtual tape); and,
p. Reference data from the SI/DH.

No TPL-specific MECT 2.3 Checklist requirement has been identified.

16. The selected Offeror's solution must support the following query and reporting outputs, including:
    a. Cost avoidance summary report;
    b. List of cost-avoided claims;
    c. Questionnaires for recovery cases, Trauma Code Tracking ("TCT"), and estate;
    d. List of potential recovery claims and encounters to support the statement of claim process and the recovery of claims (e.g., Commercial, Medicare);
    e. Cost recovery reports;
    f. TPL provider invoices;
    g. TPL-related letters and notices;
    h. Provider-reported third-party payments sorted by Medicare and commercial resources for each invoice type by category and program status codes of recipient groups;
    i. All required files for the Contingency Fee Contractor; and
    j. Financial reports detailing cost avoidance and recovery activities including:
        i. Gross adjustments
        ii. Duplicate rejects
        iii. Reconciliation reports for approved claims previously rejected

    No TPL-specific MECT 2.3 Checklist requirement has been identified.

17. The selected Offeror's module must allow authorized users print capability to generate and edit TPL reports in formats, as requested by the Department. No TPL-specific MECT 2.3 Checklist requirement has been identified.

18. The selected Offeror's module must identify, capture, report, maintain, and track TPL Coordination of Benefits ("COB") activities. The corresponding CMS MECT 2.3 Checklist requirement numbers are FM.DSS1.7, FM.ME2.1, and FM.TPL1.3

19. The selected Offeror must assist the Department in identifying creative methods for TPL recoveries. No TPL-specific MECT 2.3 Checklist requirement has been identified.

20. The selected Offeror's module must identify, invoice, receive, and reconcile insurance premium payments by recipients; support "buy-in" to employer or Department-operated benefit packages (e.g., Children's Health Insurance Program); and allow for recipient co-pay based on a sliding payment scale. The corresponding CMS MECT 2.3 Checklist requirement numbers are FM.DSS4.2 and FM.CM24.2

21. The selected Offeror's module must create detail and summary reports of premiums paid, recipient deductibles, and coinsurance paid by Medicaid on behalf of the recipient. The corresponding CMS MECT 2.3 Checklist requirement number is FM.DSS1.11.

22. The selected Offeror's module must manage accounts receivables identified as Statement of Claims and claims adjustments as TPL-related invoices are paid. The corresponding CMS MECT 2.3 Checklist requirement number is FM.TPL2.14.

23. The selected Offeror's module must support real-time queries to recipient eligibility, claims/encounters history, capitation rate history, and premium history to support TPL recoveries. The source of this data may be retrieved from other MMIS 2020 Platform modules via the SI/DH and transmitted to the TPL Module. The corresponding CMS MECT 2.3 Checklist requirement number is ME.PH1.1.

24. The selected Offeror's module must provide for automated TPL recovery tracking (within module) and support a process to send updates to the Fee-for-Service Module to flag claim history as TPL recovered. The source of this data may be posted to other MMIS 2020 Platform modules via the SI/DH and transmitted to the TPL Module. No TPL-specific MECT 2.3 Checklist requirement has been identified.

25. The selected Offeror's module must convert Julian date to Gregorian date and vice versa as defined by the Department. No TPL-specific MECT 2.3 Checklist requirement has been identified.

26. The selected Offeror's module must have the ability to archive historical data as defined by the Department. No TPL-specific MECT 2.3 Checklist requirement has been identified.

27. The selected Offeror's module must provide users with query capability to all reference data maintained in the system (e.g., procedure codes, diagnosis, NDC, provider). No TPL-specific MECT 2.3 Checklist requirement has been identified.

28. The selected Offeror's module must provide the ability for multiple concurrent functional windows to be opened at the same time. No TPL-specific MECT 2.3 Checklist requirement has been identified.

29. The selected Offeror's module must allow for authorized Commonwealth staff to create and modify all default settings (e.g., Workers' Compensation at 20% lien reduction, letter type, hardship waiver closing reason). No TPL-specific MECT 2.3 Checklist requirement has been identified.

30. The selected Offeror's module must display at a minimum the last fifteen (15) records accessed by the user. No TPL-specific MECT 2.3 Checklist requirement has been identified.

31. The selected Offeror's module must open a case after TPL notification that includes the following functionality:
    a. Maintain the date and time of any action taken on the case;

b. Maintain a chronological order of all events that have occurred for each case;
c. Identify when cases require action or follow-up;
d. Identify cases based upon criteria specified by Department; and,
e. Maintain a complete audit trail and activity log of every transaction and provide the capability to query this information.

The corresponding CMS MECT 2.3 Checklist requirement numbers are FM.DSS11.3 and OM.CL3.4.

32. The selected Offeror's module must generate Department-specified alerts to individual users or a group of users (e.g., not reviewed scanned documents, unprocessed checks). No TPL-specific MECT 2.3 Checklist requirement has been identified.

33. The selected Offeror's module must provide workflow functionality that facilitates the distribution of assignments to users and supervisor re-assignment capability to other users. No TPL-specific MECT 2.3 Checklist requirement has been identified.

34. The selected Offeror's module must generate data for the sending and receipt of emails and faxes via the SI/DH to the OBM Module; read incoming faxes using technology to identify and associate with appropriate case files or drop to a manual review; and scan all documents, as they were originally received, including all color font and highlighting. No TPL-specific MECT 2.3 Checklist requirement has been identified.

35. The selected offeror's module must provide the ability to track and accumulate TPL recovery amounts. No TPL-specific MECT 2.3 Checklist requirement has been identified.

36. The selected Offeror's module must track and monitor claim adjustments initiated in other MMIS 2020 modules related to a specific TPL case. No TPL-specific MECT 2.3 Checklist requirement has been identified.

37. The selected Offeror's module must provide an activity log that includes all transactions completed by the user with date and time for a specific time frame, and it must provide the ability for authorized users to access this information in real time. No TPL-specific MECT 2.3 Checklist requirement has been identified.

38. The selected Offeror's module must maintain an online system for quality assurance audit controls. No TPL-specific MECT 2.3 Checklist requirement has been identified.

39. The selected Offeror's module must generate and support standard and ad-hoc reports based on a schedule of any available data fields and provide print capabilities to authorized users to generate TPL reports in formats including Excel and XML. Output reports must be in a format that allows printing. Reports must be generated based on a schedule to be determined during JAD sessions (e.g., weekly reports generated each Monday by 9am). The selected Offeror must ensure accuracy of all TPL reports generated. No TPL-specific MECT 2.3 Checklist requirement has been identified.

40. The selected Offeror's module must provide the following production reports and allow on-demand access to the reports and corresponding information to include:
    a. Number of active cases;
    b. Number of cases opened;
    c. Number of cases closed;
    d. Number of cases closed by user and reason for closing;
    e. Summary report of cases by claim type or referral source;
    f. Number of cases filed with the court;
    g. Number of cases by incident type;
    h. Outstanding claim balance of all open cases;
    i. Number of cases by attorney, insurance company, or title company;
    j. Number of cases assigned to each staff person;
    k. Number of undue hardship waiver requests for estates;
    l. Number of denied undue hardship waiver requests for estates;
    m. Number of granted undue hardship waiver requests for estates and value of asset waived;
    n. Number of estate cases marked for delayed recovery;
    o. Source of payment summary report; and,
    p. "Follow up" reports.

    The corresponding CMS MECT 2.3 Checklist requirement number is FM.DSS1.11.

41. The selected Offeror must support the Department in developing and enhancing reporting and accuracy of data. No TPL-specific MECT 2.3 Checklist requirement has been identified.

42. The selected Offeror's solution must generate and produce all user-defined standardized and ad-hoc reports as specified by the Department on a schedule and in a format defined by the Department, including:
    a. Aging reports that include details of the type and reason for recovery, and monetary value;
    b. Recovery Report by case type; and,
    c. Casualty and estate reports through the TPL case management system.

    No TPL-specific MECT 2.3 Checklist requirement has been identified.

43. The selected Offeror must ensure accuracy of all TPL reports generated for the Department, users, Commonwealth agencies, and federal agencies. No TPL-specific MECT 2.3 Checklist requirement has been identified.

44. The selected Offeror's module must provide functionality to query data relevant to TPL and recoveries. The corresponding CMS MECT 2.3 Checklist requirement number is FM.DSS3.7.

45. The selected Offeror's module must allow users to create a recovery case that includes both summary and detail criteria. No TPL-specific MECT 2.3 Checklist requirement has been identified.

46. The selected Offeror's module must associate recoveries (including post-payment) with recipients, providers, and services for claim-specific activities. No TPL-specific MECT 2.3 Checklist requirement has been identified.

47. The selected Offeror's module must provide on-line display, inquiry, and update functionality of post-payment recovery case records by claim, recipient, insurance company, provider, or a combination of these data elements. The corresponding CMS MECT 2.3 Checklist requirement number is FM.DSS1.12.

48. The selected Offeror's module must identify and support recovery actions for Medicaid paid claim records that subsequently become eligible for Medicare or other health-related insurance coverage. No TPL-specific MECT 2.3 Checklist requirement has been identified.

49. The selected Offeror's module must track individual claim records and multiple claim records that reach a user-defined threshold for recovery. (The threshold must be variable.) The corresponding CMS MECT 2.3 Checklist requirement numbers are FM.DSS1.12 and FM.TPL2.10.

50. The selected Offeror's module must initiate automated claim-specific adjustments for initiation by other MMIS 2020 modules for retroactive recoveries. No TPL-specific MECT 2.3 Checklist requirement has been identified.

51. The selected Offeror's module must initiate the parameters to filer/screen verified TPL resources against a paid claims history retroactively for a period of time specified by the Department; to identify ad-hoc special recoveries. Claims history data is available from other MMIS 2020 Platform modules via the SI/DH. The corresponding CMS MECT 2.3 Checklist requirement number is FM.TPL2.9.

52. The selected Offeror's module must apply, track, document, and report fully or partially recovered or recoverable monies to the appropriate claims/encounters, at the line level. No TPL-specific MECT 2.3 Checklist requirement has been identified.

53. The selected Offeror's module must generate Department-defined data for automated TPL billing information to providers for recipients with third-party coverage. The data will be sent via the DH to the appropriate MMIS 2020 modules to process the invoices. The corresponding CMS MECT 2.3 Checklist requirement number is FM.TPL2.4.

54. The selected Offeror's solution must use demographics to identify a recipients' age. Describe how your module uses demographics to identify recipient's age. No TPL-specific MECT 2.3 Checklist requirement has been identified.

55. The selected Offeror's solution must capture, maintain, and view on-line settlement data including the total settlement amount, Medical Assistance settlement amount, and other parties' settlement amount associated with a recovery action. No TPL-specific MECT 2.3 Checklist requirement has been identified.

56. The selected Offeror's solution must create and maintain contact information for the associated attorney, personal representative, court, or others interested parties for all TPL recoveries. It must also allow the user to change contact information without impacting case-specific or global contacts. No TPL-specific MECT 2.3 Checklist requirement has been identified.

57. The selected Offeror's solution must have an automated workflow for sorting, tracking, and distributing information into the TPL case management system, including:
    a. TCT documents
    b. Estate questionnaires
    c. Revenue matches

    No TPL-specific MECT 2.3 Checklist requirement has been identified.

58. The selected Offeror's solution must accept an input file from the Department via the SI/DH that generates estate questionnaires, including date of death and revenue match. No TPL-specific MECT 2.3 Checklist requirement has been identified.

59. The selected Offeror's solution must automatically request encounter data via the SI/DH from all associated managed care entities. No TPL-specific MECT 2.3 Checklist requirement has been identified.

60. The selected Offeror's solution must track the recovery of funds from third parties and estates when TPL and estate resources are identified. No TPL-specific MECT 2.3 Checklist requirement has been identified.

61. The selected Offeror's solution must provide aggregated recipient and claims history profiles obtained from other MMIS 2020 Platform modules via the SI/DH for TPL investigations. The corresponding CMS MECT 2.3 Checklist requirement number is FM.DSS2.8.

62. The selected Offeror's solution must search client eligibility data and other MMIS 2020 Platform modules via the SI/DH to determine if the recipient has received benefits or has any pending applications or purge data when entering client information into the TPL Module. The TPL Module must alert Department staff of the eligibility decision once determined. No TPL-specific MECT 2.3 Checklist requirement has been identified.

63. The selected Offeror's solution must search specific client eligibility information, including:
    a. Name,
    b. Social Security Number ("SSN"),
    c. CIS number

    Provide eligibility details (MCO, facility, and waiver types). Interface with CIS via SI/DH and the TPL case management system. No TPL-specific MECT 2.3 Checklist requirement has been identified.

64. The selected Offeror's solution must allow users to document the case status, add notes or comments to the case file, and link and cross-reference cases. No TPL-specific MECT 2.3 Checklist requirement has been identified.

65. The selected Offeror's solution must document and maintain casualty and estate data. No TPL-specific MECT 2.3 Checklist requirement has been identified.

66. The selected Offeror's solution must provide functionality to store, search, retrieve and edit all received requests from users. No TPL-specific MECT 2.3 Checklist requirement has been identified.

67. The selected Offeror's solution must perform calculations of Department-specified formulas (e.g., pro rata share, percentage reductions) and retain all data as entered based on Department-defined retention rules. No TPL-specific MECT 2.3 Checklist requirement has been identified.

68. The selected Offeror's solution must automatically generate the data required to produce a letter to the applicable contact on open cases in a time frame or process specified by Department. It must allow the Department to disable this feature on a case-by-case basis. The corresponding CMS MECT 2.3 Checklist requirement number is FM.TPL2.12.

69. The selected Offeror's solution must:
    a. Provide functionality for the Outbound Mail module for on-line creation, generation, maintenance, modification, storage, and historical viewing of standard and ad-hoc letters to recipients and their representatives, insurance companies, employers, providers, and other parties;
    b. Document the date sent and date of occurrence for all written communication;
    c. Retain all incoming correspondence for a period of time to be established by the Department;
    d. Provide print preview, editing, and deleting functionality; and,
    e. Track all correspondence with a unique identifier.

    The corresponding CMS MECT 2.3 Checklist requirement number is OM.TPL1.2.

70. The selected Offeror's solution must retain cases in a pending status for all recipients with no established eligibility for a certain amount of time and to periodically check for eligibility. It must be able to alert Department staff of eligibility decision once determined. No TPL-specific MECT 2.3 Checklist requirement has been identified.

71. The selected Offeror's solution must retain cases in a pending status when there is no initial record of Medicaid payments, periodically check as determined by the Department for recent payments prior to closing the case, and alert staff of those payments and closures. No TPL-specific MECT 2.3 Checklist requirement has been identified.

72. The selected Offeror's solution must automatically assign additional incident dates to users already working on an open case for the same recipient. No TPL-specific MECT 2.3 Checklist requirement has been identified.

73. The selected Offeror's solution must allow cases to have the same date of incident with different case types. No TPL-specific MECT 2.3 Checklist requirement has been identified.

74. The selected Offeror's solution must store and retrieve casualty-related information (e.g., Motor Vehicle Accident and Workers' Compensation information) through an automated process. The corresponding CMS MECT 2.3 Checklist requirement number is FM.TPL1.2.

75. The selected Offeror's solution must automatically generate casualty-related follow-up correspondence ,using templates from the OBM Module through the SI/DH, to the following, including:
    a. Recipients
    b. Attorneys
    c. Motor vehicle department
    d. Insurance companies
    e. Workers' Compensation

    The corresponding CMS MECT 2.3 Checklist requirement number is OM.TPL1.3.

76. The selected Offeror's solution must capture paid fee-for-service and encounter claims and import them to cases established for recovery on a predetermined schedule as specified by the Department. No TPL-specific MECT 2.3 Checklist requirement has been identified.

77. The selected Offeror's solution must maintain and display the following data for each claim associated with an estate case, including:
    a. Recovered amount
    b. Date recovered
    c. Source of collection (insurance company, recipient, prior authorization/program exception)
    d. Real estate value
    e. Zip code of real estate

    The corresponding CMS MECT 2.3 Checklist requirement number is TA.FR.1.

78. The selected Offeror's solution must support recovery and produce reports to support recovery from an estate or designated trust. The corresponding CMS MECT 2.3 Checklist requirement numbers are FM.TPL2.8.

79. The selected Offeror's solution must support non-administered estates regulations per the regulatory requirements found at 55 Pa. Code §258.11. No TPL-specific MECT 2.3 Checklist requirement has been identified.

80. The selected Offeror's solution must provide the ability to set parameters for automated management of casualty and estate cases. No TPL-specific MECT 2.3 Checklist requirement has been identified.

81. The selected Offeror's solution must purge case records using a Department-defined date with override capability on selected records. No TPL-specific MECT 2.3 Checklist requirement has been identified.

.

82. The selected Offeror's solution must allow authorized Commonwealth staff to update tables and manage user security table access levels. Describe how your solution permits the Department to update tables and manages user-restricted access to these tables. No TPL-specific MECT 2.3 Checklist requirement has been identified.

83. The selected Offeror's solution must be able to accept check updates/alerts (such as returned checks, insufficient funds, wrong recipients, incorrect amounts) as errors as discovered and received from the Financial Module. The system, at a minimum, must include:
    a. Recipient
    b. Service program
    c. Claim number
    d. Category of receivable (e.g., TPL, rate adjustment)
    e. Transaction source (e.g., system-generated, refund, Department-generated)
    f. Provider number/entity name and identification number
    g. Payment/recoupment detail (e.g., dates, amounts, check number, cash, or recoupment)
    h. Account balance
    i. Appropriation of funds (e.g., FFS, Long Term Care ("LTC"), cash, capitation, federal state split/exceptions)

    No TPL-specific MECT 2.3 Checklist requirement has been identified.

84. The selected Offeror's solution must support a process to accumulate, track, edit, and report on financial data related to recovery and cost-avoidance activities of TPL. The corresponding CMS MECT 2.3 Checklist requirement number is FM.DSS2.3.

85. The selected Offeror's solution must allocate funds and recoveries from other agencies outside of TPL (e.g. family planning). The TPL Module must maintain and create a record of transactions collected and provide the ability to report. No TPL-specific MECT 2.3 Checklist requirement has been identified.

86. The selected Offeror's solution must track and report post-payment and other types of recoveries. No TPL-specific MECT 2.3 Checklist requirement has been identified.

87. The selected Offeror's solution must send revenue transfers (e.g., restitution due to assault cases) to TPL's Module case management system for documentation purposes, automatically add narrative, include transfer amount, automatically reduce the amount of the Statement of Claim ("SOC"), and allow for supervisor override of any entry. No TPL-specific MECT 2.3 Checklist requirement has been identified.

88. The selected Offeror's solution must maintain a running total of amount due for cases that have received manual checks or revenue fund transfers. No TPL-specific MECT 2.3 Checklist requirement has been identified.

89. The selected Offeror's solution must auto-update individual cases based on system alerts generated from other modules and transmitted via the SI/DH. No TPL-specific MECT 2.3 Checklist requirement has been identified.

90. The selected Offeror's solution must support the following overpayment functionalities:
    a. Support identification of overpayment;
    b. Notify the Finance Module to generate a general invoice via the SI/DH;
    c. Automatically credit the amount owed to the SOC;
    d. Update the TPL narrative about overpayment, and
    e. Delete or recall a general invoice.

    No TPL-specific MECT 2.3 Checklist requirement has been identified.

91. The selected Offeror's solution must link returned TCT forms to the original questionnaire and then link with the TPL Module case management system. No TPL-specific MECT 2.3 Checklist requirement has been identified.

92. The selected Offeror's solution must generate trauma lead letters on demand and produce reports of all letters, using templates from the OBM Module, through the SI/DH. No TPL-specific MECT 2.3 Checklist requirement has been identified.

93. The selected Offeror's solution must track and report amounts billed, paid, and collected on current and historical cases. No TPL-specific MECT 2.3 Checklist requirement has been identified.

94. The selected Offeror's solution must provide a SOC process that includes the following functionality:
    a. Sort, filter, and search, and upon review, default print by provider or service location;
    b. Administer the SOC screen and output by Commonwealth staff;
    c. Subtotal based on Department specified criteria;
    d. Allow users to review the case and update the SOC as necessary until the date of distribution of settlement funds;
    e. Request claims and encounters on a regular and continuous basis, on an interval specified by the Department, for follow-up on active cases at a time frame specified by the Department and notify users accordingly; and,
    f. Provide the ability to link related claims and encounters to view a complete history.

    No TPL-specific MECT 2.3 Checklist requirement has been identified.

95. The selected Offeror's solution must allow Commonwealth staff to generate the SOC and lien. No TPL-specific MECT 2.3 Checklist requirement has been identified.

96. The selected Offeror's solution must sort and include claims when creating a SOC based on data fields as defined by Commonwealth staff. No TPL-specific MECT 2.3 Checklist requirement has been identified.

97. The selected Offeror's solution must, once the case is established, allow staff to prepare and issue an accurate and complete SOC to all potentially liable parties. The SOC will consist of all Medicaid claims paid that relate to the incident, as well as any recoverable cash assistance received from the time of the incident until the distribution of settlement funds. The SOC, at a minimum, includes the following elements:
    a. Client's name, identification number, and date of incident present on each page;
    b. A summary page that includes a breakout of the Department's claim by claim type, cash assistance due, date of incident, and the tax identification number of the Department; and,
    c. Summary by provider that includes the following:
        i. Provider's address, phone number, MPI, and NPI numbers
        ii. SOC production date
        iii. Dates of service
        iv. Payment date
        v. Original and adjusted claim reference numbers
        vi. Usual charge/amount billed; amount approved/amount paid
        vii. Diagnosis code, if available
        viii. Procedure code, if available
        ix. A subtotal of usual charges and amount approved
        x. National Drug Code ("NDC") for all pharmacy claims
        xi. Reduction amounts applied to the SOC
        xii. Page number
        xiii. Date of incident ("DOI")
        xiv. Subtotal per provider and/or page
        xv. Reduction details

    The corresponding CMS MECT 2.3 Checklist requirement number is IA.DS.13.

98. The selected Offeror's solution must generate detail and summary reports for SOC. No TPL-specific MECT 2.3 Checklist requirement has been identified.

99. The selected Offeror's solution must coordinate with all MA MCOs to collect paid claims data necessary for completion of SOCs. No TPL-specific MECT 2.3 Checklist requirement has been identified.

100. The selected Offeror's solution must include in the SOC, at a minimum, the following elements using a format to be determine in JAD sessions:
    a. Decedent's name and Medicaid identification number present on each page of the SOC;
    b. Identification information for the Department as claimant and for the selected Offeror as the Department's representative on each page;

c. A summary page that includes a breakout of the Department's claim both by claim type and by creditor classification of 3 or 5.1 and the tax identification number of the Department;
d. Check off option to describe reason for service; and,
e. A summary by provider that includes the provider's contact information, address, phone number, and MPI and NPI numbers, as well as include the following data:
    i. SOC production date
    ii. Dates of service
    iii. Provider of service
    iv. Payment date
    v. Original and adjusted claim reference numbers
    vi. Usual charge/amount billed
    vii. Amount approved/amount paid
    viii. Diagnosis code, if available
    ix. Diagnosis code description
    x. Procedure code, if available
    xi. Procedure code description
    xii. Subtotal of usual charges and amount approved
    xiii. National Drug Code (NDC) for all pharmacy claims
    xiv. Reduction amounts applied to the SOC
    xv. Page numbers

The corresponding CMS MECT 2.3 Checklist requirement number is PL.RDM1.18.

101. The selected Offeror's solution must import claims or capitation payments imported to an estate SOC must have a date of service on or after the decedent's 55th birthday. Medicare crossover claims should not be imported when using paid claims. No TPL-specific MECT 2.3 Checklist requirement has been identified.

102. The selected Offeror's solution must rerun and update estate SOC. No TPL-specific MECT 2.3 Checklist requirement has been identified.

103. The selected Offeror must support the use of the Management and Administrative Reporting System ("MARS"). No PA-specific MECT 2.3 Checklist requirement has been identified.

104. The selected Offeror must identify and prepare data, as it is created/received, that will need to be shared by the Data Hub to other stakeholders. No PA-specific MECT 2.3 Checklist requirement has been identified.

105. The selected Offeror's solution must provide the capability to create, open and close care management records. No PA-specific MECT 2.3 Checklist requirement has been identified.

H. TPL System, Cyber and HIPAA Security Plan. The selected Offeror will design, develop, implement, and maintain TPL System, Cyber and HIPAA Security Plan ("SCHSP"). The initial TPL SCHSP must be delivered forty-seven (47) business days after the purchase order effective date. The plan must detail how the selected

Offeror will maintain compliance with Commonwealth Information Technology Policies in **Section I-31.A** of this RFP. The SCHSP must detail how cyber security measures and HIPAA security measures are built into the proposed solution. Include in the SCHSP how the measures will keep Pennsylvania's Medicaid data secure from cyber data breaches and HIPAA violations.
The selected Offeror must describe how its SCHSP monitors for and prevents cyber breaches, identifies cyber breaches, rectifies cyber breaches that occur, and reports HIPAA violations. The selected Offeror must describe the frequency of review and update of the SCHSP and the testing frequency and process.

The Offeror must provide detailed information regarding its system, cyber, and HIPAA security strategy.

1. Describe the security measures that are built into proposed solutions to prevent system and data breaches.
2. Describe preventative measures, such as policies and procedures, taken to reduce the risk of system cyber-attacks and HIPAA violations.
3. Provide details of how your solution's cyber security and risk mitigation plan prevents cyber data breaches, monitors and identifies cyber data breaches, and rectifies cyber data breaches that occur.
4. Describe the frequency of reviews and updates of the cyber security and risk mitigation plan and the testing process and testing frequency.
5. Use of PII and PHI and a description of the types of data that will be collected.
6. Sources of PII/PHI, populations, and transfer and disclosure mechanisms.
7. Details about the entities with which the collected information will be shared.
8. Privacy and security standards for business partners, other third parties and the agreements that bind these entities.
9. Incident handling procedures.
10. Privacy and security awareness programs and materials for the Offeror's workforce.
11. A statement that the system meets HIPAA requirements for transactions and code sets, privacy and security, and when required, NPI. This statement is in addition to the completion of all the HIPAA-related checklist criteria.

The selected Offeror must detail in the TPL SCHSP how it will enforce security within the TPL Module and the selected Offeror's organization including physical security of hardware, interactions between other MMIS 2020 Platform modules and the Department, identification of individuals who have privileged access, and how data to and from external sources is controlled.

The selected Offeror must report all system security breaches including Cyber intrusions to the Department within fifteen (15) minutes of incident identification regardless of the known scope of the incident. The selected Offeror must report misuse of IT resources and loss or theft of equipment (USB drives, laptops, smartphone, etc.) that may contain MMIS 2020 Platform data, via email, to the Department within one hour of the incident. The selected Offeror is required to follow incident-handling procedures to document the full scope of the incident, containment, eradication, and recovery as appropriate to the situation for all incidents. Failure to report any security issues or breach incidents as noted and provide sufficient response to any security issue/breach is subject to liquidated damages

Deliverable: TPL System, Cyber, and HIPAA Security Plan

The Offeror must describe its approach to the development and execution of the TPL System, Cyber and HIPAA Security Plan. The selected Offeror must deliver the TPL System, Cyber and HIPAA Security Plan sixty-five (65) calendar days prior to the TPL Module implementation and must be update the Plan annually.

I. TPL Tier 2 Technical Support. The selected Offeror must provide SMEs who can assist stakeholders with TPL-related issues for Tier 2 Technical Support. Stakeholders will communicate TPL-related issues to the Tier

1 Support Center by phone, web form, or email. When the Tier 1 Support Center is unable to resolve a TPL Module-related issue, it will create and route a trouble ticket to the selected Offeror through a CRM tool for Tier 2 assistance. The CRM tool will create a trouble ticket to track the activities taken to resolve the TPL Module issue. Upon successful completion of the issue, the selected Offeror will complete the trouble ticket showing the corrective actions taken and will route back to the Tier 1 Support Center via CRM. The selected Offeror will collaborate with the Tier 1 Support Center Contractor to design and develop the Tier 2 escalation process and the CRM workflow, including the trouble ticket template.

The selected Offeror must, at a minimum:

1. Coordinate resolution of trouble tickets for TPL functions sent via CRM from the Tier 1 Support Center;
2. Facilitate resolution of TPL issues with users and document action in trouble ticket;
3. Return completed trouble ticket via CRM to the Tier 1 Support Center;
4. Escalate TPL trouble tickets that cannot be resolved to Tier 3 via CRM for resolution;
5. Collaborate with ITC/QA contractor on documenting the knowledge base of information to allow the Tier 1 Support Center to answer common TPL questions;
6. Acknowledge 99% or greater of all inquiries from the Tier 1 Support Center within one (1) hour of receipt; and,
7. 99% or greater of all inquiries from the Tier 1 Support Center must have a resolution, plan of action or escalation to a defect within three (3) business days.

The Offeror must describe its approach to the development and execution of the TPL Tier 2 – Technical Support.

J. Input and Output File Updates. The selected Offeror must use a solution that processes input files updates accurately and makes all file uploads available within sixty (60) minutes (or depending on the file, at an agreed upon time identified in the project schedules). Likewise, the Offeror's module must provide for the production and delivery of all output files within sixty (60) minutes of sending (or depending on the file, at an agreed upon time identified in the project schedules).

All input and output file protocols and procedures must align and comply with Chapter 11 of the State Medicaid Manual on Medicaid Management Information Systems.

K. Reuse. In accordance with CMS directive, the Department is seeking a TPL solution that will maximize reuse opportunities for other states and local governments or that has been used by other states and can be reused by the Department. Please explain how your solution will allow reuse by other states in their solution, which may include cloud hosting, open source development, and share customization. If you have reused your module in the past with other states in their MMIS, please identify the state and what was reused. See State Medicaid Director Letter #18-005 Mechanized Claims Processing and Information Retrieval Systems – Reuse at https://www.medicaid.gov/federal-policy-guidance/downloads/smd18005.pdf.

The Offeror must describe its approach to the development and execution of Reuse.

II-18. Reports and Program Control. The selected Offeror must work with the Department to define weekly, monthly, quarterly, and annual reporting requirements during JAD sessions. The selected Offeror is responsible for the

accuracy of calculations and completeness of data used as input. All defined reports must be available online and in the required format by the scheduled time as defined and mutually agreed upon.

A. Operations Report. As the MMIS 2020 Platform Dashboard is being developed by the ITC/QA and SI/DH Contractors, the selected Offeror must produce inputs to the Dashboard that detail TPL operations. The selected Offeror must develop an Operations Report that includes:

1. Operations Production Status with agreed upon metrics
2. Performance Standards Reporting
3. Other operational metrics as required by the Department

B. Weekly Status Reports. The selected Offeror must submit an electronic weekly status report aligned to the TPL-MWP in a format approved by the Department. The selected Offeror must submit weekly reports for the previous week to the Department no later than 12pm on the first business day of the following week. The reports will cover the previous week's reporting period (Sunday through Saturday). At a minimum, weekly status report must contain the following:

1. Updated detailed Project Plan schedule with upcoming milestones and overall percentage complete.
2. A dashboard that shows the overall status of the project.
3. The plans for activities scheduled for the next week.
4. The status of Deliverables as defined in **Section II-16. A.**
5. Time ahead or behind schedule for applicable tasks.
6. New risks identified in the previous week.

The Offeror must describe its approach and execution of the weekly status reports. The Offeror may propose additional or more frequent reports and report items based on its experience with IT projects of this size and scope. The Offeror must provide a sample weekly status report with its Technical Submittal.

C. Monthly Status Reports. The selected Offeror must submit an electronic monthly status report aligned to the TPL-MWP in a format approved by the Department. The selected Offeror must submit monthly reports for the previous month to the Department no later than 8 a.m. on the fifth business day of the subsequent month. The reports will cover the previous month's reporting period (1st calendar day through last calendar day of the month). At a minimum, monthly status report must contain the following:

1. A description of the completion status of the Project in terms of the approved Project Plan incorporating an Earned Value Analysis for schedule and cost.
2. KPIs, including Cost Performance Index ("CPI") and Schedule Performance Index ("SPI"), with explanations if CPI or SPI are beyond thresholds.
3. Updated Project schedule with upcoming milestones and overall percentage complete.
4. A dashboard that shows the overall status of the project.
5. The plans for activities scheduled for the next month.
6. The status of Deliverables as defined in**, Section II-16.A.**
7. Time ahead or behind schedule for applicable tasks.
8. Updated issue management report including the issues from the IV&V Contractor's Post-Implementation Assessment Review.
9. A risk analysis of actual and perceived problems along with their suggested mitigations.

10. Strategic changes to the Project Plan, if any.
11. Any organizational changes that may have taken place or will take place.
12. Changes in key personnel must be approved by the Commonwealth in advance.
13. Key activities completed during reporting period.

The Offeror must describe its approach and execution of the monthly status reports. The Offeror may propose additional or more frequent reports and report items based on its experience with IT projects of this size and scope. The Offeror must provide a sample monthly status report with its Lot 2 Technical Submittal.

D. Meetings. During the course of the contract, the selected Offeror must attend, or lead meetings as requested by the Department. At the Department's discretion, these meetings will take place in the Harrisburg, Pennsylvania area or be conducted via conference calls.

The selected Offeror must attend MMIS 2020 Platform meetings as directed and support these meetings by providing reports, participating in brainstorming and planning activities, providing consultation and technical assistance, and helping to resolve issues.

For meetings lead by the selected Offeror, the selected Offeror must produce meeting materials, which include schedules, written status reports, draft and final minutes, decision registers, agendas, recaps and other meeting materials. The selected Offeror must provide meeting materials as follows:

1. Distribute agendas at least two (2) business days prior to meetings.
2. Submit meeting minutes to the Department for approval within two (2) business days of meeting being held.
3. Review available project artifacts prior to any meeting.
4. Meeting materials are subject to recording in the MMIS 2020 Platform artifact library.

At a minimum, the selected Offeror must participate as directed in the following meetings:

1. **TPL Kick-off Meeting.** The selected Offeror must conduct a kick-off meeting within sixty (60) calendar days of the effective date of the contract for the MMIS 2020 Platform stakeholders confirming project scope and objectives, summary of the project, project schedule, methodology, the roles, responsibilities and expectation of the team, and milestones of the TPL Module.

2. **Change Control Board Meeting.** The ITC/QA Contractor will facilitate the CCB Meetings that includes the Department, the selected Offeror, and other MMIS 2020 Platform module and legacy system contractors. The selected Offeror must attend the CCB and will be notified by the Department for required support as needed.

   The CCB reviews defects and requested changes for each module or functional area and ensures that DHS and the contractors have a mutual understanding of what is to be delivered, when it is to be delivered, and the cost impact in effort hours, if applicable. The CCB serves as a clearinghouse for all defects and changes, including changes to scope and cost. The CCB reports to the MMIS 2020 Platform Steering Team. If a change control item must be elevated above the CCB for resolution, it will be sent by the CCB to the Steering Team for decision. The CCB will meet on a frequency and at a time mutually acceptable to all stakeholders.

   The CCB is comprised of Department resources from multiple program offices and the contractors who have the authority to make decisions related to the defect or status of a change order, its financial impact,

and its importance. The core membership of the CCB will invite SMEs and stakeholders to CCB meetings as needed. During the transition from legacy system to the MMIS 2020 Platform, the legacy contractor may also be invited to attend.

3. **Release Planning Meeting.** Release Planning is the logical output of the CCB. Release Planning involves the scheduling of change orders ("CO") agreed upon by the CCB and the impact to Department and MMIS Business Operations. During the transition from legacy system to MMIS 2020 Platform, release planning must account for changes to existing modules or functionalities. Release planning must also continue during the M&O phase of the MMIS. The selected Offeror must attend the Release Planning Meeting and will be notified by the Department for required support as needed.

   Under the strategic guidance of the Department, the ITC/QA Contractor will facilitate the Release Planning Meetings that includes the Department, the legacy system contractor, and MMIS 2020 Platform module contractors. The ITC/QA Contractor will produce a proposed system CO release schedule and documentation of its impact to MMIS Business Operations and the EDW. The Release Planning Meetings will convene on a frequency and at a time mutually acceptable to all stakeholders.

   Release Planning is comprised of DHS resources from multiple program offices and the contractors who have the authority to make decisions related to the release. The Department resources may invite SMEs and stakeholders to the meetings as needed. During the transition from legacy system to MMIS 2020, the legacy system contractor may also be invited to attend as necessary.

4. **QA/QC Meetings.** Under the strategic guidance of the Department, the ITC/QA Contractor will facilitate and document in writing all project meetings that are necessitated as part of the QA/QC scope of work. The selected Offeror must attend the QA/QC Meetings and will be notified by the Department for required support as needed.

5. **Requirements Gathering related meetings.** Under the strategic guidance of the Department, the ITC/QA Contractor will facilitate, and document requirements gathering and JAD sessions, as defined in **Section II-16.B TPL Charter and Project Roles** for the TPL Module. The selected Offeror must attend all Requirements Gathering related meetings for the TPL Module and other MMIS 2020 Platform Modules Requirements Gathering related meetings as needed.

6. **Status Meetings**. The selected Offeror must participate in status meetings with the Department. Under the strategic guidance of the Department, the meeting will follow an agenda and allow the selected Offeror to report to the Department on the projects' schedules, risks, issues, decisions, action items, and accomplishments, at a minimum.

The Offeror must describe its approach to facilitating and participating in meetings. The Offeror may propose additional meetings based on their experience with IT projects of this size and scope. DHS may require the Offeror to attend and facilitate other meetings at its discretion.

II-19. Performance Standards. The Commonwealth has developed a set of minimum Performance Standards defined below, which the selected Offeror must meet, or exceed in order to be in good standing. The Department may, at its discretion, assess liquidated damages. Where an assessment is defined as an "up to" amount, the dollar value will be set at the discretion of the Department. The selected Offeror's performance will be reviewed and assessed monthly. The DHS Contract Administrator will give written notice of each failure to meet a performance standard to the selected

Offeror. If Department does not assess liquidated damages in a particular instance, the Department is not precluded from pursuing other or future assessments relating to those performance metrics and their associated damages.

Table 4. TPL Module Performance Standards

Performance Standard	Minimum Acceptable	Non-Compliant Remedial Action
TPL – 1 Personnel	**Key position:** TPL Executive Account Director TPL Project Manager TPL Testing Manager TPL Functional Lead	Failure to notify DHS Contract Administrator of voluntary diversion within thirty (30) calendar days may result in the Department assessing liquidated damages of up to $2,500. Failure to Interim fill a Key Personnel vacancy within thirty (30) calendar days and/or permanently fill a vacancy within ninety (90) calendar days may result in the Department assessing liquidated damages of up to $2,000 per day for each day vacancy.
TPL – 2 System availability	Access to all production MMIS 2020 Platform activities are available for all MMIS users at all times except during scheduled maintenance.	Any unscheduled downtime whether consecutive or intermittent cannot exceed one (1) hour per calendar month in total. • Unscheduled downtime in excess of one (1) hour but fewer than five (5) hours in one (1) month may result in the Department assessing up to $250 for each partial or full hour in liquidated damages. • Unscheduled downtime exceeding five (5) hours per month but fewer than twelve (12) hours may result in the Department assessing up to $500 for each partial or full hour in liquidated damages. • Unscheduled downtime exceeding twelve (12) hours per month may result in the Department assessing up $1,000 for each partial or full hour in liquidated damages.
TPL – 3 System availability	All test and training environments will be available 6 a.m. – 6 p.m. Monday through Friday and as agreed to during testing and training windows.	Any unscheduled downtime whether consecutive or intermittent cannot exceed one (1) hour per calendar month in total. • Unscheduled downtime in excess of one (1) hour but fewer than eight (8) hours in one (1) month may result in the Department assessing up to $500 in liquidated damages. • Unscheduled downtime exceeding eight (8) hours per month may result in assessing up to $1,000 in liquidated damages.

Performance Standard	Minimum Acceptable	Non-Compliant Remedial Action
TPL – 4 Interactive Response Time	Ninety-eight percent (98%) of all interactive transactions will have a responses time of two (2) seconds or less measured from the receipt of transactions to the response back to the sender. Response for this Performance Standard is based on the average time between the receipt of a transaction and response/acknowledgment of the transaction.	Interactive Response Time for each transaction will be recorded daily from midnight to midnight each day. The sum of transactions exceeding the two (2) second Interactive Response Time will be divided by the total number of transactions for each twenty-four (24) hour period. Should the resulting percentage equal less than ninety-eight percent (98%), the Department may assess up to $1,000 in liquidated damages.
TPL-5 Outbound Response	All outbound files received from the SI/DH must be transmitted back to the submitter or intended receiver within four (4) hours.	All outbound files will be measured in a calendar month. The Department may assess up to $2,500 in liquidated damages for each file when response time exceeds the allowable response time by one (1) hour or more.
TPL – 6 Disaster Recovery	Conduct and pass a 24-Hour Recovery Point Objective and a 36-Hour Recovery Time Objective test of the DR Plan biannually.	Failure to pass the biannual 24-Hour Recovery Point Objective or the 36-Hour Recovery Time Objective may result in the Department assessing up to $1,000 in liquidated damages; for each failure.
TPL – 7 Disaster Recovery	On the occurrence of a disaster, the selected Offeror must meet the following 24-hour Recovery Point Objective and the 36-hour Recovery Time Objective when executing the DR plan.	Failure to meet the 24-hour Point Objective may result in the Department assessing up to $10,000 in liquidated damages. Failure to meet the 36-hour Recovery Time Objective may result in the Department assessing up to $10,000 in liquidated damages.
TPL – 8 Audits	Pass all audits without incurring monetary fines to include those conducted by the Commonwealth, CMS, and annual SOC 3 audits.	The Department may assess liquidated damages equal to the costs incurred and monetary fine to address any audit findings.
TPL – 9 Compliance	All software utilized within the TPL Module must be a version compatible with the SI/DH, unless otherwise approved by the Department. Waived for the first six (6) months of each module's M&O.	The Department may assess liquidated damages in the amount of up to $1,000 per month when TPL software is not compatible with the SI/DH. Compatible is define as the SI/DH and TPL Module cannot function because of version mismatch.
TPL – 10 Compliance	Adhere to and remain current with applicable State and Federal laws, rules, regulations, guidelines, policies, and procedures relating to information systems, information systems security and privacy, physical security, PHI confidentiality and privacy, Americans with Disabilities Act and Section 508 of the Rehabilitation Act.	The Department may assess liquidated damages of up to $2,500 plus any incurred cost to remediation for each non-compliance condition it identifies during the course of normal day to day operations, as the result of a finding in an audit, or as reported in a monthly report
TPL – 11 Auditing /Archiving	Maintain audit log data online for a minimum of one hundred and twenty (120) calendar days. Waived for the first one hundred and twenty (120) calendar days of M&O.	The Department may assess liquidated damages of up to $1,000 per month for noncompliance.

Performance Standard	Minimum Acceptable	Non-Compliant Remedial Action
TPL – 12 Auditing /Archiving	Maintain all original inbound and outbound transactional data for a minimum of sixty (60) calendar days. Waived for the first sixty (60) calendar days of M&O.	The Department may assess liquidated damages of up to $1,000 per month for noncompliance.
TPL – 13 Auditing /Archiving	Maintain system reports and extracts online for a minimum of one hundred and eighty (180) calendar days. Waived for the first one hundred and eighty (180) calendar days of M&O.	The Department may assess liquidated damages of up to 1,000 per month for noncompliance.
TPL – 14 Reporting	Standard, recurring reports, including CMS required reports and Medicaid Chapter 11, must contain accurate data and made available by the date and time specified by the Department. • Daily reports - due by 8 a.m. of the next business day. • Weekly reports - due by 12 p.m. of the first business day of the following week. • Monthly reports - due by 8 a.m. the 5th business day of the following month. Quarterly Reports - due by 8 a.m. the 1st business day the third week of the first month following the end of the quarter. • Annual reports - due by 8 a.m. the 1st business day of the second month of the following year. • All other reports not defined above will be due as mutually agree upon during JADs.	The Department will review report accuracy and delivery on a monthly basis. •Any report containing data the Department determines as incorrect may result in the Department assessing liquidated damages in the amount of up to $250 for each incorrect report. Each report delivered after the time specified and due date may result in the Department assessing liquidated damages in the amount of up to $250 for each late report.
TPL – 15 Updates	Upload all input files from internal and external sources and make available at date and time schedules as mutually agreed to by the Department and the selected Offeror during the DDI prior to M&O.	File uploads delayed by more than sixty (60) minutes after the agreed upon time frame will result in a penalty as follows: •Up to ten (10) files delayed in one (1) month may result in an assessment of up to $1,000. •Eleven (11) or more files delayed in one (1) month may result in an assessment of up to $2,000. Files uploads not completed accurately may result in an assessment of up to $1,000 per incident.
TPL – 16 Updates	Accurately produce and deliver all output files at agreed upon date and time schedules.	File uploads delayed past the scheduled time by more than sixty (60) minutes may result in the Department assessing liquidated damages as follows: •Up to ten (10) files delayed past the scheduled time in one (1) month may result in liquidated damages of up to $1,000 •Eleven (11) or more files delayed past the scheduled time in one (1) month may result in liquidated damages of up to $2,000

Performance Standard	Minimum Acceptable	Non-Compliant Remedial Action
TPL – 17 Updates	Download all output files at agreed upon date and time schedules as mutually agreed to by the Department and the selected Offeror during the DDI of each module prior to M&O.	Output files delayed past the scheduled time by more than sixty (60) minutes may result in the Department assessing liquidated damages as follows: •Up to ten (10) files delayed past the scheduled time in one (1) month may result in liquidated damages of up to $500. •Eleven (11) or more files delayed past the scheduled in one (1) month may result in liquidated damages of up to $1,000.
TPL – 18 Security	All system security breaches must be reported to the DHS Contract Administrator within fifteen (15) minutes of incident identification regardless of the known scope of the incident. Misuse of IT resources, loss or theft of equipment (USB drives, laptops, smartphone etc.) that may contain MMIS 2020 Platform data must be reported via email to the DHS Contract Administrator or designee within one (1) hour of the incident. All incidents will be required to follow incident handling procedures to include scope of incident, containment, eradication and recovery as appropriate to the situation.	Failure to report incident or provide sufficient response to any security breach may result in the Department assessing liquidated damages in the amount of up to $10,000 per security issue/breach/insufficient handling procedures response not reported.
TPL – 19 Defect Management	A CAP must include the proposed timeline for correcting the issues conforming to **Section II-16.6 TPL Defect Management Plan** for approval by the Commonwealth. The listed qualifying conditions provided below are examples for each severity level. DHS may change the severity level of any system event or issue after considering the effect on the provider community, population served, and continued system operations. When reconciliation is required to correct the downstream influence of a defect, the selected Offeror must provide a plan within two (2) business days. The reconciliation plan will detail how the affected issues will be corrected for the Department's review and approval. In instances where claims are affected, the report must include number of claims affected, original amount paid, adjusted amount of payout or take back, affected providers, and other elements required for the Commonwealths' review and approval. Upon Commonwealth's approval, the correction will occur within the time frames on **Section II-16.6 TPL Defect Management Plan**.	DHS will monitor all reported system issues and associated timeframes. Failure to meet any assigned timeframes for Critical, Significant and Moderate defects may result in the Department assessing liquidated damages up to $2,000 for each issue. Additional liquidated damages will be assessed at up to $1,000 every seven (7) calendar days until correction is implemented. Minor defects may result in the Department assessing liquidated damages up to $1,500 per incident if agreed-upon resolution time is not met. Failure to deliver a CAP within given timeframe may result in the Department assessing liquidated damages up to $750 per calendar day for each calendar day delayed. Failure to implement an approved reconciliation CAP within approved timeframe may result in the Department assessing liquidated damages up to $750 per calendar day for each calendar day delayed.
TPL – 20 Maintenance	All scheduled maintenance must be communicated to the Department at least ten (10) business days prior to the maintenance occurring.	Failure to notify the Department at least ten (10) business days prior to scheduled maintenance may result in the Department assessing liquidated damages of up to $1,000 for each day for which notice is late.
TPL-21 Tier 2 Response	Acknowledge 99% or greater of all inquiries from the Tier 1 Support Center within one (1) hour of receipt.	Failure to acknowledge 99% or greater of all inquiries in any calendar month may result in the Department assessing liquidated damages of $500 per month.

Performance Standard	Minimum Acceptable	Non-Compliant Remedial Action
TPL-22 Tier 2 Resolution	98% or greater of all inquiries must have a resolution, plan of action or escalation to a defect within five (5) business days.	Failure to resolve 98% or greater of all inquiries within five (5) business days may result in the Department assessing liquidated damages of $1,000 per month.
TPL-23 Response Time	Response time requirements are classified in four (4) categories. Each real-time service will be assigned a priority during the requirements and design process. The selected Offeror is responsible for response times only within its end points. Once assigned a priority, responses must meet the following response time requirements: Category 1: equal to a sub-second, 99% of the time Category 2: equal to a sub-second, 98% of the time Category 3: less than or equal to two (2) seconds, 98% of the time Category 4: less than or equal to twenty (20) seconds, 90% of the time	For each category's hourly average that exceeds the threshold response time in a calendar month, the Department may assess up to $2,500 in liquidated damages for each category.
PIMS – 24 Deliverables	Delivery of acceptable developed materials (either approved or conditionally approved) as determined solely within the discretion of the Department, including acceptable updates to developed materials, by the date and time specified by the Department.	A late deliverable may result in the Department accessing liquidated damages in an amount of up to $500 per calendar day up to 5% of the monthly fixed fee invoice.

A. For any deficiency, including ones relating to the performance metrics, the selected Offeror will prepare and submit a CAP for any observation or finding contained in a notice of deficiency. Unless another time period has been specified for submission, the selected Offeror must submit the CAP to the Department within ten (10) business days of notification of the deficiency or such longer time as may be agreed to by the Department.

B. The selected Offeror will include in the CAP:

1. Brief description of the findings;
2. Specific steps the selected Offeror will take to correct the situation or reasons why it believes corrective action is not necessary;
3. Name(s) and title(s) of responsible staff person(s);
4. Timetable for performance of the corrective action steps;
5. Monitoring that will be performed to ensure that corrective action steps were implemented; and,
6. Signature of the selected Offeror's Executive Account Director.

C. The selected Offeror must implement the corrective action plan within the timeframe agreed to by the parties for that particular corrective action plan. Failure to implement a corrective action plan, in the manner agreed to, may result in further action by the Department, including a finding of default.

D. In the event the Department determines a deficiency to be a serious non-compliance with the selected Offeror's obligations under the contract, the Department may find the selected Offeror in default.

II-20. Objections and Additions to Standard Contract Terms and Conditions. The Offeror will identify which, if any, of the terms and conditions it would like to negotiate and what additional terms and conditions the Offeror would like to add to the standard contract terms and conditions as part of its Lot 2 Technical Submittal, not via the Question and Answer process. The Offeror's failure to make a submission under this paragraph will result in its waiving its right

to do so later, but the Department may consider late objections and requests for additions if to do so, in the Department's sole discretion, would be in the best interest of the Commonwealth. The Department may, in its sole discretion, accept or reject any requested changes to the standard contract terms and conditions. The Offeror will not request changes to the other provisions of the RFP, nor will the Offeror request to completely substitute its own terms and conditions for the Standard Terms and Conditions. All terms and conditions must appear in one integrated contract. The Department will not accept references to the Offeror's, or any other, online guides or online terms and conditions contained in any proposal.

Regardless of any objections set out in its proposal, the Offeror must submit its proposal, including the cost proposal, based on the terms and conditions set out in the Standard Terms and Conditions**.** The Department will reject any proposal that is conditioned on the negotiation of the terms and conditions set out in the Standard Terms and Conditions or to other provisions of the RFP as specifically identified above.