ATTACHMENT A

SCOPE OF WORK AND FUNCTIONALITY

Through this ITN the Department seeks to procure a computer software tracking system that allows the Department to receive, store, and access seed-to-sale data from all Medical Marijuana Treatment Centers (MMTCs) and Certified Marijuana Testing Laboratories (CMTLs) to enable the Department to track, trace, and monitor marijuana from seed to sale, or other final disposition (the "State System").

This Attachment A - Scope of Work and Functionality document addresses the functionality and services that the Department believes are necessary to implement the State System. This Attachment A is intended to reflect the requested service and functionality components the Department is seeking. Although this Attachment A includes references to service and functionality components that "must," "shall," or "will" be delivered during contract performance, some of the services and functionality may be subject to change or deletion during negotiations. Final services and functionality will be resolved through the negotiations process. Although the Department reserves the right to negotiate any service or functionality components during the negotiation process, the vendor agrees that its initial reply is based on the assumption that Attachment A and Attachment B of the ITN apply as written prior to negotiations.

I. BUSINESS FUNCTIONALITY

Global	
BF-1.1	The State System must, at a minimum, have the ability to: define user roles and access for the Department, Medical Marijuana Treatment Centers (MMTCs), and Certified Marijuana Testing Laboratories (CMTLs); create and maintain new and existing users with configurable approval rules and permissions (this may require integration with a third-party system); create and maintain a list of users and associate items to the user list; put users on hold and document the reason; allow users to pull their own detail (reporting requirement); capture user contact information for correspondence; and transmit, receive, and record documents to/from users electronically. Note: The Department maintains a single sign-on (SSO) solution (Enterprise Mobility Suite) that would require integration. SSO is only required for department staff.
BF-1.2	The State System must have the ability to provide the Department 24-hour access to data from MMTC/CMTL Systems as it is uploaded, including weight, volume, and other data points required by Florida law and as may be set forth in administrative rule. The State System must include, at a minimum, notifications during each stage of the process, including:

	planting, growing, harvesting, processing, storing, transporting, laboratory testing, inventory, dispensations, sales, wholesale purchases, destruction and disposal of marijuana. The State System must also include real-time notification when marijuana is stolen, diverted, or lost, and to transportation manifests when marijuana is in transit. Additionally, the State System must provide the Department with access to data to include the weight and volume of marijuana waste through its destruction and disposal. The State System must provide real-time dispensation data. As MMTCs are required to notify the Department of stolen, lost, and diverted marijuana through the State System, the State System must be able to capture this transaction type and the Department should be able to manually adjust the status.
BF-1.3	The State System must have the ability to receive and store data from MMTC/CMTL Systems that utilize a unique number identifier, such that the Department can trace all marijuana back to the original source, including at a minimum: 1) Harvest data (e.g., strain, marijuana wet weight, marijuana dry weight, other material wet weight, other material dry weight, location of harvested material, time and date of harvest, and waste); 2) Product processing data (e.g., product type, quantity, weight, volume, waste, manufacture date, and expiration date, if applicable); 3) Product transportation data; 4) Testing data; 5) Dispensing data, including patient-related data; and 6) All other data deemed necessary to track the product from origin to patient for the purposes of public health, public safety, or to benefit patients. Identifiers must be unique to the organization that is submitting data. The State System will be required to flag duplicate identifiers submitted by the same organization. **Note:** The Department is not purchasing RFID tags or other similar hardware that generates identifiers.
BF-1.4	The State System must retain an audit trail of modifications to records and provide system backup and archiving.
BF-1.5	The State System must be able to receive and store, at a minimum, MMTC/CMTL System data obtained at every point in the chain of custody of marijuana, in every form, from seed to sale or other disposition.
BF-1.6	The State System must allow the Department to identify the location of marijuana within a facility for a given MMTC and allow Department staff to view the data of all MMTC/CMTL Systems at the global or granular level.
BF-1.7	The State System must allow the Department to add and accept data from new MMTCs and CMTLs and their MMTC/CMTL Systems and to update existing MMTC and CMTL information, including updates in the event of an emergency and ownership changes. The State System must allow the Department to override information provided by MMTC/CMTL Systems to verify data and prevent unlawful diversion.
BF-1.8	The State System must, at a minimum, meet the Department's IT policy for data retention requirement of five (5) years from the transaction date for any records generated in the system, with the exception of receipts, which are required to be maintained in accordance with Florida's General Records Schedule, GS1-SL.

BF-1.9	The State System must allow the Department to view data regarding the movement of all marijuana including the transfer of marijuana from MMTCs to CMTLs, from CMTLs to other CMTLs, and from CMTLs to MMTCs.
BF-1.10	The State System must be scalable to account for developments including legislative changes and market demand.
BF-1.11	The Vendor, at the Department's request, must facilitate a monthly technical user group consisting of stakeholders (e.g., the Department, MMTCs, CMTLs, the Vendor) prior to launch as well as once the system is implemented. The Vendor must participate in monthly governance end-user meetings at the request of the Department. The Department will invite the participants and develop the agenda for such meetings. Such meetings may be in-person or virtual.
BF-1.12	The Department shall have complete access to and own all data in the State System at all times.
BF-1.13	The State System must have the ability to integrate with current or future Department systems (e.g., the Department's licensing system). **Note**: The Department's licensing system's application is Salesforce. The Medical Marijuana Use Registry's application is a custom developed solution(.Net/SQL). Current system integration would be expected with Application Programming Interface (API).
BF-1.14	The State System must have a robust API that defines data standards for upload from other systems (e.g., the MMTC/CMTL Systems). The State System must make available real-time API integration via secure web service. **Note:** MMTCs and CMTLs will be responsible for ensuring modifications to MMTC/CMTL Systems necessary to generate data in the appropriate format to submit to the State System's API.
BF-1.15	The API specifications for all State System functionality must be fully documented and provided to approved MMTCs, CMTLs, and the Department.
BF-1.16	The State System must allow MMTCs and CMTLs to demonstrate the correct use of the system, or API, before they are authorized to submit data to the Department via their MMTC/CMTL System. **Note:** MMTCs and CMTLs will not have direct access to the State System. State employees will be the only direct users of the State System.
BF-1.17	The State System must allow real-time, 24-hour access by the Department to uploaded data from all MMTCs and CMTLs.
BF-1.18	The Vendor must be located within the U.S. and perform all tasks related to the ITN inside the U.S. No offshore development services may be used. All State System data must be store within the U.S. and may not be offshored.
BF-1.19	Onsite visits to Department offices will be required during State System development at the Department's discretion.

BF-1.20	The Vendor shall meet with and present the Department with a project plan within 30 days of contract execution. The plan is subject to Department approval.
BF-1.21	The State System must operate in real-time and be accessible 24 hours a day, seven days a week, via the Internet by the Department, MMTCs, and CMTLs at any given time, with the exception of announced scheduled maintenance.
Cultivation	
BF-2.1	The State System must allow data tracking and tracing through each stage of cultivation and the destruction and disposal of marijuana waste generated during the cultivation process.
BF-2.2	The State System must be able to flag harvest failures and monitor wholesale purchases and sales. This functionality is in addition to the requirement that the State System track and trace destruction and disposal of marijuana.
BF-2.3	The State System must allow for the tracking and tracing of data from MMTC/CMTL Systems regarding products used in the cultivation of marijuana by MMTCs (e.g. pesticides, fungicides, and growth regulators).
Processing	
BF-3.1	The State System must allow for the tracking and tracing of data from MMTC/CMTL Systems regarding all methods, materials, and ingredients used in the processing of medical marijuana products, and marijuana waste destruction and disposal resulting from the production of usable product.
BF-3.2	The State System must allow for the tracking and tracing of data from MMTC/CMTL Systems regarding the active and inactive ingredient lists for each medical marijuana product (cannabinoid content and excipients) as determined by each MMTC
BF-3.3	The State System must allow for the tracking and tracing of data from MMTC/CMTL Systems regarding products remediated by MMTCs back to the original retail batch. **Note:** Products remediated by MMTCs refers to a previously failed Retail Batch remediated in accordance with emergency rule 64ER20-37.
Laboratory Testing	
BF-4.1	The State System must allow for the tracking and tracing of data from MMTC/CMTL Systems for each sample sent for testing to a CMTL.
BF-4.2	The State System must allow for the tracking and tracing of data from MMTC/CMTL Systems regarding marijuana waste destruction and disposal.
BF-4.3	The State System must receive and store data from the MMTC/CMTL Systems (the list of CMTLs may change over time, and there must be a mechanism for the Department to update the list as needed).
BF-4.4	The State System must allow for the tracking and tracing of data from MMTC/CMTL Systems regarding any sample information, including the unique sample identifier and test requisitions.

BF-4.5	The State System must allow for the tracking and tracing of data from MMTC/CMTL Systems regarding detailed results of laboratory testing including certificates of analysis (COA) as well as raw data and PDF documentation. Each final product must be traceable to a COA, which includes passing and failing tests. The pass or fail status will be an additional status in the State System.
BF-4.6	The State System must automatically flag any usable product that failed regulatory compliance testing and flag the target analyte failed. The system must have the ability to receive and store data from MMTC/CMTL Systems regarding previously failed retail batches that will be resampled and retested or remediated.
BF-4.7	The State System must generate a list of Department-approved CMTLs and must be able to link the CMTLs to the MMTCs for which they are conducting testing.
BF-4.8	The State System must allow for the tracking and tracing of data from MMTC/CMTL Systems regarding samples of a given retail batch sent to multiple CMTLs for testing.
BF-4.9	The State System must track, trace, and report, in real time, and in a data-driven, editable, searchable format, required regulatory compliance testing performed, including which CMTL performed the analysis, the specific results, and the pass / fail status of each retail batch. The data must include the percentage of retail batches passing potency testing and contaminants unsafe for human consumption. The State System does not have to include functionality to prevent MMTCs from conducting testing with multiple CMTLs on the same retail batch for the same analytes (or components) but must have the capability to flag such activity. **Note**: An MMTC may use more than one CMTL to test different analytes (or components) within the product. For example, the sample may be sent to CMTL “A” to test for contaminants unsafe for human consumption and to CMTL “B” to test for the cannabinoid profile.
Dispensing	
BF-5.1	The State System must allow for the tracking and tracing of data from MMTC/CMTL Systems of all sales and dispensations of usable product, including, but not limited to, the following: time and date of dispensation, dispensing facility data, patient data, employee ID / Name, product dispensed (including batch number and unique number identifier), weight or volume of product dispensed, and sale price. The State System must link every usable product dispensed to a passing COA generated by the CMTL.
BF-5.2	The State System must allow for the tracking and tracing of data from MMTC/CMTL Systems of all sales and dispensations of marijuana delivery devices, including, but not limited to, the following: time and date of

	dispensation, dispensing facility data, patient data, employee ID / Name, marijuana delivery device dispensed, and sale price. **Note:** The State System need not include the ability to maintain a list of approved marijuana delivery devices or assign unique identifiers to marijuana delivery devices.
BF-5.3	The State System must allow for the tracking and tracing of data from MMTC/CMTL Systems regarding patient or caregiver's Registry ID Card.
BF-5.4	The State System must allow for the tracking and tracing of data from MMTC/CMTL Systems regarding price of usable product and marijuana delivery devices. **Note:** The Department maintains a list of approved products in the CLEAR licensing system. The State System does not have to prevent MMTCs from creating new usable products and/or marijuana delivery devices for price setting.
BF-5.5	The State System must allow for the tracking and tracing of data from MMTC/CMTL Systems regarding product returns, including reason for return, date of returned product, and disposal.
BF-5.6	The State System must be able to record each unique identifier required for a dispensing transaction from each MMTC/CMTL Systems.
Transportation	
BF-6.1	The State System must at a minimum, automatically flag a retail batch that has failed regulatory compliance testing.
BF-6.2	The State System must allow for the tracking and tracing of data from MMTC/CMTL Systems regarding a given retail batch that is distributed to multiple dispensing facilities.
BF-6.3	The State System must allow for the tracking and tracing of data regarding transportation manifests that are compliant with section 381.986(8)(g), Florida Statutes.
BF-6.4	The State System must have the ability to receive and store PDF documentation of transportation manifests generated from an MMTC/CMTL System in accordance with section 381.986(8)(g), Florida Statutes.
BF-6.5	The State System must allow for the tracking and tracing of data regarding a retail batch (or portion thereof) to dispensing facilities and track/trace backwards from the product dispensed to the patient in the event of a recall.
Reporting	
BF-7.1	The State System must have the ability to produce ad hoc reports on all data elements including metadata, in addition to the requirements listed within this Reporting section.
BF-7.2	The State System must have the ability to produce reports electronically, in a specified format (e.g., CSV, PDF) and for a given timeframe, including, but not limited to, the reports regarding cultivation, processing, laboratory testing, transportation, organization-level, facility-level dispensing history, patient-level dispensing history, medical marijuana product availability, medical marijuana product utilization, destruction, returns, and production statistics.

BF-7.3	The State System must produce reports electronically, in a timeframe and specified format (e.g., CSV, PDF) as determined by the Department, for the gross sales of medical marijuana, including the facility in which the marijuana was cultivated, processed, and dispensed.
BF-7.4	The State System must generate, in real time, a file of dispensing data on demand, using the standard specific to version(s) mandated by the Department, so the Department is able to know when a product has been sold to a patient or caregiver.
BF-7.5	The State System must allow for the tracking and tracing of data from MMTC/CMTL Systems regarding all returned usable product (including RFID, barcode, and/or unique identifier number) and marijuana delivery devices and document the reason for the return.
BF-7.6	The State System must allow for the tracking and tracing of data from MMTC/CMTL Systems to generate an inventory checklist (e.g., cycle count) on demand to resolve an immediate inventory discrepancy.

II. HARDWARE AND HOSTING

Hardware and Software	
HH-1.1	The Vendor shall provide all equipment, including hardware (e.g., servers), software, and other infrastructure necessary to aid the Vendor in meeting the requirements of this contract at no additional cost to the Department, including any licenses that must be procured and maintained. Note: Hardware and other infrastructure necessary does not include mobile devices, RFID tags, barcodes, unique number identifiers, barcode scanners, tag readers, POS registers, or other accessories.
HH-1.2	The State System web interface must be robust enough to accommodate multiple types of electronic devices, for example, tablets and mobile devices, and multiple operating systems.
Hosting Environment	
HH-2.1	The Vendor shall maintain a hosting environment secured as described in the Department's IT Security Policy to provide required services under this Contract. Hosting infrastructure must be physically located in the U.S. and prohibit access from outside the U.S. to the data in the State System. **Note:** Vendors may propose commercial cloud services that meet the Department's IT Security Policy.
HH-2.2	The Vendor shall have an alternate secure site available in the event that it is not possible to restore operations in the primary site within the Recovery Time Objective (RTO) of four (4) hours as described in the Department's IT Policy.
HH-2.3	The Vendor must provide separate Quality Assurance and Training environments identical in configuration to the one in production and such environment must be accessible by the Department for testing, prototyping, and training. Testing requirements are listed in TE-1.1 through TE-1.3. User acceptance testing, workflow development and creation of job aids are three of the tasks that are necessary. **Note:** SLAs and support will be discussed during negotiations based on the solution offered by the vendor.
HH-2.4	All State System data will be owned by the Department and will be retained for the Department for a duration of the remaining portion of the current year, plus six (6) additional years, and will be backed up, co-located and replicated to be in compliance with State requirements. In addition, upon contract termination, expiration, or upon demand by the Department, all data must be provided to the Department using an agreed upon format and method of delivery at no additional cost to the Department.
HH-2.5	The State System proposed should be robust enough with configuration or customization to accommodate core functionality, customized reports, and data.
Hardware and Hosting Services	

HH-3.1	Vendor agrees to perform all tasks considered normal and routine for the State System services consistent with the scope of this ITN.
Network, Server, and Application Security	
HH-4.1	All software, including operating systems and middleware, used to host the system shall be patched no more than one month after patch availability to minimize security vulnerabilities.
HH-4.2	Vendor must have a process to manage internal staff and external user accounts and system access permissions compliant with Department standards.
System Management and Monitoring	
HH-5.1	The Vendor shall monitor all servers and applications in accordance with Department standards.
HH-5.2	The Vendor shall use appropriate automated and manual tools and processes to monitor performance, as well as prevent and detect unauthorized access.
HH-5.3	The Vendor must specify the configuration of hardware and software platforms on which the State System will be implemented, as well as their configurations.
HH-5.4	All servers and devices shall have currently supported and hardened operating systems, employing up to date anti-viral, anti-hacker, anti-spam, anti-spyware, and anti-malware utilities.
HH-5.5	The Vendor must secure an SSL certificate.
HH-5.6	The State System must retain a history of all network and application accesses including a history of all transactions performed while the user was logged on. This information must be retained in accordance with Florida's General Records Schedule, GS1-SL.
HH-5.7	The Vendor shall restore the system, online availability, and database functionality (includes front-end) within recovery time objective (RTO) of four (4) hours of a disaster affecting the service provider's data center. RTO is the maximum acceptable (tolerable) period in which the system may be down for an unexpected, unplanned event. This includes applying transaction iterations to the disaster recovery system up to the point where the production system was when it went offline. The Vendor must also maintain a Recovery Point Objective (RPO) of one (1) minute. RPO is the maximum acceptable (tolerable) period in which data might be lost from an IT system because of a major incident.
Business Continuity and Disaster Recovery	
HH-6.1	The Vendor shall define, implement, and exercise adequate business continuity and disaster recovery procedures. These procedures will be reviewed and approved by the Department prior to implementation.
HH-6.2	The Vendor shall develop business continuity and disaster recovery plans that address the recovery of business, hardware, software, and data that meet the Department recovery time and recovery point objectives.
HH-6.3	The Vendor shall adhere to a defined and documented back-up schedule and procedure, including regular, full, and incremental back-up.
HH-6.4	The Vendor shall conduct and annually verify the proper functionality of its back-ups, off-site data storage, and restore operations.

HH-6.5	Back-up media shall be securely transferred from the primary site to another secure location to avoid data loss.
HH-6.6	Data on media transferred outside of a secure facility shall be encrypted with an algorithm and key approved by the Department.
HH-6.7	The Vendor must maintain a disaster recovery site located away from the main site where the primary system is hosted.
HH-6.8	The State System must be flexible to account for customized reports of the data storage and data backup information (e.g., SQL Enterprise).

III. SECURITY AND PRIVACY

Organization	
SP-1.1	The Vendor shall identify the primary information security officer that possesses a widely recognized information security certification.
SP-1.2	The Vendor shall develop and provide a comprehensive information security, privacy, and confidentiality plan within thirty (30) business days of contract approval by the Department. The plan is subject to Department approval
SP-1.3	The Vendor shall schedule security review meetings which include DOH, OIT, and pertinent Department staff at least monthly. Such meetings may be in-person or virtual.
SP-1.4	The Vendor shall provide a security risk assessment at least annually.
SP-1.5	The Vendor shall comply with all applicable laws and procedures pertaining to security and confidentiality including, but not limited to, those listed in the Department's Information Technology policies and those contained in Attachment D, Standard Application and Data Security/Confidentiality Policy. The Department's Information Technology policies are contained in Attachment E, Department of Health Information Security and Privacy Policy, Attachment F, Collection, Disclosure, and Safeguarding of Social Security Numbers, and Attachment G, Access Control of Social Security Numbers. In the event of any conflict between the terms in Attachment A and Attachments D, E, F, or G, the more stringent term shall govern.
SP-1.6	The Vendor must fulfill regulatory requirements to which the information system will be subject to, including, but not limited to, the following: • Section 282.318, Florida Statutes, "Information Technology Security Act" • Sections 282.601 - 282.606, Florida Statutes, "Accessibility of Information and Technology" • Florida Administrative Code Chapter 60GG-2 "Information Technology Standards" • Florida Administrative Code Chapter 60-8 "Accessible and Electronic Information Technology" • Chapter 119, Florida Statutes, "Public Records"
SP-1.7	The Vendor must fulfill regulatory requirements to which the data held within and processing performed by the system will be subject to, including, but not limited to, the following: • Section 501.171, Florida Statutes, Florida Information Protection Act of 2014 (FIPA) • Section 381.987, Florida Statutes, "Public Health: General Provisions"
SP-1.8	The Vendor will work with the Department on application compliance. Existing application and infrastructure security controls will be evaluated against current polices. If needed, the Vendor will configure, troubleshoot, and monitor security related tools and technologies to protect the Department from cyber risks.
SP-1.9	The Vendor will work with the Department on activities pertaining to the development and maintenance of a security program. It will work with the Department to identify opportunities to enhance and track compliance with the security program.

SP-1.10	The Vendor must provide System Access reports documenting all access granted to the system and all successful attempts to gain access to the system.
Operations	
SP-2.1	The Vendor shall: • Provide to the Department, in writing, evidence of security testing of State System prior to release for use; • Provide to the Department, in writing, the contents of the system for third party certification program and proof that it can be reconciled without loss of data or security; • Demonstrate what level of system security will be provided using such artifacts as reports, third party audit results, etc.; and, • Demonstrate security capabilities around processes and personnel.

IV. TESTING

TE-1.1	Development testing must include at a minimum: Unit, Integration, System, Regression, Interface, Performance, Usability, Stress, User Acceptance Testing (UAT), Parallel, Software Patching and Fix, and Business Continuity Testing (Disaster Recovery) Testing.
TE-1.2	The Vendor shall: • Design, implement, and manage Test environments, including the developer (DEV) environment, systems test (ST) environment, and user acceptance test (UAT) environment; • Design, implement, and manage from a detailed testing work plan that is integrated into the overall project management plan; and, • Design testing documentation to include, at a minimum: testing approach, detailed test plans, expected results, testing schedules, test scripts, and defect tracking.
TE-1.3	All patches and updates shall be fully tested prior to implementation in the production environment. The Vendor will maintain a test environment to be used for such testing, as well as other functions as may be required.

V. PROJECT MANAGEMENT AND STAFFING

Project Management	
PM-1.1	The Vendor shall provide a Project Management Professional (PMP)-certified project manager with a minimum of 8 years' experience in software solutions who will be responsible for management of the project to ensure successful completion of the scope of services. The project manager (PM) will follow an "agreed upon" approach based on established project management best practices following Project Management Institute (PMI) / Project Management Body of Knowledge (PMBOK) recommended methods. Subject matter expertise in the cannabis industry is preferred but not required.
PM-1.2	The Project Management Plan shall abide by Rule 60GG-1, Florida Administrative Code, and include, at a minimum: • Use of a Project Manager • A kick-off meeting and initial working session • Project Scope Statement • Project Schedule, to integrate with the master schedule for the overall program • Project Budget • Quality Management Plan • Risk Management Plan • Change Control Process • Acceptance Management Process • Issue Management and Escalation Process • Communication Management Process • Organizational Change Management Process • Development and Management Plan for Project Resources • Implementation and Transition Plan • Regular project management meetings, and status reporting Unless otherwise directed or approved by the Department, the Vendor shall maintain a project schedule using a Department-approved software tool. Project schedule is subject to review and approval by the Department. The project schedule must include a relevant and sufficiently detailed work breakdown structure (WBS). The project schedule shall clearly identify predecessor and successor activities, task dependencies, deliverables, key milestones, milestones, and critical path. The project schedule shall be baselined. Actuals will be tracked and variance from baseline will be measured and reported on a weekly reporting cycle. Any significant variance from baseline or re-baselining of the schedule must be submitted for review and approval by the Department. The Vendor shall confer with the Project Director (or his/her designee), as necessary, to assess the impact and likelihood of occurrence of identified risks. The Vendor shall develop risk mitigation plans for identified risks based on risk rating, as directed by the Department. The Vendor shall effectively collaborate with the Department PM to utilize the risk log maintained by the Vendor and identify the most critical project-level risks that need to be reported on the overall project status report and potentially escalated to the Steering Committee.

PM-1.3	The Vendor shall ensure that the configuration, implementation, and transition plan for the State System and its seamless integration with other components of the medical marijuana program are such that the overall project objectives are achieved on time and on budget.
PM-1.4	All project artifacts and deliverables will be submitted for review and must be approved by the Department. **Note:** The Department uses SharePoint, Microsoft Teams, and MOVEit for collaboration and sharing of documents. The Department is not purchasing such document sharing systems through this procurement.
Project Tracking and Status Reporting	
PM-2.1	The Vendor shall track progress against the project schedule and report status in a format approved by the Department. The Vendor project lead or designee will also work closely and collaboratively with the Department project manager or designee to provide status and other related updates specific to the State System implementation on a monthly schedule to be finalized in a timely and comprehensive manner to support the generation of the overall project status report.
PM-2.2	During development and implementation, the Vendor shall provide daily status briefings on production operations. Beyond immediate implementation for the first thirty (30) days of the system being in production, the Vendor shall provide weekly status briefings of production operations.
PM-2.3	The daily and weekly status briefings shall include, at a minimum, an assessment of progress against plan, any slipped or slipping tasks, risks and issues, mitigation plans, and changes needed to the Go- Live Plan or Transition Plan.
PM-2.4	The daily and weekly status briefings shall include, at a minimum, an assessment of progress against plan, any slipped or slipping tasks, risks and issues, mitigation plans, and changes needed to the implementation plan or transition plan.
Risk, Issue, Decision, and Action Tracking	
PM-3.1	The Vendor shall provide an open communication method with which team members and stakeholders can collaborate on project risks, issues, decisions, and action items as directed and consistent with the Department's project management methodology.
Meetings	
PM-4.1	Unless otherwise designated or approved, all project meetings shall take place at State offices in Tallahassee, FL. Project meetings may be virtual, at the discretion of the Department.
Reports and Information Access	
PM-5.1	The Vendor shall provide ad hoc progress reports, data, and information as requested by the Department.
Project Documents and Artifacts	
PM-6.1	The Vendor shall maintain a repository, accessible to State staff, of all project documents and artifacts and maintain a version history of all project documents and artifacts.

Ownership of Information	
PM-7.1	Data, information, and reports collected or prepared by the Vendor as part of the project shall be deemed to be owned by the Department.
Contract Transition	
PM-8.1	The Vendor shall develop and submit, three (3) months prior to conclusion of the Contract, a detailed transition plan to facilitate the seamless transition of the responsibility of the system operations to another entity. The transition plan should, at a minimum, include procedures for data erasure, documentation, and cooperation in moving the system to a different entity while maintaining all agreed service levels at all times. The plan is subject to Department approval.
PM-8.2	The Vendor shall cooperate with any new Vendor and with Department staff to ensure that all existing data is supplied and that any data and/or code and documentation needed to provide continuity of the project is supplied to the Department and de-identification and consolidation methods are fully transferred.
PM-8.3	Data shall be transmitted or supplied as directed by the Department. Any transfer media shall become the property of the Department.
PM-8.4	At the end of the contract and following approval by the Department, the Vendor shall securely destroy all program data held or stored by the Vendor.
Staffing	
PM-9.1	The Vendor project manager will be responsible for maintaining and managing a current resource plan at all times and report on any related significant issues or changes. Should it become necessary to replace key staff, the Vendor will notify the Department as soon as the need arises, shall provide replacement staff members with equal or superior skills and qualifications, and shall ensure sufficient time to complete knowledge transfer before the replaced staff is off-boarded, when possible. The Vendor shall obtain the Department's approval of the replacement key staff. Key staff, at a minimum, includes the positions identified in PM-9.2, below.
PM-9.2	Staffing shall include, at a minimum, the following positions: • Engagement Manager (Senior Executive) • Project Manager (primary point of contact for the Department project manager) • Configuration Lead (responsible for architecting all technical aspects of the State System, leading the configuration and initial setup of the State System to meet the specific needs of the Department, and unit/integration/system testing of the same) • Implementation Lead (responsible for leading the user acceptance testing, the implementation, the user training, the rollout, and the post-implementation support) • Other staff members as necessary to implement the project
Quality Assurance	
PM-10.1	Throughout the duration of the project, the Vendor shall perform routine quality assurance measures as planned in the quality management plan. The quality management plan shall ensure the software, data, and all other supporting processes to accomplish daily operation tasks adhere to a set of quality checks to assist in proactively identifying potential risks associated with the project and any project lags. The Vendor must communicate its plan.

Correction of Deficiencies	
PM-11.1	Any corrections of deficiencies relating to the Contract Scope of Services requirements or deliverables, and any investigation necessary to determine the source of such deficiencies, shall be completed by the Vendor at no cost to the Department.

VI. TRAINING

T-1.1	The Vendor shall provide training for the Department including, the Office of Medical Marijuana Use (OMMU), and Office of Information Technology (OIT). The schedule for these trainings should be planned in consultation with the Department and provided to the Department with sufficient notice which will allow for at least ten (10) business days for coordinating attendance.
T-1.2	The Vendor shall provide the recorded webinar training. This training must include each of the topics as specified in this section and any other materials identified by the Department or the Vendor that would aid the Department in the utilization of the State System.
T-1.3	Training must include, at a minimum, the following topics: • Software configuration; • User administration; • Security features; • Password reset instructions; • Data mapping for MMTCs or CMTLs to upload data from their MMTC/CMTL Systems to the State System • Functionality related to the inventory and chain of custody management for the manufacture, transportation, laboratory testing, transport, distribution, recall tracking, dispensing, sale, and reporting of medical marijuana; • Reporting features; • Interfaces with other State data systems; • FAQs/troubleshooting documentation; and • Train-the-trainer for Department personnel.
T-1.4	The Vendor shall track and maintain training enrollment and completion status for all persons authorized by the Department to access the system, as stipulated by the Department, and produce daily status reports for the duration of the training. The Vendor shall develop and deliver training material in electronic and paper format for classroom training.
T-1.5	The Vendor must provide training manuals and guides for modules specific to approved system user access groups.
T-1.6	The Vendor must provide a plan to train Department staff, on how to operate the State System within thirty (30) days of contract execution. The plan should include, at a minimum, the training schedule (dates and times) and the content of the training, which is subject to review and approval by the Department. The Vendor must provide training to Department staff when the State System has upgrades or scheduled changes impacting the operation of the system or MMTC/CMTL Systems. The Vendor must provide a separate and distinct system training environment dedicated for training purposes including train-the-trainer for Department personnel. The Department will provide infrastructure (e.g., classroom facilities, audio-visual) for such training.

VII. MAINTENANCE AND SUPPORT

Support Service Objectives	
MS-1.1	The Vendor shall provide reasonable, consistent, high quality-delivery of support and maintenance services for the State System for the duration of the contract.
MS-1.2	The Vendor shall oversee and maintain the State System so that all software and hardware (e.g., servers – physical or virtual, scanners, ODAs, storage, switches, firewalls) are current and supported technology, as deemed appropriate for State business functions.
MS-1.3	The Vendor shall provide support services via a call center, e-mail support and web-based support for the term of the contract to designated representatives. The Vendor shall provide access to Vendor's support resources for quick resolution, feedback, troubleshooting, and support. All Vendor personnel providing the support services pursuant to this Attachment shall have expertise and be fully trained in issue (incident and problem) identification and resolution or escalation relating to the State System and interconnection of MMTC/CMTL Systems. Vendor personnel shall provide access to Vendor's software engineering and technical resources for quick resolution, feedback, troubleshooting, and support. All incidents and problems shall be logged in designated on-line support management software. The reported incidents and problems shall be viewable in detail and summary format by designated representatives.
MS-1.4	The Vendor shall provide to the Department monthly maintenance and support reports in a mutually agreed upon format. The report(s) shall document past performance, future scheduled maintenance activities, scheduled and unscheduled downtimes, and system changes.
General Support Requirements	
MS-2.1	Upon termination of the Agreement, the Vendor will provide or make available an encrypted copy of the Department's data to the Department. Upon written acknowledgement of verified receipt and decryption of the data by the Department, the Vendor shall irreversibly erase all State data from its systems. The Vendor shall also certify, in writing, that the action has taken place.
System Management and Monitoring	
MS-3.1	The Vendor will notify the Department about unscheduled downtime prior to the unscheduled downtime taking place if they are aware in advance. In the event that the unscheduled downtime is unknown prior, the Vendor shall notify the Department within one hour of the event and complete required reports as prescribed in maintenance and support requirements.
MS-3.2	The Vendor shall notify the Department in writing of cyber or physical security issues within one (1) hour of becoming aware of an issue. The Vendor shall also provide a monthly report, in writing, about cyber or physical security risks.
Maintenance and Updates	

MS-4.1	The Vendor shall periodically deploy scheduled releases of the State System into the State System technical environments.
MS-4.2	Except in cases of emergency, the Vendor shall notify the Department, in writing, at least thirty (30) days prior to activating each maintenance update, software upgrade, or other scheduled change. If it is determined that additional time is necessary to address any impact on the integration of the State System with other system components of the overall solution including MMTC/CMTL Systems, the maintenance update, software upgrade, or other scheduled change shall be rescheduled to a later date as mutually agreed upon by the Vendor and the Department. Notification shall include the following, at a minimum: • Date of maintenance update, software upgrade, or other scheduled change activation; • Notes describing the maintenance update, software upgrade, or other scheduled change content; • Date, time, and duration of time required to deploy the maintenance update, software upgrade, or other scheduled change; and, • Results of tests that document satisfactory test run of the maintenance update, software upgrade, or other scheduled change in the pre-production (staging) environment of the State System.
MS-4.3	Vendor shall apply continuous quality assurance efforts and resources (“24 hours a day, seven days a week”) to resolve any defect, malfunction, or bug in the State System identified by the Department, otherwise brought to Vendor’s attention, or a defect, malfunction, or bug of which Vendor should reasonably become aware. The Vendor must notify the Department in writing of its plan for resolving a defect, malfunction, or bug within 24 hours of the Vendor’s awareness of the defect, malfunction, or bug. Then the Vendor is responsible for providing daily updates to the Department until the defect, malfunction, or bug is resolved.
Maintenance Schedule	
MS-5.1	Vendor shall perform, at a minimum, routine scheduled maintenance on a regular basis to ensure proper operation. The maintenance shall be within the service levels defined. The maintenance shall be performed between the hours of 11:00 PM eastern time on Saturday and 6:00 AM eastern time on Sunday. The Vendor shall provide the Department with 72 hours advanced notice, in writing, of scheduled maintenance whenever possible.
MS-5.2	Vendor may need to perform emergency maintenance, such as when a service capability cannot be met by a nonperforming application with no workaround, or when necessitated by a security patch installation or hardware replacement. The Vendor shall provide the Department with notice of emergency maintenance in accordance with the change management as defined.
Update Management	
MS-6.1	Activities include services required to appropriately manage and document changes to the application(s) and/or any of the State System (hardware, software, hosting, etc., excluding services related to implementation) components. Update management also includes services required to appropriately manage and document changes to the underlying State System hardware and software components.

MS-6.2	The Vendor shall install all hardware and software patches, maintenance updates, and other utilities according to vendor recommendations, as required to maintain system operations and security. All critical patches shall be applied within thirty (30) days of general release, or sooner if requested by the Department.
MS-6.3	The Vendor shall coordinate activities with the Department prior to any requested or required changes to the State System and hosting platform that may affect the service capability performance of any of the MMTC/CMTL System environments. Any changes to the State System must be managed consistent with the SOW and documented change management procedures defined during the State System implementation.
Monitoring and Reporting Services	
MS-7.1	Vendor shall provide monitoring and reporting services that include the activities associated with the ongoing surveillance, tracking, escalation, resolution and reporting of application development problems. These problem management activities require coordination with the designated help desk. This monitoring shall include, but is not limited to: • Monitoring the health of the application and notifying the operations team of potential issues; • Monitoring the connections between the State System and MMTC/CMTL Systems or other integrations; • Monitoring for critical exceptions within the application; • Monitoring the transaction and login rates for capacity and security; • Monitoring the connections between the different layers of the system and the public internet; • The Monitoring Plan shall provide a specific list of all physical devices (if dedicated hardware is used to host the State System), hosts, ports, URLs, Web sites and other components that are required to be actively monitored. • The Monitoring Plan shall include the provisions for the detection of actions that attempt to compromise the confidentiality, integrity, or availability of resources or data. • The Vendor shall generate and provide to the Department system usage and performance reports on a monthly and on an exception basis, including the following: • Server up-time and down-time; • All outages, including issue and resolution; • All changes, patches, and upgrades implemented; • System access; and, • Any other issues and resolution On a monthly basis, Vendor shall provide to the Department a consolidated list of major activities being performed, their status, and plans for the next reporting period.
MS-7.2	Vendor must provide service level management activities that include applying a severity level to each reported issue, monitoring, and monthly reporting of SLA activity.
MS-7.3	Vendor will be required to adhere to performance standards and service levels including, but not limited to Technology Support Center Availability, Application Availability (Application Availability—web/mobile (internal user), and

	Application Availability—web/mobile (external user)), As-Built Documentation Maintenance, Application Guides, Restore of Backup Media, Backup/Archive Management, Security Management, Passwords (establish security profiles to govern employee and agency access to sensitive data, Inventory Tracking and Maintenance, Resolve Critical Problems (without workaround), Resolve Critical Problems (with workaround), Resolve Non-Critical Problems (without workaround), Resolve Non-Critical Problems (with workaround), Software License Management Support, Security Management Services, Disaster Recovery, Project Management, Key Staff, Key Staff Vacancies, Technical Reviews and Meetings, and Status Reports. Specific performance standards and service levels will be negotiated based on the vendor's solution.

VIII. SYSTEMS CHANGE MANAGEMENT

SCM-1.1	Costs for System enhancement projects will be based on hourly rates (to be established during negotiation of this ITN).
SCM-1.2	The State System needs to have the ability to perform enhancements using established procedures and in a manner that expects changes as a result of user growth, changing legislation, improvements in software and hardware, and strategic planning.
SCM-1.3	Version control must be enabled to facilitate the restoration of an application to prior development stages as a result of maintenance, tracking and auditing of modifications to an application's components over time.
SCM-1.4	Turnover Management must be practiced during the promotion of software changes across different phases of the life cycle (e.g., development, unit test, systems test and production), including management of the approval process, production turnover, and software migration control.
SCM-1.5	Vendor shall provide enhancements to the State System at the request of the Department, throughout the contract term. All enhancements must be requested in writing, and the Vendor must provide a scope of work documenting the estimated number of hours for each position assigned, the position hourly rate (rates will be established during negotiation) and estimated total of the work.
SCM-1.6	Vendor shall respond in writing within five (5) business days of receipt of a request by the Department to make an enhancement to the system. The response must include a preliminary assessment of the number of hours required to perform the enhancement.
SCM-1.7	No enhancement will be performed until written approval is received as specified by the Department.
SCM-1.8	The system must support any enhancements or changes that will be required by the Department.
SCM-1.9	The system needs to be easily enhanced. Explain how you will be able to add new categories, new license types, test types and the ability to add and remove fields.