Section VI., Statement of Work

A. System Requirements

1. Describe how the proposed System meets applicable OIT Technical Standards and Policies

As the State's current [redacted] system provider, the [redacted] System already fully complies with all applicable OIT Technical Standards and Policies.

As the State's inventory tracking system vendor, COMPANY currently meets or exceeds all applicable OIT Technical Standards and Policies. We do so by aligning our operations with SOC security controls and the NIST 800-53 framework.

COMPANY's security practices are based on the NIST frameworks, specifically NIST 800-53 and the NIST Cybersecurity Framework (CSF). These controls provide structured, risk-based guidance for protecting systems and data. Key areas include the following: access control (who can access the System and how), audit and accountability (tracking user actions), incident response (preparing for and managing security events), system integrity (ensuring only approved changes are made), and data protection (securing sensitive information during storage and transmission). Implementing these NIST controls helps ensure that the System meets or exceeds federal, state, and industry cybersecurity standards.

COMPANY also undergoes regular SOC 2 audits, which independently validate that the System meets the TSC for our controls relevant to applicable Security, Availability, and Confidentiality.

2. What are your security certifications and compliance standards?

The System meets several key security and compliance standards:

- **SOC 2 Type II –** Independently audited by A-LIGN, confirming strong controls for security, availability, and confidentiality.
- **PCI-DSS (Payment Card Industry-Data Security Standard) –** Certified as compliant, with third-party validation of secure handling of payment data.
- **NIST 800-53 –** Implements and audits controls based on this federal cybersecurity framework.
- **OWASP (Open Web Application Security Project) Top 10 –** Developers are trained and code scanned to address the top security risks.
- **Veracode Verified –** Ongoing application security testing is integrated into the development process.

COMPANY also ensures secure handling of PII (Personally Identifiable Information) through encryption, access controls, logging, and compliance with OIT and Government Data Advisory Board standards.

3. Do you perform regular security assessments and penetration testing?

Yes, COMPANY performs regular security assessments and penetration testing. COMPANY conducts annual penetration testing as part of our security controls. Additionally, the System undergoes external penetration testing at least yearly and system vulnerability scans at least

quarterly. These assessments are integral to our security practices to identify and remediate vulnerabilities effectively.

4. What is your data retention policy?

COMPANY's default data retention policy is seven years for client data and one year for system backups. All data is stored in COMPANY's primary and disaster recovery databases and remains accessible (based on user roles) for the full retention period. To date, all data has been retained for our agency partners, including the State. As the State's retention period nears its end, we will coordinate on data removal or archiving options.

5. How do you handle data backups?

We handle data backups through a managed backup solution where backups are encrypted in compliance with FIPS 140-2 standards. A third-party vendor performs the backups and stores them off-site in a geographically separate Azure data center.

Full database backups are performed nightly, and differential database backups occur at least every four hours. Backups are periodically restored to verify their functionality and to practice restoration procedures. Additionally, backups are copied to a disaster recovery location within the continental U.S. The systems are subject to at least an annual audit (e.g., SOC 2, etc.).

For archiving and removing data from the System, we will define a mutually agreed-upon permanent storage medium with the State.

6. Can you provide details about your access controls?

COMPANY follows NIST 800-53 standards for secure user identification and authentication. All user accounts—internal staff, agency partners, and approved external agencies—are managed through a consistent, State-approved process.

Authentication – COMPANY uses secure forms authentication and cryptographically generated access tokens for web and API access. This token-based approach protects credentials and enhances system integrity.

Authorization – The System employs role-based access control, assigning permissions based on job functions. All user actions are logged for at least two years in a secure, separate datastore, ensuring full auditability.

Role-Based Security – State administrators can create, assign, and modify user roles with specific permissions at any time. Changes take effect immediately for all assigned users, streamlining access management.

Multi-Factor Authentication (MFA) – COMPANY supports and recommends MFA for enhanced security, particularly for State administrators. MFA uses time-based one-time passwords (TOTP) via popular free apps like Google or Microsoft Authenticator. Enabling MFA may qualify the State for additional cyber liability insurance, which can be discussed during contract negotiations.

7. How do you handle data when the contract ends?

COMPANY will securely destroy all held or stored program data at the end of the contract, upon approval by the State. We will collaborate with the State to determine what methodology we will use to destroy the data.

8. How do you manage user authentication and authorization?

We manage user authentication and authorization through a combination of robust processes and technologies:

Authentication:

- The System validates a user's identity before granting access. It leverages forms authentication (e.g., cookies, anti-forgery tokens) for external users accessing the web interface.
- RESTful interfaces are authenticated via cryptographically randomly generated access tokens, which are unique and highly secure, reducing the risk of credential compromise.
- MFA is offered and recommended for enhanced security.

Authorization:

- The System employs a role-based security framework to approve user actions post-authentication. User roles, defined by State administrators, determine access levels and permissions based on job functions.
- Permissions are granular and can be adjusted by State administrators at any time, with changes taking immediate effect.
- Authorization activities are fully auditable, with logs stored separately for performance and integrity, retained for at least two years, and accessible to State administrators.

9. Do you have a user access log?

Yes, the System maintains a user access log. Every System user logs in with their own unique identity, and the System records the login along with every transaction and transaction modification the user performs. That includes capturing their username, the action completed, the date, and the time at every step. These logs are retained for a minimum of 12 months.

10. Can you provide role-based access controls?

Yes, we provide role-based access controls. The System uses role-based security for System access and supported functionality. Administrators can create and maintain new and existing users, define permissions based on user type or individually expressed permissions, and add individual roles and/or read-only access to other areas within their purview. Defined user roles can be adjusted at any time by the State. Role changes take effect immediately for all users assigned to the role.

11. What's your procedure in case of a data breach?

Our conscious effort to maintain a highly secure system has paid off, with **no known data breaches or successful cyberattacks in the history of the System.** However, in the event of a data breach, COMPANY will take the following steps.

Within 24 hours of reasonably believing that a disaster or catastrophic failure has occurred, we notify the State's designee by the fastest method possible and notify the State's Chief Information Security Officer in writing. The notification will include the nature of the data breach; the data accessed, used, or disclosed; the person(s) who accessed, used, disclosed, and/or received data, if known; what COMPANY has done or will do to quarantine and mitigate the data breach; and the corrective action COMPANY has taken or will take to prevent future data breaches.

We provide daily updates (or more frequently, if the State requires) regarding findings and actions performed by COMPANY until the data breach has been effectively resolved to your satisfaction.

12. How quickly do you notify clients about security incidents?

We notify the State within 24 hours of reasonably believing that a significant security incident, disaster, or catastrophic failure has occurred.

13. Does your insurance cover data breaches?

Yes, COMPANY's insurance covers data breaches.

14. How do the security processes and access controls relate to the varying sensitivity of different data stored?

COMPANY's security processes and access controls are tailored to the varying sensitivity of data stored by implementing measures such as data classification according to sensitivity levels, encryption, tokenization, masking/obfuscation, and authorized-use system access controls. For sensitive data, encryption strength is proportional to assurance-level requirements, and encryption keys are protected and managed for data recovery and forensic investigations. This structured approach ensures clear categorization of sensitive information, enabling appropriate access controls, minimizing risks, and maintaining compliance with privacy regulations. By aligning data processing with these classifications, we maintain transparency while implementing robust security measures across both internal personnel and external data centers that handle sensitive data.

Access controls are based on NIST 800-53 security requirements, including role-based security, MFA, and authorization processes that approve users to perform activities based on their assigned roles and security levels. These controls are regularly audited, reviewed, tested, and updated to ensure compliance with federal and state standards, such as NIST SP 800-122 and SOC 2 Type II audits, and to minimize the risks of unauthorized access or data leakage.

15. What measures do you have in place to identify and protect PII within the data?

To identify and protect PII within the data, we classify all data according to sensitivity levels and implement operational controls and privacy-enhancing technologies. These measures include fields identifying all confidential data, encryption, firewalls, authorized-use system access controls, and system audit logs.

In accordance with NIST SP 800-122 and NIST 800-53, we deploy solutions that monitor network communications and prevent sensitive PII from leaving our networks. Additionally, administrative policies such as acceptable use procedures, confidential data procedures, and

email procedures are enforced, alongside security training to safeguard information privacy and control access to System data.

Our security program undergoes continuous monitoring and external verification, including SOC 2 Type II audits, to ensure the effectiveness of these controls.

16. How do you handle data masking or de-identification of PII for non-production environments?

The System does not store authentication credentials or sensitive data in its codebase for production systems or in unencrypted databases or files. The static code analysis performed against the System's first-party code detects flaws in the event that sensitive data is mistakenly or maliciously included. For non-production environments, all environments are preloaded with demo data to ensure features can be used without exposing sensitive PII.

17. What are the different ways in which different types of users, such as data entry users versus data analyst users, access information in the system?

Data entry users access the System through its user-friendly Graphical User Interface (GUI), which allows them to manually enter data, upload bulk data via CSV (comma-separated values) files, or integrate their enterprise software into the System via API. They can perform tasks and enter product data based on their role, with real-time access to the System and its data.

System users can access entered data in a variety of ways, including the searchable grids, real-time reporting in COMPANY's Control Panel, and COMPANY's standard dashboards, on top of normal day-to-day navigation within the System. State users with specific access permission have the ability to run light queries against the System database.

Should the State exercise the option to procure REPORTS, State users will have two additional data access options:

- REPPORTS provides predefined reports, dashboards, and workbooks for robust data analysis capabilities. We provide thorough details about REPORTS in response to section VI.B.1.
- COMPANY offers REPORTS customers direct access to the COMPANY Data Warehouse for more granular data analysis. User-defined queries can be stored, shared, and run on demand. Also, most ETL (extract, transform, load) tools can connect to the COMPANY Data Warehouse as they would with any other database, providing the ability to schedule and automate extracts. With direct access to the COMPANY Data Warehouse, State technical users can pipeline data from it to Data Analysts or recipients of their choosing.

18. Is there a code-based access point for authorized users, both internally and for state users?

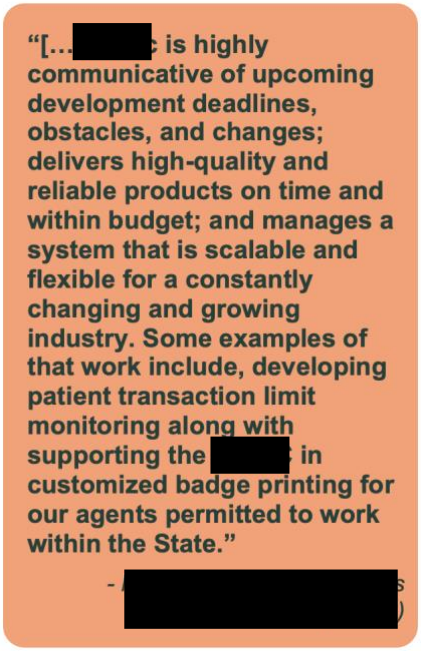
No specialized code-based access point is required to access our web-based software-as-a-service (SaaS) solution, which is accessible via modern web browsers. The System leverages forms authentication (e.g., cookies, anti-forgery tokens, etc.) as an application-integral component to authenticate external users when accessing the web interface. Additionally, the System's RESTful interfaces are authenticated via access tokens, which are cryptographically random generated strings. These tokens ensure secure access for both internal and State users.

19. How can the system receive data from other sources in an ongoing manner?

The System enables receiving data from other sources in an ongoing manner through multiple methods, including user entry, bulk uploads, and our secure, web-based API. The System supports integration with external systems, such as licensing and registry systems, and allows licensees to input data directly or integrate their enterprise software, such as POS systems.

The System's mature RESTful API architecture facilitates real-time data exchange and integration with hundreds of third-party systems daily. Data transmitted through the API receives immediate format and validity feedback, ensuring seamless and ongoing data reception.

Additionally, the System offers CSV upload capabilities for various industry needs, serving as a backup if API capabilities are unavailable.



<<< NEW SAMPLE SECTION >>>

c. Required Functionality

COMPANY has provided details about all required functionality listed in RFP VI.B.1-18 in response to questions 1-5 in this section. We have mapped where each item is addressed in the following table for the State's convenience.

Required Functionality from VI.B:	Addressed in Response to:
1, 17, 18	VII.B.3
2, 3, 4, 5, 6, 7, 10, 11, 12, 13, 14, 15, 16	VII.B.1
8	VII.B.5
9	VII.B.4

2. Describe the ability to configure and customize the System.

The System is extremely adaptable and enables changes to be made quickly and efficiently as laws, regulations, and user needs evolve. Historically, over 90% of regulatory partner requirements are typically met by configuration of the current System, meaning that less than 10% of requirements require custom development work. As noted previously, we have determined that the System meets OOTB every system and functional requirement included in RFP VII.E except one, which will be completed during implementation and before go-live.

The System was intentionally designed to be highly adaptable to ensure it can exceed all of our regulatory partners' needs when it goes live and can support future program growth and regulatory changes. One key to achieving that level of adaptability is our single-code-base approach: every regulatory partner receives an individualized and separate instance of the

System, but each is built on a single code base. The instances are configured to each partner's unique needs, which also helps ensure the separation of data, processes, and users. As COMPANY makes enhancements in response to requests from partners, we often make the updates available across all instances. The new features are created as a "switch" and are turned on or off based on the decision of each partner for their instance of the System. Any partner may opt-out, but the approach provides the option for them to benefit from the experience and improvements made by other regulators.

Since 2018, the State has leveraged nearly 100 system enhancements developed at the request of other partners for its instance of the System.

Configuring & Customizing the System

One of COMPANY's first steps in working with the State to configure and customize the System to meet new requirements is to conduct a Fit/Gap Analysis. The Fit/Gap Analysis involves evaluating every RFP requirement against the current functionality of the State's System instance to validate as a "fit" (current functionality meets the requirement) or identify a "gap" (additional development is required for functionality to meet the requirement). The Analysis is reviewed with State stakeholders and becomes the foundation for project development work and implementation. The Fit/Gap also enables us to identify needs that may not have been recognized in the State's RFP requirements—our analysis frequently identifies items that lead to new requirements.

To configure the System to meet partner requirements, we use a Testing environment that includes all available features and configurable items in the System. We then work with the State to identify the baseline functionality and items that require configuration. Following that, we begin the change control process to document, develop, and review System updates with the State. We confirm the configurations through UAT and user training. Since COMPANY is already operational in State, the Fit/Gap analysis and configuration steps will be completed in significantly less time than it would take to implement a new system.

For requirements that cannot be accommodated through configuration, COMPANY follows a document development process, involving the following steps:

- COMPANY's Product team reviews the RFP and proposal and submits any identified modifications for review with the State.
- Once we receive authorization from the State, the Product team provides the requirements, the proposed solution, and, in some cases, wireframes or a prototype to the Development team.
- Based on that input, development work begins as follows:
    - We assign the work to one or more Developers based on the expertise needed and what area of the System is involved.
    - Development leads hold scheduled team meetings as required.
    - The Release Coordinator monitors progress and addresses any roadblocks by involving appropriate resources.
    - The Product team is always available to help clarify regulatory partner requirements and answer related questions.

After development work is completed, unit tests run automatically to validate functionality. Development leads then perform a thorough code review, examining both the technical implementation and adherence to coding and quality standards. Once the code passes this review, it is merged into a testing build, during which it is also scanned for security vulnerabilities. The finalized testing build is then deployed to a Quality Assurance (QA) environment for further evaluation.

State-Configurable Items

The System also offers numerous items that can be configured directly by the State's administrator, giving the State control to adjust administrative elements to keep it in sync with the State's intricate day-to-day regulatory activities. State configurable items include rules-based configurations, user roles and security levels, account creation, reporting options, data dashboards, multiple search options, audit tracking, system alerts, administrative holds, and other common functions. State-configurable areas include the following: License Types, Employee Types, Item Categories, Action Reasons, Administrative Hold Reasons, Transfer Types Limits, Lab Test Types, Waste Types and Methods, Location Types, Occupations, and Remediation Methods.

State-configurable items are designed to be easy to use and provide self-service functionality. But should the State ever need assistance, COMPANY's team will provide any necessary support.

3. Describe how to accomplish required interfaces and integration.

The following describes how the System accomplishes required integration; it also addresses RFP VI.B.1, 17, and 18.

The System provides a secure, web-based API for integrating external information systems, data, and hardware, and COMPANY has significant experience coordinating and implementing our System with other vendors to integrate both regulatory and enterprise software solutions.

Regarding vendors that offer regulatory solutions, we have extensive experience working with the following solutions, vendors, and IT staff in various states, as follows:

- XXXXX – regulatory solution in State
- XXXXX – patient registry and/or licensing solutions in STATE, STATE, and STATE
- XXXXXX – patient registry and/or licensing solutions in STATE, STATE, STATE, STATE, and STATE
- XXXXX – regulatory solution in STATE
- XXXXX – regulatory solution in STATE
- XXXXX – regulatory solution in STATE
- XXXXX – online system for PRODUCT and liquor licensing and permitting in STATE
- XXXXX – regulatory solution in STATE
- Custom solution built on Pega – regulatory solution in STATE
- Custom-built, in-house – regulatory solutions in STATE, STATE, STATE, and STATE

Regarding vendors that offer enterprise solutions, over 300 software providers have active integrations into the System nationally, including POS, inventory management, cultivation management, ERP, and LIMS (of these, 120 are integrated with State's System instance). For example, integrated POS providers include XXX, XXX, XXX, XXX, and XXX and integrated ERP and inventory management providers include XXX, XXX, XXX, and XXX.

Integration with other systems is achieved via the System's API—nationally, hundreds of third-party systems connect to the System every day through the System's mature RESTful API architecture. The System's robust API defines data standards for upload from other systems and allows for real-time system integration via secure web service. It includes an out-of-the-box RESTful JSON interface to receive external data (e.g., license and patient information) into the System. Data transmitted through this interface receives immediate format and data validity feedback from the System.

"Working with [redacted] over the course of the last several years has been nothing short of an outstanding experience. [redacted]'s industry-leading product has a robust set of APIs that makes integration a breeze. The [redacted] team is world class and is always a pleasure to work with. We've integrated our cannabis patient registry and cannabis business licensing system with [redacted] in several states, and each integration has been a tremendous success, creating a streamlined experience for regulators and industry stakeholders alike."

- [redacted]

Web Services control integration with external sources. The System's web services are created using C#, HTML5, RESTful methodology, and JSON and contain the following parts:

- **Regulatory –** Exposes the regulatory reporting functionality via secure API.
- **Industry –** Exposes the industry workflow functionality via a secure API, allowing third-party solution providers to optimize licensees' business processes.
- **Licensing –** Supports a RESTful integration with regulatory licensing solutions.

Integration with Licensees' Third-Party Solutions (e.g., POS, ERP, etc.)

COMPANY manages third-party business solutions for licensees through our integration portal. We designed our integration portal to provide robust and efficient integrations with the System and deliver an exceptional customer experience. It includes up to 50,000 calls per month and up to 2 calls per second per integrator.

Some of our integration portal's benefits include the following:

- **Endpoints,** over 150 unique endpoints.
- **Pagination,** which eliminates the need to do work natively in code, improves reliance on expected data return, and enables fast data pulls.
- **Webhooks** to create workflow efficiencies and offer real-time visibility into customers' activities.

COMPANY will continue to support integration with new and existing third-party systems throughout the implementation and the contract's duration.

Integration with Regulatory Systems

The System supports integration with external systems through its robust API, which allows for secure, real-time data exchange. The API includes endpoints for various functionalities, such as

regulatory reporting, industry workflow, and licensing. Additionally, the System can send data and reports to external systems via secure web services, such as SFTP (Secure File Transfer Protocol) or Azure Blob storage.

COMPANY has extensive experience integrating with external licensing systems through our internal, secure API, and our flexible approach to engineering new features allows for integrations to new systems such as Case Management. We also have the capabilities to integrate with the State's Data Lake.

Data can be exported in industry-standard formats, including CSV, Excel, PDF, and more. COMPANY will work with the State to ensure that the data is provided in a mutually agreed-upon format.

4. Describe the proposed ongoing maintenance and support.

The following response describes COMPANY's proposed ongoing maintenance and support; it also addresses how we support training due to changes in the System as required by RFP VI.B.9.

Ongoing Maintenance & Support

COMPANY provides ongoing maintenance and support through a comprehensive M&O Plan, ensuring the System remains current, secure, and adaptable to evolving needs. Preventive maintenance is prioritized to avoid application problems and component failures, and routine maintenance is performed while the System is online to minimize downtime. Non-routine maintenance requiring downtime is scheduled in collaboration with the State, with advance notifications provided to end users. Updates are deployed using automated tools to reduce errors, and COMPANY communicates release notes and provides demonstrations and documentation to the State during the testing phase. Continuous and automated monitoring takes place to ensure a fast response in case of system degradation. Furthermore, the COMPANY CSM acts as the primary point of contact for daily operations (including weekly status meetings with the State) and any requested configuration modifications or enhancements. This helps ensure that both the System and our services continue to meet the State's evolving needs.

Additional information on how COMPANY maintains, upgrades, and supports the System is provided in the following responses.

Training Due to System Changes (addresses RFP VI.B.9)

COMPANY provides various training options to ensure users can use new functionality effectively and efficiently:

- **Guidance Bulletins –** Issued by the Customer Success team to highlight functionality changes, workflows, and best practices, including links to supplemental training. **For State, COMPANY has released over 100 Bulletins to licensees and the State showcasing numerous new System features over the course of our current partnership.**
- **AUTOMATED INTELLIGENCE –** Embedded in the System, offering real-time guidance, step-by-step instructions, and searchable features that allow users to ask questions and

receive AI-powered assistance. AUTOMATED INTELLIGENCE is updated before new System functionality goes live.

- **Technical Manual/User Guide –** Covers all industry functionality in a single location. It will be available via AUTOMATED INTELLIGENCE and will reflect System updates when new functionality goes live.
- **State User Guide –** Helps State staff use the System proficiently. It will be available via AUTOMATED INTELLIGENCE and will reflect System updates when new functionality goes live.
- **COMPANY Trainings –** COMPANY updates the New Business Training, Advanced Trainings, LMS Journeys, and State training to reflect System changes that affect functionality so that users who take these courses are proficient in using the System's most current functionality.

"I really enjoy the new feature of [redacted] as well as [redacted]. Looking forward to more trainings from [redacted] for our staff."

- [redacted]

- **TPI Training –** Includes API instruction to ensure a baseline understanding of the System and concludes with a required test. TPIs also receive customized system and API documentation, including user manuals and developer guides. The API documentation is updated as needed to reflect any related System updates.