RFP XXXX: <<State Name>>

Child Care Exchange Solution Description

v.01232026

Table of Contents

1.0 Overview

Agency XXXXX is responsible for the licensure, inspection, and monitoring of the State's child care providers and facilities to ensure that children are being cared for in safe, healthy, and nurturing environments. The Agency performs various functions such as professional development, instructor approval, course approval, provider and staff fingerprinting and background checks, facility and home inspections for licensure, and providing resources and referrals to families and others seeking child care options. In addition, the Agency is responsible for the eligibility determinations and case management of the child care assistance program. It is critical that the Agency provides an efficient and manageable process to support families in need of financial assistance and child care.

Agency XXXXX is seeking proposals for the design and implementation of a comprehensive, fully integrated, modular early childhood data management system. The system shall function as a configurable platform or "off-the-shelf" product that incorporates best practices and minimizes the need for code-based customization. The Agency intends to procure an existing child care solution that is in operation in at least one state. The result of this procurement will be a new, comprehensive, fully integrated, modular early childhood experience for families, child care providers, and the Agency. This will be accomplished by multiple modules that integrate to function as a single system that has relevant functionality for internal and external users and shall meet the desired goals of the Agency. The Agency expects proposed solutions to meet the needs and expectations as described within this RFP. The desire to reduce complex customizations is meant to encourage an expedited implementation timeframe to support the Agency's needs.

The State desires a modular solution to incorporate the following programs and processes into a modular, next-gen fully integrated system that has robust functionalities for all users. The modules included in this RFP are:

1. Module 1 – Integrated Child Care Marketplace: Provider Portal with attendance tracking; public-facing Family Portal with shopping, resources, and referral tracking.
2. Module 2 – Workforce Credentialing, Development, and Training: Fingerprint coordination, Learning Management System (LMS), training approval and tracking, and provider-facility licensing and renewals.
3. Module 3 – Child Care Assistance Eligibility: Eligibility pre-screen, rules-based determination, provider payment, case management.
4. Module 4 – Business Intelligence and Reporting: Integrates with other modules and provides historical and near-real-time reporting capabilities for all program and functional areas.

The solution description provides Offeror with the opportunity to describe their proposed solution and elaborate on how the solution will meet the State's requirements. The response must include a thorough description of the solution, the overall approach to implementing the solution, and the approach to addressing each requirement.

The State expects that Offeror will address each requirement in its response. Due to the detailed nature of many requirements, the State expects that, in some instances, individual statements, paragraphs, or other content may be sufficient to address multiple requirements simultaneously.

The State has identified three (3) phases for the Contract term.

1. Phase I – Start-Up Phase: Business-process evaluation and a detailed product review/conceptual design.

2. Phase II – Implementation Phase: Includes development encompassing the design, build, testing, and installation of the new integrated system.

3. Phase III – Maintenance and Operations Phase: Maintenance, enhancements, and periodic system releases for any modules for one (1) year following the system's Go-Live date. Transfer of the system along with knowledge transfer will also be included in this phase. Transition approach shall include a no-cost license to the base product, a reasonably priced maintenance agreement for bug fixes and security patches at the agreed rate cards, and rights for the State to host the product for a determined amount of time.

This solution description includes baseline requirements and is intended to be updated throughout the procurement process as appropriate. This solution description is a template that aligns with the categories of the solution requirements contained in this RFP. They include:

Functional & Technical Requirements		**Implementation Requirements**
• Consumer Shopping • User Portals • Application, Eligibility, and Enrollment Management • Notice Management • Provider Management • Provider Payments • Learning Management • Communications & Engagement • Integration with Verification Data Source • Parent and Child Scheduling • Attendance Tracking	• User Experience • Consumer and User Support • Document Management • Data Management • Reporting and Analytics • Availability &Performance • Solution Architecture • Integration & Interoperability • Quality Assurance & Solution Audit • Security and Privacy: Data security and integrity, security and privacy regulations, and standards • Provider Licensing Module	• Implementation Support • Maintenance & Operations (M&O) • Capacity, Scalability, & Extensibility • Disaster Recovery & Business Continuity • Project Management & Governance • Project Schedule • Training • Data Migration

2.0 Instructions

Offeror must submit the solution description as part of its RFP response submission. The file must be used in its entirety as the template to provide Offeror's narrative responses to the items requested in the exhibit.

The technical proposal and cost proposal should be uploaded as separate documents and identified as such.

Proposals should be accompanied by the attached Proposal Price Sheet and signed by the proper official of the firm. All proposals should be submitted through the State online bidding system. Proposals sent by facsimile, email, or paper copy may be rejected.

Proposals should be submitted through the State online bidding system on or before the date and time

specified. Proposals received after the date and time specified may be rejected.

The State reserves the right to withdraw this Request for Proposal without cause at any time before a contract has been fully signed and submitted to the Procurement Office.

Specific instructions for preparing the solution description include the following:

1. Offeror will modify the electronic version of this solution description, as provided by the State with the RFP materials, to respond to the requirements herein and by completing all sections within this document. Offeror will refrain from modifying section titles or removing sections.
2. Offeror may remove the State-provided guidance shown in each section and any instructions.
3. Although sections are related, Offeror should refrain from repeating responses in subsequent sections. Offeror must tailor each section's response to the request in that section.
4. Offeror does not need to restate the requirements; rather, Offeror should articulate how their unique solution will meet the requirements.
5. Offeror will include materials specific to their solution for this RFP. Offeror will refrain from providing "marketing materials" and background information already provided to the State or otherwise available in the public domain.
6. Offeror will return the completed file as part of its overall response to the RFP, in accordance with the submission and file-naming requirements indicated in the RFP instructions.

Please note that the solution description is intended for Offeror to further describe and elaborate on its solution. Any proposed changes to solution requirements must be noted in the Offeror response.

Offeror may submit the full bid of the project (all modules), partner with another vendor to provide those services, or bid on individual modules without the full project bid.

The solution description must contain the components listed in Section 3.0 of this exhibit and in the order specified.

3.0 Functional and Technical Requirements

The Agency XXXX defined the requirements stated herein and created this RFP.

THE REQUIREMENTS/SPECIFICATIONS ARE MANDATORY REQUIREMENTS. THEY ARE SUBJECT TO VARIATION AND MODIFICATION ONLY THROUGH WRITTEN APPROVAL OF THE AGENCY.

3.1 General Requirements

Offeror shall describe the overall approach to meeting the General Requirements of this RFP. The response shall explain how the proposed solution and services satisfy the requirements identified in this section and shall include a description of the Offeror's methodology, assumptions, and any dependencies relevant to successful implementation and ongoing operations. Offeror's response should demonstrate an understanding of the Agency's objectives and clearly articulate how the proposed approach supports those objectives.

3.1.1 Communication Requirements

A. Offeror shall provide a single point of contact and a Communication Plan. It shall encompass objectives,

goals, and tools for all communications, including top-down, bottom-up, and cross-organizational communications.

B. Offeror shall provide weekly project status reports and submit them to the Agency Project Manager. Status reports must outline the project's progress updates by including key issues, identified unknown risks, accomplishments, and compliance with milestones and delivery dates.

3.1.2 Equipment Requirements

Offeror shall provide all electronic and telecommunications equipment supporting the Contract, including but not limited to: file servers, database servers (development and testing), application servers (development and testing), and personal computers.

3.1.3 Functional Requirements

A. Module 1 – Integrated Child Care Marketplace

This module will include the Family Portal and the Provider Portal. The goal for the **Family Portal** is to provide families with a seamless, end-to-end, and integrated user experience to apply for child care subsidies, receive a no-touch eligibility determination, shop for available child care providers meeting the needs of the family, and enable enrollment with a provider of choice in a single virtual interaction. The same experience must be available for families not needing child care financial assistance.

The goal of the **Provider Portal** is to allow child care providers to complete the licensure and certification processes (applications and renewals), upload background check documents, list their business(es) and services, and manage invoicing processes with the Agency for any child care assistance cases.

1. Family Portal

The Family Portal is designed to allow each family to:

a. Search for and secure all child care needs based on individual need.

b. Conduct a pre-screening of potential eligibility and benefits using a benefit calculator-type function without initiating an application.

c. Apply for child care subsidies and receive a no-touch eligibility determination.

2. Family Portal: Application for Child Care

a. The application shall be dynamic and with questions tailored to each family's specific circumstances.

b. No-touch eligibility shall have the tools to verify attested family circumstances against State, commercial, and public systems to enable real-time decisions.

c. Data elements shall be used to make an automated eligibility determination.

d. Eligibility determination shall be conveyed to the family in real time to allow for instant and no-touch eligibility results.

e. Eligibility determination and verification sources shall be automatically transferred to the

Agency's child care eligibility assistance system for the next Agency action. This may require integration with the Agency's document management technology.

f. Allow families to access their application status.

g. Provide the following for situations in which no-touch eligibility is not successful:

   i. Allow the family to upload required documents to determine eligibility.

   ii. Allow Agency staff to review and take action on any documents that have been uploaded.

   iii. Connect and integrate with the child care assistance eligibility system.

   iv. Ability to display a minimum of three (3) language selections.

h. Provide communication functionality that includes, at a minimum, the following capabilities:

   i. Ability for each family to securely communicate with the Agency if experiencing issues with establishing child care assistance eligibility (i.e., email, text [SMS]).

   ii. Ability for each family to report changes.

   iii. Communications between each family and the corresponding provider so the family may request enrollment with that provider and allow the provider to confirm enrollment.

i. Allow families to compare to and select from child care providers based on various criteria.

j. Provide system links to important resources and assistance sites, including but not limited to, the state's QRIS, SNAP, TANF, and WIC.

k. Provide technical-assistance tools within the portal to assist with navigation and functionality of the systems.

l. Allow Agency administrators to have role-based access and the functionality to support families. Functions shall include:

   i. Keeping Agency staff informed, with important data and reports.

   ii. Accessing status of each application.

   iii. Viewing any communications sent or received.

m. The system shall interface in real time with other Agency systems to include but not limited to:

   i. In-rule business rules engine

   ii. Child Care Assistance Case Management System

   iii. Agency-identified work-routing system

   iv. Agency document-management system, if applicable

v. Provider Portal

3. **The Provider Portal** is designed to function as the central hub for providers and shall allow for the following:

   a. Providers to create and easily update their business profiles (e.g., list of services, slot availability, pricing, photographs) that an individual or family can utilize when searching for child care.

   b. If a provider is already in the Agency's licensing management system, then integration shall be required to extract the business information to assist in the creation of that provider's profile.

   c. Each provider to update their profile if any changes to their business profile occur (e.g., phone numbers, hours of operation, days of operation, ages of care and slot availability).

   d. Password management.

   e. Streamlining the facility licensing process by allowing providers to submit an inquiry application and apply for licensure or renewal. License-exempt providers may be allowed to submit necessary requirements for certification to receive child care assistance. The system shall support provider licensing and certification processes through the following capabilities:

      i. The completion and upload of all required documentation, including document generation, document submission, electronic signatures and ability to email forms after being electronically signed. Multiple file types shall be supported (e.g., videos, photos, PDFs, text files, Word).

      ii. The ability for non-exempt facilities to pay licensing fees.

      iii. The uploading of third-party and/or external inspection documentation.

      iv. A work-routing technology solution that integrates with the licensing management system and routes uploaded documents to Agency staff for required action. Any status or determination related to application, renewal, or certification shall be conveyed to the provider in real time.

      v. All providers, whether licensed or license-exempt, shall have the ability to view requirements for certification and training.

   f. Roles and titles may be given to provider personnel (e.g., owner, director, staff, and non-staff).

   g. Attendance tracking to include the following functionalities:

      i. Generate attendance sheets for each authorization based on the child's schedule entered by the parent or family member.

      ii. Require providers to verify each child's attendance and confirm accuracy prior to payment processing.

iii. Use verified attendance information to calculate subsidy payments due to providers.

iv. Track payment adjustments for external payments made to providers outside of the system.

h. The system shall provide communication, notification, and technical assistance functionality that includes, at a minimum, the following:

i. Ability for the provider to securely communicate via email with the Agency if experiencing issues with application, recertification, and profile management. Such communication shall be routed to the licensing staff.

ii. Ability to ingest and deliver/display electronic provider notifications, generated from the licensing management system.

iii. Advanced notifications to the provider or educator that credentials are missing or in need of renewal.

iv. Initial notifications to appeal any negative actions taken against provider licenses or registrations.

v. Text (SMS) functionality to communicate with and receive responses/inquiries from providers such as child care slot availability.

vi. Integration with the Agency's existing licensing management system.

i. Provider technical assistance shall include technical assistance, access to needed trainings, and technical assistance tools that assist with navigation and functionality of the system.

j. Connection to and integration with the Agency's existing licensing management system, specifically:

i. A display of visits, internal and external inspections, and violation information.

ii. Aggregate data on child deaths, maltreatment, and serious injuries, with a preference for automatic integration with the Agency's child welfare information system.

iii. Actions taken by child care providers that would lead to the issuance of a license, registration, and/or certification.

k. The system shall provide payment functionality that includes, at a minimum:

i. The use of a statewide card processor

ii. Documentation of any exception where use of a statewide card processor is not feasible, including a clear explanation of the reasons.

l. The system shall integrate with the Agency's existing payment mechanism to support provider fee payments. At a minimum, the system shall provide the following capabilities:

i. Ability to integrate with, receive, and present providers with an invoice from the child care assistance eligibility system.

ii. Ability to interface with the State's financial accounting system and ingest payment status updates.

iii. Secure notification of completed payment to the family and provider.

iv. Reporting and reconciliation functions for providers.

m. The system shall provide Agency administrators with the following:

i. Role-based access and functionality to support families.

ii. The ability to be easily informed and to inform others, as needed, with important data and reports (e.g., dashboards, trends)

iii. Access status of each application, renewal, or certification.

iv. View any communications sent or received.

n. The system shall interface in real time with other Agency and State systems, including but not limited to:

i. Licensing management system
ii. State fiscal system
iii. Family Portal
iv. Workforce credentialing, development, and training
v. Central Registry
vi. Agency's payment solution for application and background-check fees
vii. Early childhood integrated data system

4. There must be functionality connecting the Family Portal and the Provider Portal to enable families to apply for child care assistance, search for providers, and enroll with a selected provider. The system shall support this functionality by providing the ability to:

a. Enable secure communication between families and providers, including the submission, receipt, acceptance, and confirmation of enrollment requests.

b. Provide facility and program search functionality in both text-based and map-based formats, allowing families to filter results by zip code, county, hours of operation, provider type, age group, slot availability, date of last inspection, corrective actions taken (if available), family needs or circumstances, and the results of internal and external monitoring and inspection reports, including substantiated major complaints.

c. Integrate with the licensing management system to support provider eligibility and status verification.

d. Support participation by licensed and license-exempt providers.

e. Require multi-factor authentication (MFA), in addition to username and password, for access to all portals.

f. Provide navigational videos and informational tips to assist users with system workflows

and navigation.

B. Module 2 – Workforce Credentialing, Development, and Training

Module 2 includes a Learning Management System (LMS) that supports the training, technical assistance, tracking, and growth of early childhood education programs, educators, providers, and instructors and sponsors (Module 2a), as well as workforce credentialing for central registry and fingerprint checks (Module 2b). Offeror's system must be capable of integrating with the existing LMS and accessible through the self-service child care provider portal. This system should have the capabilities to support virtual communities of practice and asynchronous trainings.

1. **Module 2a – LMS and Training Module** must provide the following functionalities:

a. Meets the standards of the Partnership Eligibility for the National Workforce Registry Alliance for program integrity and accountability and the CDA Council requirements for professional development reporting.

b. Allows actions taken in user portals and/or modules to trigger work items and actions in other relevant portals and/or modules within the system.

c. Integrates with the appropriate portals and other system components to support system-generated training prompts, business rule–driven referrals for required post-training actions, and notifications to users when credentials or certifications are nearing expiration.

d. Allows users to complete training, quizzes, surveys, and required documentation on unlimited topics and through available training organizations.

e. Provides training online through webinars, learning forums, real-time chat, and potentially other digital methods.

f. Includes a user dashboard that shows user activity, learning-opportunity enrollments, completed trainings, earned certificates, progress toward earning certificates and career ladder, action items, and other information.

g. Allows users to view and register through a training catalog that includes the ability to filter information.

h. Includes training and training evaluations and trainer approval and competency assessments.

i. Allows sponsors to request course approvals, communicate with course registrants, submit course credit for attendees, change course credits after approval, monitor course status, and create course expiration dates.

j. Includes a calendar that allows users to see upcoming learning opportunities and provides users with the ability to filter information.

k. Allows the system to generate a transcript or professional development reports so the user may easily demonstrate cumulative professional development and training that adheres to the Council for Professional Recognition.

l. Allows the user to be affiliated with and visible to multiple employers.

m. Allows employers to access educator and staff professional-development reports, verify employment, upload documents, create educator goals and track progress, and create other canned and ad hoc reports.

n. Allows for translation from English to Spanish and for the user to maintain a preference each time they log into the system.

o. Includes the ability to import, export, process files quickly, and generate multiple types of reports, including reports that are canned, ad hoc, and demonstrate course completion.

p. Allows an unlimited number of system users and tracks and reports which user entered information into the system.

q. Allows a single sign-on for all parts of the system for which the user has access rights to include other Agency systems.

r. Interfaces with federal and other Agency systems that include:

   i. Learning Management System (LMS)

   ii. Provider Portal

   iii. Central Registry

   iv. Early Childhood Integrated Data System

2. Module 2b – Workforce Credentialing

Background checks must be completed on each child care educator, provider staff, and non-staff. The work includes processing background checks for both in state and out of state. Background checks must be processed pursuant to federal requirements. This module should include the following functions:

a. Allow actions taken in the Provider Portal and/or modules to trigger work items and actions in other relevant portals and/or modules within the system.

b. Integration with the Provider Portal so users may request a background check and submit completed fingerprint cover letters and DCI waiver and release forms as well as forms required for the applicant's review process.

c. Back-end management of background-check forms to allow the Agency to upload files to a background-check record as well as the ability to log and track incoming requests and outgoing results.

d. Generation of the appropriate label for program type/reason for fingerprint cards.

e. Document upload and management capabilities.

f. System communication with the submitter/provider through the system via email or the messaging system.

g. Generation of letters and documents for printing or electronic delivery including electronic

signatures.

h. Reports and dashboards for advanced reporting and data analysis.

i. Integration with the State's payment system to accept electronic payment of processing fees.

j. A single sign-on for all parts of the system for which the user has access rights to include other State systems.

k. An interface with federal and other State systems to include the licensing management system, the Provider Portal, and the Early Childhood Integrated Data System.

C. Module 3 – Child Care Assistance Case Management System

1. This module should encompass case management and significant business rules–engine functionalities with customized workflows associated with eligibility determinations. This module also should support correspondence management or provide customer relationship management (CRM) functionality. The module should include, but not be limited to, the ability to interface with federal and other state systems such as:

    - SNAP and TANF
    - Child welfare
    - Child support
    - Licensing management
    - State fiscal
    - Fraud and recovery
    - Utility assistance
    - Early Childhood Integrated Data

2. Eligibility Information
    a. The Agency owns all client eligibility information that may be extracted and/or obtained from any Agency application by Offeror for analysis purposes and transferred to Offeror's owned technology resources/media. Upon termination of the services, for any reason, Offeror agrees to return all original eligibility information and any derivative work to the Agency in a usable format. Delivery must be through a secured electronic transmission in accordance with NIST guidelines for data in transmission/data at rest and must include secure disposal of identified/de-identified data.

    b. Following the Agency's verified receipt of the original eligibility information and derivative work, Offeror agrees to physically and/or electronically destroy or erase all residual eligibility information regardless of format from Offeror's entire technology resources and any other storage media or areas. This includes, but is not limited to, all production copies, test copies, backup copies, and/or printed copies of information created on any other servers or media and at all other Offeror sites. Offeror will provide a record of data destruction to the Agency for inspection and records retention no later than 30 days after destruction.

    c. If, for any reason, the eligibility information cannot be returned and/or destroyed upon termination of services, Offeror agrees to notify the Agency with an explanation as to the conditions that make return and/or destruction impossible. Upon mutual agreement by

both parties that the return and/or destruction of the data is not possible or feasible, then Offeror must make the eligibility information inaccessible to those purposes that make the return or proper destruction impossible. Offeror must provide the Agency with a detailed description of the procedures and methods used to make the eligibility information inaccessible no later than 30 days after making the data inaccessible.

D. Module 4 – Business Intelligence and Reporting

This module will provide self-service business intelligence and analytics with reporting capabilities necessary for State and federal compliance. Near-real-time reporting and transmission of data into the State's data warehouse is expected. This module should include, but not be limited to, the following functions:

1. Static/historical and near-real-time reporting of all program and functional areas
2. Visualization of data and drill-down capabilities
3. A semantic layer that allows end users to perform self-service reporting within the scope of their security and access rights
4. User-defined reports and views based upon different roles and security profiles of various stakeholders.
5. The ability to export report results to common data formats (e.g., Excel, CSV, PDF, Word)
6. An easy-to-use web-based library of canned reports for viewing, printing, and download
7. The data model and definitions of the system and bi-directional integration into the data warehouse
8. Full access to all data points collected in the software
9. Dashboard views of aggregated data with drill-down capabilities, including the ability to view and analyze data across multiple dimensions (e.g., geographic location, type, or party) and to identify trends
10. The ability to interface with other State systems to include but not be limited to:
    a. Existing licensing management system
    b. State fiscal system
    c. Family Portal and Provider Portal (shown as Module 1 in this RFP)
    d. Workforce Credentialing, Development, and Training (shown as Module 2 in this RFP)
    e. Central registry
    f. Child Care Assistance Case Management System (shown as Module 3 in this RFP)
    g. Early Childhood Integrated Data System
    h. Federal systems that provide real-time data
    i. State and federal systems unable to provide real-time interfaces
11. A single sign-on for all parts of the system for which the user has access rights to include other Agency systems.

3.2 Technology and Specifications

The Agency is seeking a solution that meets all, or as many, of the functional and technical requirements as possible. The software can be purchased or licensed, giving the Agency the right to own, install, configure, and operate the software. The Agency places a high priority on a system that is efficient, intuitive, user-friendly, accessible, and reliable. The Agency shall be responsible for the management and configuration of the software beyond the initial project period. Offeror's solution shall be configurable to meet the specific needs and

practices of the Agency, as well as successfully interface with necessary external systems to ensure federal and State compliance. Any existing modules or systems to be integrated into the newly built system will continue to be managed by the respective vendor.

3.2.1 Offeror Description and Approach to Technology and Specifications

Offeror shall describe the proposed technology solution and technical approach for meeting the requirements outlined in this RFP. The response shall explain how the proposed software, architecture, and technical components meet the Agency's functional and technical requirements and support an efficient, intuitive, user-friendly, accessible, and reliable system.

3.2.2 Technical Architecture Requirements

The Agency system architecture defined for the system shall be highly configurable and use a development layer with pre-built, case management–specific, mobile, and cloud applications. The goal of this architecture is to enable the Agency to build a system that promotes modularity, interoperability, and a high degree of reusability that is configurable. If Offeror proposes a solution that is not highly configurable, then Offeror must provide an explanation in the Technical Proposal as to why it would be in the Agency's best interest. Offeror shall create a Design and Architecture Plan to demonstrate the following:

A. Offeror shall utilize cloud-based technology wherever advantageous to maximize the efficient and effective utilization of technology. The Agency architecture shall include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and/or Software as a Service (SaaS). The cloud-based system model shall be hosted on a FedRamp-compliant Cloud Service Provider (CSP).

B. The system shall enable the Agency to develop Application Programming Interfaces (APIs) that support automated data exchanges, including APIs that use Extensible Markup Language (XML) and web services to allow external organizations to connect automatically. The Agency architecture shall also have an API layer with pre-built connectors, business rules, maps, and transformation capabilities to facilitate bi-directional data exchanges between the new system and the system data exchanges. This eliminates double entry of data and promotes the sharing of critical information.

C. Acceptable technology (hardware and software) encompass SAAS, PAAS, and IAAS, as they fit within the proposal. If IAAS is utilized, then Offeror shall utilize Windows operating system. If the proposal recommends cloud hosting, then the solution shall require FEDRAMP and FIPS 140-2 compliance.

D. Any cloud-based solution proposals will be required to configure logging information (for the entire environment) to be ingested by any applicable State solutions.

E. Cloud-based solutions will implement the State standard solution for compliance status monitoring; alternatives will be considered with State coordination and approval.

F. Applicable documentation and certification must be provided, at a minimum, annually and upon any significant change to the environment. Documentation and certification must include:

    a. Business Continuity Plan (BCP) testing; 4.1.2.1.3.2. Business Impact Analysis Testing

    b. Hardware and software risk assessment report(s), based on NIST or an alternative industry best-practice framework for assessment)

c. Disaster recovery testing

d. Detailed data flow diagrams, to include IP, ports, protocols, and normal operational baseline(s)

e. FedRAMP status

f. ISO 27001, ISO 27017, ISO 27018

g. SOC 2 audit(s)

h. Cloud computing compliance controls

i. Data center locations

j. Physical data center security-testing reports

k. PCI DSS compliance and assessment

l. Security incident response plan(s)

G. If an existing State environment will be utilized, then Offeror must provide details as to the configuration and the operating system.

H. The development of business logic shall utilize a modern development language.

I. The system shall have the ability to interface with the State data warehouse solution.

3.2.3 Device-Agnostic Mobile Accessibility

A. Offeror shall ensure the solution has sufficient mobile capabilities, as defined in this subsection. The Agency would like to provide this valuable customer service feature to clients via portable devices. This shall engage participants and help achieve better business outcomes.

B. Offeror shall provide Mobile Web Applications (MWAs), also known as Mobile Thin Client Applications, within the confines of a mobile device browser.

C. Offeror shall build rich front ends (for both web and mobile apps) from a single model that supports reuse and responsive design. This flexible framework shall help create a single portal that serves components to multiple web-capable devices seamlessly and simultaneously. When a device accesses the portal, the portal detects the device type and automatically serves the content with responsive design.

D. For MWAs, Offeror shall ensure the MWA works in most widely used smartphone and tablet browsers and has the capability to alter formatting based on the device. The MWA shall meet the following criteria:

a. Portal changes that can be reflected on the web app with minimal effort

b. Secure access

c. Sensitive or confidential data lives only on the system infrastructure

d. Secure and tested for vulnerabilities (e.g., attackers cannot present versions of the address bar)

e. Performs both over high-speed wireless networks and bandwidth-limited mobile networks and can establish limits on the amount of data transmitted from server to device.

f. Tracks performance and behavior analytics.

g. Easy to maintain and allows for flexibility in future deployments.

E. Web development shall use industry standards.

F. The system's front-end user interface shall comply with applicable Americans with Disabilities Act (ADA) requirements and Web Content Accessibility Guidelines (WCAG) 2.1 Level AA standards.

G. Interfaces and integration with existing systems shall utilize the technologies in the following order: REST services and flat file (CSV or space delimited).

H. Knowledge transfer shall be conducted with IT staff for maintenance and support.

I. Reliability shall support uptime of 99.9%.

J. Mechanism shall be identified to handle disaster recovery situations with the proposed environment.

K. Security within the application shall be role based, with the ability to restrict access to view individual records or identify data within restricted records. This restriction, however, cannot prevent users from running comprehensive reporting or bulk reporting that may utilize data from restricted records.

L. Allows for single sign-on for all parts of the system for which the user has access rights to include other state systems.

3.2.4 Scope of Activity: State Agency Staff

The Agency is dedicated to providing the necessary staff: executive sponsors, Steering Committee, Agency administrators, subject matter experts for each of the identified functional areas, and any other needed resources.

A. Project Management Responsibilities

i. Monitor Offeror performance.

ii. Meet with Offeror on an ongoing basis to discuss any details or issues related to the project implementation, the schedule for development, conflicts with other activities, and the implementation approach.

iii. Meet with Offeror staff, as necessary, to clarify the requirements in this RFP.

iv. At Offeror's request, provide clarification regarding Agency policy, regulations, and procedures.

v. At Offeror's request, provide clarification regarding Agency policy, regulations, and procedures.

B. User Acceptance Test Responsibilities

i. Review and provide feedback to Offeror, develop test data, and review and approve the

UAT test plan, test cases, scripts, and scenarios once all questions and concerns have been resolved.

ii. Execute User Acceptance Testing (UAT) and validate test results.

iii. Evaluate test results as testing is conducted, identify issues or defects, and document them for resolution by Offeror.

iv. Retest resolved issues and defects, as appropriate.

v. Review final results and provide approval for implementation once all outstanding questions and concerns have been resolved.

C. Implementation Preparation Responsibilities

i. Review and provide feedback to Offeror and approve the format of the intended pilot period once all questions and concerns have been resolved.

ii. Review and provide feedback to Offeror and approve the implementation of the project, including operational readiness as described in the RFP once all questions and concerns are resolved.

iii. Review and provide feedback to Offeror and approve the operational readiness plan once all questions and concerns are resolved.

iv. Estimate number of state resources that may be needed for ongoing system maintenance.

3.2.5 Scope of Activity – Offeror

The following table outlines the minimum system requirements and expectations for Offeror's proposed solution. These requirements define the functional, technical, security, performance, and compliance capabilities the system must support and will be used by the Agency to evaluate the completeness and suitability of each proposal.

#	System Requirements	Description
1	Modern Development Language	Modernization shall result in a system utilizing a modern development language that is actively supported, widely adopted, and suitable for enterprise-scale applications.
2	Existing Functionality	Offeror's solution shall provide functionality that is the same or better as the mainframe's existing application. Reporting shall allow for integration into a data warehouse.
3	Compliance with State Standards & Policies	Proposed applications and integrations shall comply with federal and State IT standards, State IT standards, and statutory mandates for system hardware and development components, such as National Institute of Standards and Technology (NIST) compliances and IRS – Publication 1075.
4	Strong Security	The system will be integrated with the authentication providers being utilized by the Agency or the State.

5	Requirements Development & Detail Design	Offeror shall provide GAP analysis, detailed system design specifications, design walkthroughs, and a detailed functional requirements definition.
6	Data Cleansing/Data Conversion/Bridging	Offeror shall work with staff to cleanse legacy data before its conversion to the updated system and shall perform all conversion and bridging activities. Offeror shall comply with record retention, archives retrieval, and e-discovery as defined in State statutes.
7	Data Security	A detailed data security plan shall be provided and implemented.
8	Application Framework	The application framework shall have been previously used by Offeror in a similar engagement and shall be fully operational in a production environment at the time of proposal submission. The Agency seeks a solution that maximizes long-term flexibility and viability, supports scalability and ongoing maintenance, and minimizes enterprise cost, architectural complexity, and implementation risk.
9	Minimum Processing Requirements	• The system shall be sufficiently sized and appropriately configured for memory, disk capacity, processor speed, and similar or related criteria to meet the performance specified requirements for expected volumes of staff and external users; however, the system shall allow increases in sizing. • The system shall be designed in such a way that the system is “up” and available at least 99.9% of the time (i.e., 24 x 7 x 365). Activities such as maintenance, backups, system change migration, and unattended processes should generally take place while the system is up, minimizing the need for scheduled downtime. • The system shall be architected, configured, and sized so that all functionality (including ad hoc reporting) can be processed online in real time. • The environments used to support the application life cycle (both initial and ongoing) shall provide the ability to integrate new functionality and perform the unit system regression test and the end-to-end test. • Performance testing shall include load testing, stress testing, endurance testing, spike testing, capacity testing, configuration testing, volume testing, scalability testing, and response time. • Performance testing shall also include the identification of “bottlenecks” in the system, test-result walkthrough stage changes, the troubleshooting of production issues, and the training environment. • The production environment shall operate at an undiminished capacity with respect to response and availability requirements. • Application life cycle tasks shall be accomplished independent of, and unfettered by, other tasks related to application revisions in other stages of the life cycle. • Security requirements shall be verified and validated to ensure the appropriate safeguards are in place to prevent unauthorized use such as role-based access control. • Data conversion (transmission) shall be verified and validated to confirm that data converted and migrated from the legacy system is accurate and data is transmitted correctly when interfacing with external systems.

		• Data conversion (received) shall be verified and validated to confirm that data converted and migrated from the legacy system is accurate and data is received correctly when interfacing with external systems.
10	User Authentication	The proposed solution shall interface with the State's existing authentication providers and support multi-factor authentication for designated roles.
11	Gartner PACE Layered Application Model	The service-oriented browser-based application shall have the ability to capture and analyze data on a variety of devices (e.g., desktop computers, laptops, mobile devices, tablets).
12	"Anywhere" Access	Capability shall be provided to allow authorized users to modify documents from a device-agnostic browser.
13	Database Criteria	The database shall use the current release version. If the current release version is not implemented, the version shall be no more than one major version behind the current release and shall be fully supported by the vendor. The database shall have the ability to export any or all data to the State-designated data warehouse or reporting environment data warehouse for reporting purposes.
14	Application Code Criteria	Programming language shall be the current version or no more than one version from the current release version; regardless, the version used shall be fully supported by the vendor.
15	Application Platform Criteria	Web applications shall be the current version or no more than one version from the current release version; regardless, the version used shall be fully supported by the vendor.
16	ADA Compliant	The browser-based application(s) shall comply with applicable Americans with Disabilities Act (ADA) requirements and conform to the Web Content Accessibility Guidelines (WCAG) 2.1 Level AA.
17	Web Server Criteria	The web server shall be the current version or no more than one version from the current release version; regardless, the version used shall be fully supported by the vendor.
18	Operating System Criteria	Linux, Microsoft Windows 10 or later, and Mac iOS with internet access capabilities shall be the current version or no more than one version from the current release version.
19	Integration Points	Integration points shall be defined in advance with associated costs. If Offeror has integration points to orchestrate the data exchange, then the points shall include the ability to integrate with the State data-warehouse solution.
20	Workflow	Workflow should be configurable by an EPICS/JAS administrator, with proper system permissions, to create multiple workflows.
21	Support a Wide Range of Hardware	Software should not require the Agency to use only one specific hardware Offeror but should allow the use of the Agency's existing IT infrastructure as well as new hardware. It shall run on desktops, laptops, mobile phones, and tablets.

22	Mobile Accessibility	Mobile system accessibility shall be provided with offline data entry for end users. It shall improve access to information and data in the field and prevent lost information. All mobile platforms shall be fully supported (e.g., iOS, Android).
23	Simple Access and Retrieval	Multiple methods of searching and the ability to find all related or attached documents shall be available.
24	Reporting Ability	Configurable and customizable reports and metrics shall be provided. Ad hoc reporting shall be easily created by authorized users. The system shall provide real-time reporting and integrate with a data warehouse for ad hoc and other canned reports.
25	Data Migration	A defined migration plan shall allow for the successful migration of data to new versions of the software. The defined migration plan shall have a straightforward option to migrate data to a new application as mandated by State statutes or federal requirements.
26	Legacy Data Conversion	The solution shall migrate legacy data into the application without loss of information and while maintaining data integrity.

3.2.6 Non-API Data Sharing

For organizations without API capabilities, the system shall support delivery of external data extracts via Secure File Transfer Protocol (SFTP) from a predefined secure location on a scheduled basis, in compliance with Agency standards.

3.2.7 System Data Management

A. To support effective program management and administration, Offeror shall design and implement a Master Data Model (MDM) for the entire system. The MDM shall identify and support all program data required by federal and State law, as well as Agency policy and practice, including data used for federal reporting, federal expenditure tracking, and case management activities required for federal monitoring.

   The MDM shall support accurate and current data, comprehensive data traceability, and appropriate data quality documentation. This design requirement shall:

   1. Centralize access to and administration of program data by reducing or eliminating duplicate data collection points and systems.
   2. Enable efficient generation of real-time analytics and ad hoc reporting.
   3. Maintain an inter-relational and normalized data structure.

B. To support effective use of information technology, Offeror shall provide technology capabilities that address current system and operational deficiencies and improve data quality and case outcomes. These capabilities shall include:

   1. Data and analytics: Configurable reports and dashboards that provide access to real-time data, role-based tasks and action items, and system notifications to support operational efficiency and decision-making.

2. Guided intake and workflow integration: Guided, step-by-step data entry integrated with workflow to ensure required data is captured consistently and in accordance with defined business practices.

3. Machine learning: Machine learning capabilities to support prediction of case outcomes and identification of potential risk factors.

4. Matching and de-duplication: Matching logic to identify and prevent duplicate records (e.g., individuals, households, and service records) using standard and configurable matching rules to support data quality.

C. The system shall support a design, development, and implementation (DDI) approach that minimizes duplicative application development and software maintenance. The solution shall allow configuration of pre-built objects and applications and provide any additional custom functionality necessary to meet the system's functional and operational requirements. The system architecture shall promote interoperability, modularity, and reusability through the use of discrete modules and reusable components, including applicable interchange modules. The solution shall support adaptability to changes in federal and State laws and Agency policies.

D. To achieve the data-related objectives, specifications for the system shall include a socio-technical enterprise approach that addresses the human, operational, and IT system interactions that impact data quality to ensure improvement and consistency.

3.2.8 Data Migration

A. Data Conversion and Migration

Offeror shall perform data conversion and migration activities to transform data from required legacy programs into the system. Conversion planning and execution shall ensure data accuracy, integrity, security, and alignment with Agency data-quality standards throughout the conversion life cycle.

B. Conversion Planning

Offeror shall develop and submit a comprehensive Data Conversion and Migration Plan that includes the following:

1. Conversion and migration approach, including synchronization strategy

2. Data mapping and transformation methodology

3. Data cleansing activities, including manual and automated preparation efforts

4. Exception and error-handling procedures

5. Data quality assurance and control measures

6. Conversion and migration risk factors and mitigation strategies

7. Contingency planning

8. Mock conversion and Go-Live schedule

9. Resource management, including staffing, training, facilities, and tools
10. Data security controls
11. Interfaces required to support conversion and migration activities

3.2.9 Data Mapping and Transformation

A. Offeror shall complete data mapping between legacy program data elements and system data models and define transformation rules for all converted data elements. Where source data fields cannot be mapped, agreed-upon default values shall be applied through conversion modules with Agency approval.

B. Offeror shall provide reporting tools and a user interface to document data mappings, transformation rules, and exceptions and to support collaboration with Agency stakeholders in reviewing and validating data translation between programs and system data models.

3.2.10 Conversion Execution and Validation

A. During conversion and migration, Offeror shall ensure that converted data is available in non-production environments (e.g., development and UAT) for testing and verification in accordance with Agency security and data quality policies. The conversion process shall account for and address duplicate records identified in legacy programs.

B. Offeror shall recommend and execute Agency-approved procedures for handling exceptions and errors identified during mock conversion runs, including data cleanup or modification of conversion programs as needed.

C. Offeror shall produce data exception reports for each mock conversion iteration, using predefined, Agency-approved severity levels to support prioritization of data cleanup activities.

3.2.11 System Conversion Capabilities

A. System data conversion and migration routines shall:

1. Maintain data integrity for all converted records
2. Identify records successfully converted and those requiring reprocessing
3. Capture and log system errors (e.g., network or database connectivity failures)
4. Support retry logic to resume processing from a defined point of failure
5. Exclude records based on Agency-defined business rules
6. Support execution and testing of multiple mock conversion cycles
7. Perform file processing during synchronization (e.g., sorting, merging, filtering, de-duplication) before and after batch processing

B. System conversion routines shall not:

1. Convert records that violate the system data model's integrity rules
2. Convert records containing invalid or out-of-range data values
3. Deliverables
4. At a minimum, Offeror shall produce the following conversion and migration deliverables:
5. Data Conversion and Migration Plan
6. Data dictionary, data models, and data flow models
7. Draft conversion and migration results reports
8. Final conversion and migration results reports
9. Go-Live Conversion Scope

3.2.12 Data Quality

A. The system shall provide data quality, validation, and security controls that include the following:

1. Require completion of designated data fields.
2. Encrypt data both in transit and at rest.
3. Validate data formats at the time of entry and during data exchange.
4. Maintain data snapshots to preserve original entry dates, where required for federal reporting and internal audit purposes.
5. Enforce validation rules for data entered directly into the system and for data received through integration points, including validation and translation as needed.
6. Protect Personally Identifiable Information (PII) through secure data exchange between systems and role-based access controls in compliance with applicable State and federal standards, including Federal Bureau of Investigation (FBI) security and encryption requirements.
7. Support Agency practice models, policies, and organizational objectives through system data collection and user interface visualizations, while maintaining historical tracking to manage changes over time.
8. Default all data fields to null, provide appropriate selection options, and associate fields with the correct data structures without duplication.
9. Track required data elements at each workflow event and monitor their collection and entry.
10. Generate alerts and notifications for missing required data elements, including escalation through the organizational hierarchy and real-time notification of improper data formatting at the time of entry.
11. Notify assigned individuals responsible for data completion and support escalation when notifications are not resolved within defined timeframes.
12. Maintain relationships between data fields across objects, avoid unnecessary duplication, and support versioning for fields that persist across object instances with incremental updates.

13. Provide real-time, on-demand reports identifying missing required data elements, viewable at multiple organizational levels, from individual users to system-wide views.

B. Offeror must demonstrate that the system enables specified Agency users to:
    1. Ensure that the data entered is complete, correct, and timely.
    2. Store data in a manner appropriate to federal reporting requirements.
    3. Review data at regular intervals.

C. Offeror shall ensure that data integrations are maintained to allow for updates to fields, required data collection, and data validation as those updates occur and are reviewed at regular intervals.

D. Offeror shall enact changes to remedy deficiencies uncovered by regular reviews of data exchanged across integration points.

E. Offeror shall review data quality and mitigation of deficiencies to inform updates to annual documents submitted to the Administration of Children and Families (ACF) and Office of Child Care (OCC).

F. Offeror shall review compliance with data quality standards and evidence of compliance in annual and supplemental documents submitted to the ACF and OCC.

G. The Agency leads data quality monitoring and reporting efforts, including development of the Data Quality Plan. Offeror shall collaborate with the Agency to ensure data quality can be effectively monitored and reported by ensuring that data mapping, data conversion, and Offeror's master data management (MDM) solution meet data-quality standards and align with the Agency's Data Quality Plan.

3.2.13 Cloud-Based Technology

Offeror shall utilize cloud-based technology wherever advantageous to maximize the efficient and effective utilization of technology.

3.2.14 Workflow-Engine Requirements

A. Offeror shall implement a workflow engine that utilizes forms validation to provide comprehensive data collection and commitment in operational workflow.

B. Offeror shall ensure the system adheres to the following workflow and management specifications:

    1. A workflow management system that drives the Agency's business processes
    2. A method to track key dates
    3. The ability to create and send notifications to both users and specified external parties
    4. The capability to provide default or pre-populated values for information where it is needed
    5. Customizable dashboards
    6. A clear outline of all tasks a user needs to complete
    7. Assignment and reassignment capabilities for specific users

8. Approval capabilities for specific users
9. Locking (of documents and forms) capabilities for specific users
10. Ability to incorporate multi-tier approvals, if necessary
11. Restricted access to certain content
12. Ad-hoc reports and alerts based on user roles and their configurations

3.2.15 Workflow Support Requirements

A. Workflow support includes the maintenance of the system, including user support and ensuring the system functions as intended. The system shall include:

1. Support of the bi-directional exchange of information between the system and other relevant data systems.
2. Use of a business-rules engine that will standardize business practice and trigger specific tasks and events.
3. A structure by which users will be alerted or notified to complete or perform specific tasks, including triggers to complete specific tasks based on established timeframes.

B. The system shall allow users to utilize:

1. Robust search functionalities, including the ability to filter searches through one or a set of user-specified values.
2. Search parameters that include exact matches and partial matches.
3. Search results that can be exported to the Agency in specified formats, printed, and emailed.

C. The system shall include a structure that provides review and quality assurance throughout the system.

3.2.16 User-Support Requirements

A. Offeror shall provide a sandbox environment that mirrors the live environment for training and testing purposes.
B. Navigational videos and informational tips shall be included to assist users with workflow and navigation of the system.

3.2.17 Data and System Security

A. Offeror shall ensure the data within the system is secure. Offeror shall establish a System Security Plan and ensure the system supports compliance with the latest federal and State laws, regulations, and policies relevant to system security, privacy, confidentiality, and safeguarding of information. Where policies overlap, the system must comply with the more stringent policy. The most recent versions of standards and specifications shall be applicable.

B. Offeror shall provide a process for which modifications to the security controls are addressed in future enhancements or maintenance of the system by authorized users or staff to relax or strengthen controls based on policy changes.

C. The system shall be built in compliance with the following security guidelines, acts, and standards as they relate to the respective modules and/or interfaces:

1. Service Organization Control (SOC) 1/2/3
2. National Institute of Standards and Technology (NIST)
3. Federal Information Security Management Act of 2002 (FISMA)
4. International Organization for Standardization (ISO) 27001 and ISO 9001
5. Federal Information Processing Standard (FIPS) 140-2
6. Cloud Security Alliance (CSA)
7. Federal Risk and Authorization Management Program (FedRAMP)
8. Internal Revenue Service Publication 1075 (IRS Pub 1075)
9. Social Security Administration (SSA)

D. The Offeror shall find, hire, and pay a third-party security testing vendor to evaluate whether the solution meets established standards. Results shall be reported to the Agency.

3.2.18 Offsite Work and Independent Audit Requirements

If the Offeror elects to have any staff perform work offsite, the following requirements shall apply:

A. Independent Audit Engagement: The Offeror shall engage, at its own expense, an independent Certified Public Accounting (CPA) firm to perform an attestation of the Offeror's internal controls in accordance with the American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements (SSAE) No. 18.

B. SOC 2 Type II Report – Initial Submission: The Offeror shall provide the Agency with a copy of its most recent Service Organization Control (SOC) Type II report, including the controls and tests of operating effectiveness:

C. Within thirty (30) calendar days of contract effectiveness, or

D. If the Offeror is a new service organization, within thirty (30) calendar days following completion of the initial audit period.

E. Annual Audit Requirement: The Offeror shall undergo a SOC 2 Type II audit annually for the duration of the contract.

F. Ongoing Reporting: The Offeror shall submit a copy of each annual SOC 2 Type II audit report to the Agency upon completion.

G. Subcontractor and Subservice Organization Compliance: These requirements shall apply equally to any subcontractor or subservice organization that performs activities within the Offeror's service organization controls. Offeror shall provide the Agency with corresponding SOC 2 Type II audit reports for such entities.

H. IT system development must adhere to the security concept of separation of duties by assigning roles that prevent a conflict of interest:

1. The system shall provide appropriate and secure role-based access capabilities for users, including, but not limited to, a fiscal staff role, providers, and Offeror staff, security staff, Agency

staff, and external users as designated by the Agency.

2. Offeror shall:

   i. Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.

   ii. Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

   iii. Provide access to any books, documents, papers, and records pertinent to this contract.

   iv. Offeror shall, immediately upon receiving written instruction from the Agency, provide any independent auditor, accountant, or accounting firm with all books, documents, papers, and records of Offeror that are pertinent to this Contract.

   v. Offeror shall cooperate fully with any such independent auditor, accountant, or accounting firm during the entire course of any audit authorized by the Agency.

   vi. Offeror shall maintain all records and documents relevant to the Contract for five (5) years from the date of final payment to Offeror. If an audit, litigation, or other action involving records is initiated before the five-year (5-year) period has expired, then Offeror shall maintain records until all issues arising from such actions are resolved or until an additional five-year (5-year) period has passed, or whichever is later.

3.2.19 Offline Capabilities for Field Users

The system shall allow users to enter data while disconnected from the network or internet, with appropriate validations applied at the time of entry. When a secure network connection is re-established, the system shall automatically synchronize and upload the entered data, applying required edits and audit controls without user intervention. The system shall make key application features and data available while offline, including common forms and templates needed by licensors to complete and save work. Upon successful synchronization, any temporary or locally stored data shall be securely removed.

3.2.20 Document Management

The Offeror shall ensure the system allows users to:

A. Upload capabilities for documents, files, videos, and photographs.
B. Accept all common file types, including but not limited to, .JPEG, .PDF, .TIF.
C. Store all electronic documents.
D. Preview and print files in all file types.
E. Integrate with MS Office Suite or other similar application suite.

3.2.21 Interfaces and Data Exchanges

Offeror shall configure the platform to integrate with and facilitate bi-directional exchanges currently in place and planned. Integration and facilitation shall include consideration for data use in functional components to enhance child outcomes and improve user productivity. Specific interfaces and/or integrations shall be identified under each module.

3.3 Hosting

Provide a description and approach for hosting requirements. The proposer should provide the multiple layers of external and internal security that provide the administrative, physical, and technical means to protect the sensitive or confidential information that performs the responsibilities and duties set forth in this RFP. In addition, the Offeror shall include, but not be limited to, the following requirements:

3.3.1 Physical Location: Primary and Failover Facility or Facilities

Offeror shall implement physical security controls to protect facilities, equipment, and information assets used in support of the services provided under this RFP. Such controls shall include, at a minimum:

A. Controlled access to facilities housing systems, equipment, or data, limited to authorized personnel only.
B. Physical safeguards to prevent unauthorized access, damage, or interference with facilities and equipment.
C. Visitor access controls, including sign-in procedures and escort requirements where appropriate.
D. Environmental protections (e.g., fire suppression, climate control, and power backup) to ensure system availability and integrity.
E. Secure allocation and storage of equipment and media to prevent loss, theft, or unauthorized use.

3.3.2 Staffing Security

Offeror shall maintain policies and procedures for security clearance and staffing controls, allowing Offeror personnel to have access to Agency-owned confidential information and/or to restricted areas within the Offeror's host environment.

3.3.3 Security and Environmental Controls

3.3.3.1 Physical and Environmental Safeguards

A. The proposer shall maintain proper power and cooling, including redundant power and cooling, to safeguard all hardware, software, and State-owned data. The secure perimeter of defense includes, but is not limited to, the use of technical barriers, physical barriers, and administrative safeguards.

B. The server(s) shall be protected from intrusion through the use of physical barriers, technical barriers, and administrative barriers.

3.3.3.2 System Architecture and Infrastructure

A. Offeror shall provide a description and/or network diagram of the hardware infrastructure, database structure, and operating system (OS).

B. Offeror shall provide sufficient data storage to operate and support the proposed solution.

3.3.3.3 Network and Application Security

A. The network shall be secured through the use of multiple redundant firewalls, anti-virus software, and data encryption for files transferred to and from external users. Data encryption shall meet Federal Information Processing Standard (FIPS) 140-3.

B. Access to the proposer system shall be granted through the use of a unique user identifier and user profile, combined with a strong password. Any transaction or change to data shall be traced and audited down to the user-ID level.

3.3.3.4 Security Policies, Awareness, and Monitoring

A. Security policies and procedures shall be maintained for each location or account.

B. Offeror shall routinely review logs of system activity for suspicious activity.

C. If applicable, the proposer shall provide HIPAA privacy and security training to all new hires and subcontractors.

3.3.3.5 Availability, Performance, and Resilience

A. The proposer shall maintain adequate technical staffing to provide 24x7x365 hosting services.

B. The system shall be available 24x7x365. Any maintenance outages shall be coordinated in advance with Agency-designated personnel.

C. Offeror shall provide sufficient bandwidth and redundancy to support access to the proposed solution functionality and mitigate internet congestion.

D. Offeror shall provide examples of policies, procedures, and safeguards employed to respond to and/or recover from denial-of-service (DoS) attacks. Proposals should also include the Recovery Time Objective (RTO) metric.

3.3.3.6 Disaster Recovery and Restoration

A. Offeror shall maintain a disaster recovery facility and documented policies and procedures to implement recovery activities.

B. In the event of a complete failure, the proposed solution shall be available within twenty-four (24) hours.

C. Annual disaster recovery testing shall be conducted to ensure a smooth transition should the plan be activated. The Offeror shall provide a copy of the annual test results to the Agency within thirty (30) days of the disaster recovery demonstration.

D. Offeror shall describe the prioritized order of restoration for the proposed solution's hosted services.

3.3.3.7 Data Security and Incident Response

A. Offeror shall maintain policies and procedures to protect the security of confidential information.

B. Offeror shall provide a description of policies, procedures, and protocols to be followed in the event of a data security breach.

C. Data breach notification procedures shall comply with applicable State statutes.

D. If the Offeror's solution is selected, the Offeror shall acknowledge that State law shall have jurisdiction with respect to data security breach notification.

3.3.3.8 Compliance, Audits, and Reporting

A. Offeror shall demonstrate compliance with the Agency's archiving requirements and, where applicable, with industry standards and best practices.

B. Offeror shall provide a description of website archiving practices and how those practices meet the requirements of the State's Public Records Act **[insert statute number]**.

C. Offeror shall discuss any certifications or audits achieved that are applicable to the requirements of this RFP (e.g., SAS 70 Audit, HIPAA, SOX, GLB) and shall provide copies of such certifications or audits, including the dates conducted.

D. Offeror shall provide hosting reports that include, but are not limited to, uptime, utilization, traffic patterns, and hosting certifications.

3.4 Risk Management

A. Offeror shall describe how they will conduct risk management planning, identification, analysis, responses, and monitoring and how they will control the risks throughout the project's life cycle. Offeror shall identify how the Offeror's Risk Management Plan will increase positive impacts and decrease adverse events in the project.
B. For work performed in each location, Offeror shall describe the plans/arrangements in place for an alternative work site should the facilities become inoperative because of a fire, earthquake, flood, or another catastrophic event.
C. Offeror shall describe the emergency and disaster recovery plans.

3.5 Reporting

3.5.1 Weekly Status Reports

Distribute weekly status reports with the agenda to Agency participants. The Agency reserves the right to review and approve each weekly status report and request information be added to the report template at any point in the project. Weekly status reports shall contain, at a minimum, the following information:

A. Key accomplishments
B. Key issues and their status
C. Deliverable and milestone reporting/Burndown Chart
D. Anticipated tasks to be completed in the next week
E. Issues to be addressed before proceeding with the next tasks
F. Risk and mitigation planning

3.5.2 Monthly Status Reports

A. Offeror shall provide the Agency with a monthly status report for high-level project status reporting within the Agency-defined timeframe. Monthly status reports shall contain, at a minimum, the following:

    1. Description of the overall completion status of the project in terms of the approved Project Plan Baseline
    2. Estimated efforts/Burndown Chart (hours by activity, for each activity, and timeframe for

completion)
3. Plans for activities scheduled for the next month
4. Proposed changes to the Project Plan Baseline, if any
5. Status of progress against the Project Baseline
6. Deliverable status, with percentages of completion
7. Updated issues log, including issues encountered, proposed resolutions, and actual resolutions
8. Progress against planned Quality Assurance/Quality Monitoring (QA/QM) metrics
9. Analysis of risks anticipated, proposed mitigation strategies, and resolved risks
10. Updates required in the change management strategy
11. List of change requests, if applicable
12. Identification of Offeror employees assigned to specific tasks and any anticipated staffing changes

B. The Agency may request a meeting with the Offeror Project Manager and key staff to discuss the monthly status reports. The Agency reserves the right to review and approve each monthly status report and request that additional information be added to the report template at any point in the project.

3.6 Training and Knowledge Transfer Plan

3.6.1 Training Program Overview and Scope

A. The Offeror shall provide a comprehensive, high-quality training program for all internal and external users to support a smooth transition from individual programs to the integrated system. Training shall be delivered either onsite or virtually and shall continue throughout implementation and the Maintenance and Operations (M&O) period, as needed.

B. The training program shall support statewide implementations and be delivered in collaboration with the Agency and the Project Team.

3.6.2 Training Governance, Staffing, and Roles

A. Offeror shall provide sufficient qualified staff to successfully execute all training requirements.

B. Offeror's training team shall demonstrate proven experience in:

1. Developing and delivering comprehensive training programs supporting organizational transformation.
2. Training end users during new system implementations, including the use of Train-the-Trainer and end-user approaches.
3. Maintaining professionalism and effectively engaging with Agency staff, stakeholders, and Project Team members.

C. The Offeror shall designate a Training Lead responsible for leading the development and execution of the Training Plan and serving in a peer management role with the Agency Training Unit Manager.

D. The Agency Training Lead shall provide oversight of the Offeror-led training effort and supervise Agency training staff. The Agency Training Lead shall be responsible for reviewing and approving Offeror training content and Agency stakeholder communications and engagement activities.

3.6.3 Training Planning and Management

A. Offeror shall develop, maintain, and execute a detailed Training Plan, subject to Agency approval. The Training Plan shall include, at a minimum:

1. Training scope and objectives
2. Schedule and milestones
3. Roles and responsibilities
4. Training environments
5. Delivery methods and training types
6. Curriculum and materials
7. Evaluation and metrics
8. Knowledge transfer approach
9. Approval and acceptance criteria
10. Training Delivery and Methods

B. The Offeror shall develop and deliver training using appropriate delivery methods, including live instructor-led sessions, virtual training, recorded sessions, webinars, and computer-based training.

C. The Offeror shall provide training to all internal Agency users and external users of the system, including clients and providers (e.g., parents, child care providers, and staff). Training for external users shall be delivered via webinars or computer-based formats.

D. The Offeror shall deliver a system overview training module that provides a high-level introduction to system functionality and context for subsequent training. This module shall be recorded and designed for use as both a prerequisite and a stand-alone course for non-system users.

3.6.4 Train-the-Trainer, Super User, and Knowledge Transfer

A. The Offeror shall design and deliver comprehensive Train-the-Trainer and Super User courses in accordance with the approved Training Plan. These courses shall prepare designated Agency staff to independently conduct end-user training following implementation. Train-the-Trainer and Super User curricula shall:

1. Instill Super User–level knowledge of the system
2. Ensure consistency in training delivery
3. Incorporate hands-on exercises using training and sandbox environments
4. Provide instructional guidance and delivery tips
5. Include practice delivery sessions

B. The Offeror shall engage Agency staff early in the project to support hands-on learning and knowledge transfer and shall collaborate with the Agency and organizational design vendor at key integration points.

3.6.5 Training Materials and Deliverables

A. The Offeror shall be responsible for the development of all training curricula and materials and shall incorporate feedback from the Agency and any organizational design vendor.

B. All training materials shall be delivered to the Agency in editable formats. At a minimum, deliverables shall include:

1. Course curricula and presentation materials
2. Job aids, quick reference guides, and exercises
3. Train-the-Trainer and Super User materials
4. End-user reference materials
5. Recorded training sessions
6. A comprehensive User Manual

3.6.6 Training Environments

A. The Offeror shall develop and maintain separate technical environments dedicated to training and sandbox use. Training environments shall:

    1. Be accessible to both Offeror and Agency staff
    2. Support classroom, virtual, and hands-on training
    3. Allow trainees to explore system functionality
    4. Support concurrent execution of multiple training sessions

B. One training environment shall primarily support Offeror-led training delivery, while a separate environment shall support Agency preparation and maintenance of training materials.

3.6.7 Ongoing Training and M&O Readiness

The Offeror shall provide ongoing training to Agency staff throughout all phases of implementation to ensure readiness for long-term system maintenance and operations. Training shall address, at a minimum:

A. System administration and configuration
B. Database, software, and hardware maintenance
C. Application development and batch processing
D. Architecture and security maintenance
E. Testing and quality assurance
F. User support tools and help desk operations
G. Rules engines and BPM tools

3.6.8 Knowledge Transfer Plan and Transition

A. The Offeror shall develop and maintain a Knowledge Transfer Plan for Agency staff assuming responsibility for ongoing maintenance. The plan shall include:

    1. Objectives and scope
    2. Relationship to other project plans
    3. Schedule and milestones
    4. Knowledge transfer methods
    5. Resources and risks
    6. Curriculum and materials
    7. Metrics and evaluation criteria
    8. Third-party vendor involvement
    9. Locations of all SOPs, manuals, and checklists

B. The Knowledge Transfer Plan shall be updated throughout the project.

C. During the final four (4) weeks of the M&O phase, the Offeror shall support a structured shadowing period during which Agency staff lead operational tasks with Offeror support.

D. At project closeout, all training materials, documentation, and system knowledge shall be fully transitioned to the Agency.

3.7 Operational Readiness and Operability Testing

A. The Offeror shall conduct a formal operational readiness walkthrough with the Agency to demonstrate the Offeror is ready to begin operations.
B. The Offeror shall conduct the operational readiness walkthrough with the Agency as defined by the approved Project Work Plan for implementation and meet any other related performance requirement included in this RFP.
C. The Offeror shall demonstrate its ability to operate the software and testing environments by completing an Operational Readiness Checklist that includes, at a minimum, the following:
    1. Hardware and software installation and operations
        a. Configuration Management Plan
        b. Punch List(s)
    2. Telecommunications
    3. Interfaces
        a. Setup
        b. Maintenance
    4. Training
        a. Agency staff training
        b. Technical training
        c. External-user training
    5. Application and Toolset Documentation
        a. System
        b. User
        c. Operations
    6. System Security
        a. Confidentiality of data
        b. System access
        c. Vulnerability testing to ensure security of the system. A third party may be contracted.
    7. Report generation and distribution process
    8. Coordination of responsibilities with other component users
    9. Pilot

3.8 Quality Assurance and Quality Control

The Offeror will need to meet the following quality assurance and quality control measures to ensure the quality of the product solutions and services. The quality assurance and control measurements include, but are not limited to, the following:

A. The Offeror shall implement comprehensive quality management practices that will be used throughout all phases of the Contract and include standards on timeliness, accuracy, and completeness for performance of, or reporting on, operational functions.

B. Offeror shall develop and provide a Quality Assurance/Quality Monitoring (QA/QM) Plan that reflects the Offeror's experience and approach to providing high quality services and how the Offeror will measure, report on, and ensure performance expectations are met. At a minimum the QA/QM plan shall address the following key components:

   1. An overview of quality assurance activities and tasks to be performed
   2. Processes and procedures for conducting QA/QM activities, including:
      a. Procedures for documenting, resolving, and reporting issues and risks identified during QA/QM activities, including issues identified by the Agency.
      b. Performance-monitoring reviews, measures, and reports that provide cross-project status information to support project management review and decision-making.
      c. Defined roles and responsibilities of Offeror, subcontractors, and the Agency for performing QA/QM activities and resolving identified issues, including identification of Offeror team members and their respective responsibilities.

C. Monitor the quality and accuracy of all Offeror work and deliverables.

3.8.1 Quality and Control Measurements

Offeror's quality assurance and control measurements shall include but are not limited to:

A. Test plans

B. Test Region (mirroring the production environment)

C. Test cases and scripts, detailed with measurable outcomes

D. Traceability Matrix – The mechanism for tracing requirements and specifications throughout the entire project (i.e., hardware and software)

E. Test results/walkthroughs

F. Performance requirements – The establishment and monitoring of the defined performance requirements for any technology solutions offered.

3.8.2 Documentation

Offeror shall document the methods that will be employed to control variance from the quality measurements and will provide them within the Quality Assurance Plan.

3.9 Change Control Management

A. Offeror shall maintain a control change process with all changes approved through the Agency. The control change process should include the reason for the change, complete description of the work to be performed, estimate of time and cost to complete the task, completion date for the change, and an impact analysis that indicates ramifications or impact to the project.

B. If unforeseen circumstances arise where a dispute resolution may be needed, then the Offeror shall

submit, in writing, a description of the problem and Offeror's resolution to the project manager and Agency primary point of contact. If change requests are needed, then the Offeror shall agree to continue at the hourly rate specified in the proposal.

C. In the event a change to the Statement of Work is required, a contract amendment shall be made to the contract in accordance with the Contract.

3.10 Auditing

A. Offeror, who accesses and/or maintains Agency data, must meet all federal, State, and Agency audit and compliance standards.

B. No additional funding will be allocated to the Offeror for the audits required under this RFP. Offeror is responsible for the cost of all audits and should ensure those costs are included in the price of the Contract. Detailed requirements are described below.

3.10.1 General Audits

A. Offeror must respond to requests for information or access in the Agency-specified timeframe.

B. Audits may be performed by a number of State and federal agencies or authorized agents. The Offeror must fully cooperate with the audit process. An audit may include, but is not limited to, the following capabilities and applies to the applications and architecture:

1. Storing, retrieving, and executing programs, whether such programs are part of the Offeror's production Application, or generated by Offeror staff.
2. Sampling and reconciling Application files to ensure accurate and timely maintenance.
3. Demonstrating services and/or benefits were provided for eligible clients.
4. Reviewing the Offeror's organization, policies, procedures, practices, and effectiveness of control, operating efficiency, facility and software security, and backup procedures.
5. Reviewing the Offeror's compliance with Contract terms, Application specifications, State or federal regulations, administrative directives, and program documentation.
6. Reviewing any phase or aspect of the project for any purpose related to the Application.
7. Responding to requests for data or information.
8. Having access to files, documentation, and Offeror personnel, or any site in which the Offeror performs any work related to this Contract or maintains any records related to this Contract.

C. Assisting Agency staff in responding to federal inquiries. This level of support must also be provided to all other Agency audit agencies or their designees.

3.10.2 Performance Auditing

A. Offeror shall agree that authorized federal and State representatives – including, but not limited to, State personnel, other State entities with statutory authority, independent auditors acting on behalf of the State, and federal agencies providing funding – shall have access to, and the right to examine, the

items listed above during the term of the Contract and for a period of six (6) years following Contract termination or until all audit findings are fully resolved, whichever occurs later. During the Contract term, the Offeror shall provide such access within the State. During the six (6)-year post-Contract period, delivery of and access to the listed items shall be provided at no cost to the Agency. All audit outputs deemed retainable shall comply with record retention policies and procedures.

B. The Agency reserves the right to independently audit monthly performance reports and metrics, as deemed necessary, to ensure material compliance with all Contract provisions. Completed assessments may be kept on record at the State and may serve as past performance data. Past performance data will be available to assist State agencies in the selection of IT service providers for future projects and procurement efforts. All audit outputs deemed retainable by the Agency must follow record retention policies and procedures .

3.10.3 Financial Compliance

A. Offeror shall maintain accounting records that relate directly to the performance of this Contract. Such records shall be maintained in accordance with Generally Accepted Accounting Principles (GAAP) and shall be kept separate and apart from Offeror's other corporate accounting records.
B. Offeror shall maintain books, records, documents, and other supporting evidence pertaining to the administrative costs and expenses of this Contract in sufficient detail to accurately reflect all revenues, net costs, direct and allocated costs, and any other costs or expenses for which reimbursement is claimed under the Contract.
C. Offeror shall agree that authorized federal and State representatives – including, but not limited to, Agency personnel, the Auditor General, the Comptroller General of the United States, and other State or federal agencies providing funding – shall have access to, and the right to examine, the records listed above during the Contract term and for a period of three (3) years following Contract termination or until final resolution of all pending audit questions and litigation, whichever occurs later.
D. During the Contract term, access to these records shall be provided at the Offeror's office in Wyoming during reasonable business hours. During the three (3)-year post-Contract period, delivery of and access to the records shall be provided to the Agency at no cost.

3.10.4 Security Auditing

Offeror shall, at its own expense, procure an independent vulnerability assessment, penetration test, and security audit of the system to meet State and federal requirements. If Offeror proposes to conduct any audit activities using internal resources, Offeror's Quality Assurance/Quality Monitoring (QA/QM) Plan shall clearly document the internal organizational structure and controls that ensure audit independence.

3.10.5 Access to Records

The Agency and any of its representatives must have access to any books, documents, papers, and records of the Offeror that are pertinent to the Contract. Upon receiving written instruction from the Agency, the Offeror must immediately provide any independent auditor, accountant, or accounting firm with all books, documents, papers and records of the Offeror that are pertinent to this Contract. The Offeror must cooperate fully with any such independent auditor, accountant, or accounting firm during the entire course of any audit authorized by the Agency.

3.11 Ownership and IP

A. The State retains exclusive ownership rights, title, and interest in all data (including any data uploaded, created, or processed by the SaaS application) reports, and custom-configured work generated,

ensuring data portability upon contract termination.

B. The State agrees that all material appropriately marked or identified in writing as proprietary and furnished hereunder by the Offeror are provided for the State's exclusive use for the purposes of this Contract only. All such proprietary data shall remain the property of the Offeror. The State agrees to take all reasonable steps to ensure that such proprietary data are not disclosed to others, without prior written consent of the Offeror, subject to the (applicable) Public Records Act or other lawful process.

3.11.1 Location of Data

Regardless of any other provision of this Contract or its incorporated or referenced documents, all of the data identified by the State as requiring their data to remain in the continental United States shall remain and be stored, processed, accessed, viewed, transmitted, and received, always and exclusively within the contiguous United States.

3.11.2 Ownership of SaaS Product

A. Offeror retains ownership of its pre-existing, proprietary software and/or platform, and any improvements made to it as set out in Offeror's Licensing Agreement. All inventions, discoveries, intellectual property, technical communications and records originated or prepared by the Offeror pursuant to this Contract including any upgrades or enhancements to software programs, hardware, or other equipment, whether electronic or physical, paper, reports, charts, customized software, and other documentation or improvements thereto, and including the Offeror's administrative communications and records relating to this Contract, shall be the Offeror's exclusive property.

B. The State retains ownership of any configurations or customizations, exclusive of the deliverables contemplated by this Contract, developed solely for the state and its exclusive use. Such configurations and customizations must be specifically identified as such at the time the State orders them, and all such configurations and customizations to be owned by the State shall be paid for exclusively by the State.

3.12 Deliverables and Milestones

All deliverables require written approval for acceptance by the Agency.

Table XX: Deliverables by Phase

Table XX: Deliverables by Phase

Deliverable	Phase
Kick-off Agenda, Material, and Meeting Minutes	Start Up
Project Work Plan	
Project Management Plan, including a Staffing Plan	
Communication Plan	
Quality Assurance Plan	
Configuration Management Plan (documentation- version control and software-version control)	

Requirements Specification Document Detailed system design specification to include all components of the system	
Business Process Redesign Activities	
Implementation Plan Strategy description and estimated costs for application maintenance with a maximum escalation percentage for maintenance based on the total cost of the software.	
Operational Readiness Checklist, including Hardware and Software Installation Punch List	
Risk Management Plan	
Change Control Management Plan	
Software Utilization Documentation	
Application navigation, data dictionary, and installation guide	Implementation
Data Migration Plan, including: • Data Conversion and Migration Plan • Data dictionary, data models, and data flow models • Draft Conversion and Migration Results reports • Final Conversion and Migration Results reports	
System Security Plan	
System Test Plan, including test scripts	
System Test Results	
User Acceptance Test Plan System Walkthroughs	
Training Plan	
User Guides (online) User Training Documentation	
Project Reports and Recommendations	Ongoing

3.13 Resource Management and Staffing Plan

The proposal shall include a Staffing Plan that demonstrates how the Offeror will provide adequate, experienced, and qualified personnel to meet the requirements of this RFP throughout the Contract Term. At a minimum, the Staffing Plan shall address the following:

A. Staffing Plan Overview and Composition
   1. Identify key management positions and all other personnel proposed to fulfill the Contract.
   2. Include resumes for all staff who will manage or directly provide services under the Contract. Resumes shall be provided in Appendix XX.
   3. Provide position descriptions, including required qualifications and experience, for any positions not filled at the time of proposal submission.
   4. Identify all staff disciplines, including job titles and primary responsibilities.
   5. Identify any subcontractor staff proposed to support the Contract, if applicable.

B. Staffing Levels, Allocation, and Labor Effort
   1. Estimated staffing levels by role and discipline for each project phase, including monthly staffing estimates for the duration of the project.

2. An explanation of how staffing levels will accommodate fluctuations in workload.
3. Identification of total labor hours by project phase and for the entire project, including a breakdown of Offeror staff hours and Agency staff hours.

C. Roles, Responsibilities, and Organizational Structure
   1. A summary of all roles and responsibilities utilized throughout the Contract.
   2. An organizational chart depicting the project team structure, reporting relationships, and lines of authority.
   3. A commitment to maintain and update the organizational chart throughout the Contract term.

D. Key Personnel Commitments and Controls
   1. Key personnel shall not be removed, reassigned, or replaced without prior written approval from the Agency.
   2. Substitute or additional personnel shall not be assigned until resumes are submitted to and approved by the Agency.
   3. The Offeror shall notify the Agency at least thirty (30) calendar days in advance of any planned reassignment or change involving key personnel.

E. Staff Removal, Replacement, and Vacancies
   1. The Agency reserves the right to request removal of any proposed staff member, and the Offeror shall comply with such requests immediately.
   2. A description of the process for replacing key personnel within Agency-defined timeframes, including procedures for backfilling positions during transitions.
   3. Any replacement staff member shall meet or exceed the qualifications, skills, and experience of the individual being replaced.
   4. All replacement personnel are subject to Agency approval at the time of assignment and again ninety (90) days after assignment.
   5. Immediate notification to the Agency of any resignation or termination of key personnel, including the reason for the vacancy and an action plan for backfilling the position.
   6. A key personnel position shall not remain vacant for more than thirty (30) consecutive days.
   7. Vacant key personnel roles shall not be filled by reassignment of other key personnel without prior Agency approval.

F. Governance, Security, and Knowledge Transfer
   1. Identification of Offeror's Security and/or Compliance Officer, including contact information.
   2. A description of how knowledge transfer will be ensured for new or replacement staff to maintain continuity of services and minimize disruption.