**State of Indiana**

**RFP 26-85723**

**Inters- AE, CTE & ETP**

**Attachment — Scope of Work**

## **Introduction**

The Indiana Department of Workforce Development (DWD) and the Indiana Commission for Higher Education (CHE) request responses from qualified vendors for the implementation of modernized technology solutions for the Indiana Technical Education Reporting System (Inters). Inters is the State’s centralized platform for managing data related to Adult Education (AE), Career and Technical Education (CTE), and Eligible Training Provider (ETP) programs. This system is critical for ensuring compliance with federal and state reporting requirements, supporting program accountability, and enabling data-driven decision-making across Indiana’s workforce and education ecosystem.

The State seeks a solution that is secure, scalable, and user-friendly, capable of integrating with existing systems and adapting to evolving federal and state requirements. The selected vendor will partner with DWD and CHE to design, implement, and maintain a system that improves operational efficiency, enhances user experience, and supports Indiana’s long-term vision for workforce development.

Vendors may submit proposals for one or more solutions. Each system has unique business and technical requirements, but all must support data integration, compliance reporting, and user-centered design.

DWD and CHE welcome a broad range of technology solutions, including both configurable off-the-shelf platforms and customizable systems tailored to meet specific operational needs. Proposals should clearly outline the flexibility, scalability, and adaptability of the proposed solution to ensure alignment with current and future business requirements.

## **Overview**

Indiana’s workforce and education programs rely on accurate, timely, and comprehensive data to meet compliance obligations and inform policy decisions. Inters serves as the backbone for these efforts, supporting three distinct but complementary systems:

* **Adult Education (AE) Student Management System**
* **Career and Technical Education (CTE) Data Collection System**
* **Eligible Training Provider (ETP) & OCTS Management System**
  1. **Current State**

The current system is a custom legacy application, purpose-built in the early 2000s for CTE. Functionality for AE and ETP was added over the years. Capabilities expanded with changing business needs. It is ripe for innovation. Both agencies, DWD and CHE, use InTERs system across the three teams. See: [DWD](https://www.in.gov/dwd/career-training-adult-ed/adult-ed/amplifyae/accountability-inters/) (<https://www.in.gov/dwd/career-training-adult-ed/adult-ed/amplifyae/accountability-inters/>) and [CHE](https://www.in.gov/che/cte/intersperformance-and-accountability/) (<https://www.in.gov/che/cte/intersperformance-and-accountability/>).

## **Definitions**

**Adult Education (AE)** – State-administered programs that provide foundational skills, high school equivalency preparation, and workforce readiness for adult learners, in compliance with the Workforce Innovation and Opportunity Act (WIOA - Title II) and OCTAE guidelines.

**Career and Technical Education (CTE)** – Programs designed to prepare secondary and postsecondary students for careers through technical skills training, industry-recognized certifications, and academic integration, aligned with Perkins V requirements.

**Eligible Training Provider (ETP)** – An organization approved under WIOA Title I to deliver occupational training programs that meet state and federal eligibility criteria for inclusion on the Eligible Training Provider List (ETPL).

**Indiana Technical Education Reporting System (InTERS)** – The State’s centralized platform for collecting, managing, and reporting data for AE, CTE, and ETP programs, supporting compliance, accountability, and performance analysis.

**InTraining** – Indiana’s Eligible Training Provider List (ETPL) management system used by DWD to manage provider applications, program eligibility, and compliance with WIOA Title I requirements. It supports provider lifecycle management, performance reporting, and integration with workforce systems.

**National Reporting System (NRS)** – The federally mandated accountability system for reporting outcomes of Adult Education programs under Title II of WIOA.

**OCTAE** – The U.S. Department of Education’s Office of Career, Technical, and Adult Education, which establishes federal guidelines for Adult Education programs.

**WIOA** – Workforce Innovation and Opportunity Act, federal legislation governing workforce development programs, including Adult Education and Eligible Training Provider requirements.

**Perkins V** – The Strengthening Career and Technical Education for the 21st Century Act, which sets requirements for CTE programs and federal reporting.

## **Adult Education (AE) Student Management System**

**4.1 Purpose:**  
The Adult Education Student Management System serves as the centralized platform for the collection, management, and reporting of student data for Indiana’s Adult Education programs. The system must ensure full compliance with OCTAE and WIOA data and reporting requirements established by the U.S. Department of Education, the U.S. Department of Labor, and Indiana state legislation and policy.

This system is critical for supporting program accountability, funding, and continuous improvement efforts. It must enable the secure and accurate tracking of student progress, outcomes, and demographics, while also providing the flexibility to adapt to evolving federal and state reporting standards. The platform should support multiple user roles through tailored interfaces, offer real-time data validation and error-checking, and allow for customizable reporting to meet diverse stakeholder needs.

**4.2 Key Requirements:**

* Relational database with error-checking and edit reporting
* Interfaces for multiple user types (e.g., educators, administrators)
* Include functionality for public-facing digital registration, supporting unauthenticated users with appropriate security and workflow protocols.
* Customizable reporting aligned with U.S. Department of Education and Labor guidelines for Adult Education
* System must align and comply with National Reporting System (NRS) requirements and incorporate guidance from the April 2025 Technical Assistance Guide for Performance Accountability under WIOA.
* Outcome tracking by demographics and instructional variables
* Ability to integrate with other workforce systems as needed
* Ongoing support, training, and responsiveness to policy changes
* Support multiple data entry formats accounting for demographic, contact, assessment and attendance variables.
* Ability to add, edit, view, and delete data from an administrative view with different access levels with permissions customized per user type
* Data structure organized by groups and sub-groups within the system
* Error checking and data validation must be coded into the system to ensure data is consistent with federal and state requirements with daily system updates to ensure data accuracy and integrity. Required compliance with OCTAE 2025 Program Memoranda 19-1 and 17-6.
* File import/export capability across multiple file formats with the ability to store by user, API capability for import function
* Include functionality for public-facing data input supporting unauthenticated users with appropriate security and workflow protocol.
* System must provide a sand box environment for functionality testing prior to initial implementation and all subsequent updates and changes
* Vendor must be able to develop custom forms for specialized data collection requests.
* Vendor must be able to procure domains or URLs to facilitate student data collection through communication or public domain portals

## **Eligible Training Provider (ETP) & OCTS Management System**

**5.1 Purpose:**  
The Eligible Training Provider (ETP) Management System will serve as a centralized platform for the oversight and administration of occupational training providers and programs in Indiana. This system is essential for ensuring transparency, regulatory compliance, and performance accountability in alignment with federal and state workforce development policies.

The platform must support the full lifecycle of provider engagement—from application and eligibility determination to ongoing monitoring and reporting. It should offer role-based access for various user types, including training providers, reviewers, and state administrators, and enable public access to approved provider and program information.

The system should streamline data collection, reduce administrative burden, and enhance the ability of DWD and its partners to make data-informed decisions about training investments and workforce outcomes. The system must comply with WIOA Title I (20 CFR 680.400–680.530), support performance tracking, and integrate with workforce systems for outcome analysis.

* 1. **Key Requirements:**
* Support multiple data entry formats including provider demographics, program details, costs, performance outcomes, and accreditation status.
* Data structure organized by provider, program, and sub-program categories within the system.
* State administration must have full access to all data structures, tables, and code for monitoring and compliance
* Needs to be able to meet and support WIOA ETP requirements established under the WIOA Title I per 20 CFR 680.400 – 680.530
* Ability to add, edit, view, and delete provider and program data with role-based access permissions customized per user type (state staff, providers, auditors)
* Public-facing data input for providers applying to ETPL or OCTS approval, with secure workflows and authentication protocols.
* Vendor must procure domains/URLs to facilitate provider and program data collection through public portals
* Internal process for approving providers for DWD state team
* Error checking and validation coded to ensure compliance with WIOA, Perkins V, and Indiana state requirements. Daily updates are required to maintain accuracy and integrity.
* Vendor must support custom forms for specialized provider or program data collection requests. This would include a unified training provider application.
* Relational data structure for cross-referencing and reporting
* File import/export capability across multiple formats with API support for provider uploads and state integration.
* Integration with workforce systems to assess outcomes and ROI
* Support for federal and state reporting requirements
* Role-based access for multiple user types

## **Career and Technical Education (CTE) – Student Data Collection System**

**6. 1 Purpose:**  
The Career and Technical Education (CTE) Longitudinal Data System serves as Indiana’s centralized platform for the collection, management, and reporting of student and program data related to CTE. This system is essential for ensuring compliance with federal Perkins V requirements, supporting state and local accountability, and enabling data-informed decision-making across Indiana’s secondary and postsecondary CTE landscape.

The system must support the seamless integration of data from multiple sources, including real-time connections and file imports, to create a comprehensive view of student progress from enrollment through graduation, post-secondary education, and into the workforce. It must accommodate a wide range of users, including school personnel, administrators, grant managers, and state staff—through secure, role-based access and intuitive interfaces.

**6.2 Key Requirements include but are not limited to:**

* Student and course management (enrollment, outcomes, certifications)
* Teacher and school personnel management
* Grant management (Perkins, Reserve, PEAR forms)
* Compliance tracking (CLNA, documentation uploads)
* Federal and state reporting (performance indicators, disaggregated data)
* Integration with DOE and other state systems
* Opportunities for innovation (AI, mobile access, visual analytics)
* Enhanced user experience and streamlined workflows
* The ability to import and manually enter all required CTE enrollment data, student completion data, follow-up data, and certifications attained for funding and state reporting purposes.
* Importing official CTE enrollment figures for funding calculations and inputting essential student follow-up, completion, and certification attainment data.
* Entering CTE Area District adoption forms/programs of study, licensure information, and course waivers.
* Automated checks to prevent duplicate student records, record errors, and session errors upon entry or import. The system must prompt users to fix/resolve these errors.
* Ensuring data accuracy, resolving errors, and eliminating duplicate student or session records

## **Desired Contractor Qualifications**

* 1. **Desired Qualifications**

To be eligible for consideration by the State, a Respondent must meet the following desired requirements:

* **Experience with Adult Education Reporting**  
  Demonstrated experience designing, implementing, and managing systems that comply with **National Reporting System (NRS)** requirements and **Title II of WIOA** for Adult Education programs.
* **Integration Capability**  
  Proven ability to integrate with existing Indiana workforce systems, including **InTraining** (ETPL management system), and other state platforms as required.
* **Compliance Expertise**  
  Demonstrated understanding of federal and state compliance requirements, including **OCTAE guidelines, WIOA Title I and II**, and Indiana-specific reporting standards.
* **Security and Accessibility**  
  Ability to meet Indiana’s cybersecurity standards (GovRAMP, NIST 800-53) and accessibility requirements (WCAG 2.1).
* **Experience with Multi-System Solutions**  
  Prior experience implementing integrated solutions that support multiple program areas (AE, CTE, ETP) within a single platform or through interoperable modules.
* **User-Centered Design**  
  Demonstrated ability to deliver intuitive, role-based interfaces and mobile-responsive solutions for diverse user groups, including educators, administrators, and providers.
* **Innovation and Analytics**  
  Experience incorporating advanced features such as real-time dashboards, predictive analytics, and AI-driven data validation.

## **General Expectations for all Solutions**

**Solution Configurability and Customization Preference**

The State prefers a solution that meets requirements in the following priority order: out of the box functionality; configuration; or customization only as a last resort. The State expects the selected vendor to act as a partner to help identify potential business process changes that leverage out of the box or configuration options and reduce or eliminate the need for custom code. To help facility this, the selected vendor must document the out of the box and configuration options evaluated before proposing any customization and must demonstrate why configuration cannot satisfy the requirement.

Customizations should be considered only when one or more of these criteria apply: the requirement is necessary to meet a federal reporting requirement or regulation; the requirement is necessary to meet a state law, regulation, or rule; the requirement is necessary to satisfy state security requirements; the requirement is necessary to interface or integrate with state systems; or the requirement will produce a material improvement in service delivery, partner interactions, or utilization of state resources. Material improvements must be documented, justified, and presented to the Project Steering Committee for review.

All customizations require written approval from the Project Steering Committee before work begins. The State’s strong preference is to implement requirements through configuration of the vendor’s standard functionality rather than custom development, in order to maintain a solution that is as near to COTS as possible.

Each customization proposal must include:

* A configuration-first analysis demonstrating why configuration cannot meet the requirement
* A functional specification
* A technical design
* An impact analysis addressing maintenance, upgrade compatibility, security, performance, accessibility, total cost of ownership
* A test plan and rollback plan
* Schedule impact
* Itemized pricing, if applicable

Approved customizations must:

* Pass the same acceptance tests as core functionality
* Be upgrade-compatible or provide a documented migration path
* Meet State security standards

The vendor will deliver source code, developer and user documentation, and a perpetual royalty-free license for any custom code. Additionally, the State expects the vendor to consider approved and implemented customizations for incorporation into the vendor’s core solution going forward so that they become standard out-of-the-box functionality.

**Data Structure:** State administration must always have access to the data structure including all available data points, tables, and code for review and monitoring.

* 1. **Security & Compliance**: All proposed solutions must comply with state and federal data security standards, including but not limited to:
* **Indiana Senate Enrolled Act 472 (SEA 472)**, effective July 1, 2025, which mandates that all public entities—including state agencies and educational institutions—adopt and maintain:
  + A cybersecurity policy aligned with guidance from the Indiana Office of Technology (IOT)
  + A uniform technology resource use policy
  + Mandatory cybersecurity training for all users
* **Executive Order 25-19**, which requires vendors providing cloud-based or hosted services to:
  + Demonstrate compliance with NIST 800-53, Revision 5, or submit a roadmap to achieve compliance
  + Undergo continuous risk assessments and monitoring by an independent, nationally recognized organization
  + Include contractual language that ensures ongoing compliance and transparency with the State’s Risk and Authorization Management Program (RAMP)
* **RAMP alignment**, where applicable, to ensure that cloud service providers meet rigorous cybersecurity standards consistent with federal and state expectations. See both <https://govramp.org/> and <https://www.in.gov/iot/iot-vendor-engagement/> for more information.
* **Data Protection Laws**, including the Indiana Data Breach Notification Act and the Indiana Personal Information Protection Act, which require timely breach reporting and the safeguarding of personally identifiable information (PII). See <https://www.in.gov/mph/cdo/files/State-of-Indiana-Information-Privacy-Policy.pdf> for more information on the Management Performance Hub (MPH) policies.
* **Authentication**: The proposed solution is expected to integrate with Access Indiana. The [IN.gov Program](https://www.in.gov/inwp/) is tasked with implementing a single sign-on authentication mechanism and Identity Provider for online applications for the State of Indiana, referred to as Access Indiana. The benefits of a standard authentication solution, integration strategy, integration process, and more can be found at [Access Indiana Authentication](https://www.in.gov/inwp/applications/authentication/) (<https://www.in.gov/inwp/applications/authentication/>).
* **Artificial Intelligence (AI)**: The State of Indiana has adopted an enterprise-level policy governing the use of Artificial Intelligence (AI) within state government. The State of Indiana AI Policy is issued and monitored by the Office of the Chief Data Officer (OCDO), in cooperation with the Chief Privacy Officer (CPO) and the Management Performance Hub (MPH). In complement the AI Policy, the State Agency Artificial Intelligence Systems Standard outlines the rationale behind the AI Readiness Assessment process required for the implementation or any use of AI by a state agency. The standard outlines the requirement for the submission of a Readiness Assessment Questionnaire prior to implementation or use of an AI tool or system. Any proposed solution meeting these requirements must support the State’s AI Policy and follow the AI Readiness Assessment Process. See <https://www.in.gov/mph/AI/> for more detailed information.
* **Dat Exchange**: The Contractor’s solution must support the State’s standard API and file transfer methods to facilitate secure data transmission. The State’s standardized data transmission technologies are the MuleSoft API Management and GoAnywhere Managed File Transfer (MFT) services. See <https://www.in.gov/iot/policies-procedures-and-standards/applications-standards/>. Elaborate on how your company’s solution will accommodate the utilization of the identified technologies. If the proposed solution does not support these technologies, explain in detail why and outline the proposed alternative.
* **Independent Verification and Validation:**
  + IV&V Engagement

If the State decides to add Independent Verification & Validation (IV&V) services as part of this engagement, the contractor will copy the Indiana Department of Administration (IDOA) – Independent Verification & Validation (IV&V) team member(s) on all project related communications (emails, meeting invites, collaboration tools, etc.) and will grant access to all documents and deliverables throughout the term of the contract.

* + IV&V Payment Approval

If IDOA elects to deploy Independent Verification and Validation (IV&V) services in connection with this engagement, the IV&V Team shall review and assess all Deliverables to determine compliance with the State’s requirements as set forth in the Contract and/or applicable Statement(s) of Work. For contracts entered into, renewed, or amended after June 30, 2026, IV&V shall serve as an approving authority, and no payment shall be issued to the Vendor unless and until IV&V has provided such approval.

* **Data Ownership:** The State owns all rights, title, and interest in the data. The Contractor shall not access State user accounts or data, except: (1) in the normal course of data center operations; (2) in response to service or technical issues; (3) as required by the express terms of this contract, applicable Scope of Work, or applicable Service Level Agreement; or (4) at the State’s written request. Contractor shall not collect, access, or use data except as strictly necessary to provide service to the State. No information regarding State’s use of the service may be disclosed, provided, rented, or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this contract.
  + 1. All documentation and source code developed under this contract shall be the sole property of SOI. The vendor shall not withhold any documentation or tools necessary for the continued operation and maintenance of the system.
  1. **Ensuring Data Security and Privacy**

The State has robust and comprehensive security standards that permeate all levels of the organization. The Indiana Office of Technology (IOT) has been tasked with establishing and maintaining these security standards. The security standards include assessing security risks, developing and implementing effective security procedures, and monitoring the effectiveness of those procedures.

The following link introduces the IOT Information Security Framework (ISF): https://www.in.gov/iot/iot-vendor-engagement/. Everyone intending to access ISF policies will need to create an Access Indiana account first. Respondents will be required to sign a Non-Disclosure Agreement (NDA) to access the IOT Information Security Framework.

The Contractor shall ensure the security and confidentiality of all information. The Contractor must adhere to the State’s standards and establish, maintain, implement and manage the data ownership standards, data security standards, and arbitration protocol. In addition, the Contractor shall implement and maintain standards for confirming that only lawfully authorized users are granted access to any systems maintained by the Contractor on behalf of the State and prevent unauthorized access, use, abuse, disclosure, disruption, modification, or destruction of data.

In addition to the State standards outlined above, the State requires that the Contractor support all current and future PII/PHI Security rules, as well as any applicable federal automated data processing requirements.

The Contractor shall ensure security safeguards are in place to assure the integrity of System hardware, software, records, and files. To maintain privacy and security standards, the Contractor shall perform the roles and responsibilities listed below, including but not limited to:

* 1. Establishing, maintaining, implementing and managing privacy standards in accordance with State and Federal standards;
  2. Mitigating, to the extent practicable, any harmful effect that is known to the Contractor of PII obtained under this contract in a manner not provided for by this contract or by applicable law of which the Contractor becomes aware;
  3. Training all staff on the privacy and security requirements;
  4. Testing security compliance quarterly;
  5. Applying required changes to security methods that security compliance testing identifies;
  6. Complying with all confidentiality, security, infrastructure, application, and service solution standards established by the State in this SOW;
  7. Orienting new employees to security policies and procedures;
  8. Conducting periodic review sessions on security procedures;
  9. Developing lists of personnel to be contacted in the event of a potential or suspected security breach;
  10. Limiting physical access to systems hardware, software, and libraries; and
  11. Maintaining confidential and critical materials in limited access, secured areas.

**Minimum Security Expectations:**

* Role-based access control and user authentication
* Encryption of data at rest and in transit
* Audit logging and monitoring capabilities
* Secure integration with other state systems using Mulesoft
* Regular vulnerability assessments and patch management
* Incident response and disaster recovery protocols
  1. **User Experience:** All proposed solutions must prioritize intuitive, accessible, and mobile-friendly user interfaces that meet the diverse needs of Indiana’s workforce development stakeholders, including educators, administrators, training providers, and the public.

**Minimum User Experience Expectations:**

* **Intuitive Design:** Interfaces should be easy to navigate, with clear workflows, consistent layouts, and minimal cognitive load. Systems should follow established usability principles.
* **Accessibility Compliance:** In accordance with Indiana Code § 4-13.1-3 and the IN.gov Accessibility Policy, all systems must comply with the Web Content Accessibility Guidelines (WCAG) 2.1, ensuring that digital services are usable by individuals with disabilities, including those using assistive technologies.
* **Mobile Responsiveness:** Interfaces must be fully functional and optimized for use on mobile devices and tablets, supporting responsive design principles to ensure usability across screen sizes and platforms.
* **Role-Based Customization:** The system should provide tailored experiences based on user roles (e.g., data entry, administrators, reviewers), with dashboards and workflows that align with each user’s responsibilities.
* **User-Centered Design Process:** Vendors are encouraged to demonstrate how their solution incorporates user feedback, usability testing, and continuous improvement practices.

**8.5 Integration:** All proposed solutions must support, as needed, seamless, secure, and standards-based data integration with existing systems used by the Indiana Department of Workforce Development (DWD), the Commission for Higher Education and other relevant state agencies. Integration is essential to ensure data continuity, reduce duplication, and enable cross-program analysis that supports informed decision-making and improved service delivery.

**Minimum Integration Expectations:**

* **Real-Time and Scheduled Data Transfers:** Systems should support both real-time and batch data transfers to accommodate different operational and reporting needs.
* **Data Mapping and Transformation:** The solution must include tools or services to map, transform, and validate data during import/export processes to ensure consistency and accuracy.
* **Audit Trails and Logging:** All data exchanges must be logged and auditable to support compliance, troubleshooting, and security monitoring.
* **Compliance with the Indiana Open Data Act:** Solutions must align with the Indiana Management Performance Hub (MPH) framework, which governs interagency data sharing and analytics. This includes participation in data governance practices and use of standardized data sharing agreements.
  1. **Scalability & Maintenance:** Solutions must be scalable as needed and include long-term support and maintenance plans.
  2. **Training & Documentation**: To ensure successful implementation, adoption, and long-term sustainability of the proposed solutions, vendors must provide comprehensive training, user support documentation, and ongoing support services tailored to the needs of Indiana’s diverse user base.

**Minimum Requirements:**

* **Initial Training & Onboarding:**
  + Provide structured training sessions for all user roles (e.g., administrators, data entry staff, educators, grant managers).
  + Include “train-the-trainer” models to support internal capacity building within DWD and partner organizations.
  + Develop and deliver a detailed knowledge transfer plan and training session to state personal and other end users as needed prior to project closeout.
* **User Documentation:**
  + Develop and maintain clear, role-specific user guides, quick reference materials, and FAQs.
  + Documentation must be accessible, searchable, and available in digital, printable formats.
  + Materials should be updated regularly to reflect system enhancements or policy changes.
* **Ongoing Support:**
  + Offer responsive help desk or customer support services with defined service level agreements (SLAs).
  + Support must include multiple channels (e.g., phone, email, ticketing system) and be available during standard business hours, with options for extended support during critical reporting periods.
  + Provide regular system updates, bug fixes, and enhancements as part of a maintenance plan. Updates must be extensively tested in a sandbox setting prior to pushing live.
* **Refresher & Update Training:**
  + Conduct periodic refresher training and onboarding for new users.
  + Offer training aligned with major system updates, new features, or changes in federal/state reporting requirements.
  1. **AI** **technologies**

We seek transformative and innovative solutions executed and delivered by a skilled team via efficient and effective mechanisms. See the AI – Technical Proposal Questions attachment. Respondents are encouraged to consider AI and related emerging technologies, through the lens of public sector by offering concise and succinct responses.

## **Project Management Requirements**

To ensure proper collaboration and coordination between the Contractor, the State, DWD, and CHE, the Contractor shall comply with the following project management requirements.

* 1. **Point of Contact**:

The Contractor shall designate a primary point of contact with whom the State will primarily communicate. Any changes to this point of contact must be communicated to the State within two (2) business days of the change.

* 1. **Meeting Requirements:**

The Contractor is required to actively participate in regularly scheduled meetings and ad hoc meetings as requested by the State. These meetings are necessary to coordinate with relevant stakeholders and ensure the smooth operation of the project.

* **Kick-Off Meeting:**  
  As soon as practical after the mutually agreed upon project start date, the Contractor and State shall hold a kick-off meeting. The goal of this meeting is to make all necessary introductions between the State and Contractor and establish expectations and timelines for all deliverables.
* **Status Meetings:**  
  The Contractor shall meet with State staff and designees a minimum of once every 14 business days, or as requested, to present status updates, discuss change requests, resolve challenges, and review progress on work plans and project plans. The State reserves the right to change the cadence of these meetings at any point in the contract term.
* **Meeting Deliverables:**  
  For all meetings, the agenda and materials shall be sent to DWD/CHE at least one (1) calendar day prior to the meeting. The Contractor must also submit a list of attendees from their organization. The State reserves the right to request specific attendees if the project is not progressing as expected. The Contractor shall record and prepare meeting minutes and provide them to the State within fivebusiness days after the meeting. Agendas and minutes are subject to State review and approval.
  1. **Status Reporting**

The Contractor shall provide regular status reports to the State, including but not limited to:

* Current status of major scheduled tasks
* Recent accomplishments and setbacks
* Objectives for the next reporting period
* Staffing changes
* Key decisions made
* Release summary and testing status
* Change control summary
* Configuration management summary
* Defects identified and resolution status
* Training summary
* Outstanding issues and action items
* Security Summary
  1. **Project Governance**

The Contractor shall provide an overall project organizational chart that includes roles and responsibilities for both the Contractor and State teams. The Contractor shall also outline its recommended governance structure and escalation process for resolving risks and issues.

* 1. **Project management tool/platform**

Responsibility of the winning vendor but must be approved by SOI. Expect to use a SOI licensed platform such as AzureDevOps.

**9.10 Development Tracking**

Create dashboards to be approved by SOI. Keep development on track.

**9.11 Technology/systems stakeholder engagement**

* State your firm’s proposed approach to stakeholder engagement when it comes to technical teams such as with the respective agency’s IT staff (AE, ETP, CTE) and centralized IT (IOT).
* Tell us about:
  + Your understanding or assumptions of how agency IT works with IOT.
  + A plan that has proven successful and one that did not meet expectations when working with a client’s technical teams.
  + Lessons learned in how your firm’s approach has evolved.

## **Plans and Procedures**

The Contractor shall develop and maintain comprehensive plans and procedures to ensure successful implementation, compliance, and sustainability of the solution. These plans must be submitted to the State for review and approval within the timelines specified below.

* 1. **Project Plan:**

Submit a detailed Project Plan within thirty (30) business days of contract execution.

The Project Plan must include:

* Description of all tasks, deliverables, schedules, and dependencies.
* Identification of resource requirements for both Contractor and State.
* Approach to transitioning from the current system.
* Architectural diagram and explanation of how components work together.
* Milestones for design, development, testing, and implementation.
* Language permitting State access to the Contractor’s system for as many users as deemed necessary.
  1. **Change Control Plan:**

Submit a detailed Change Control Plan sixty (60) business days prior to commencement of services.

The plan must define:

* Process for identifying, validating, approving, and implementing changes.
* Roles and responsibilities for change management.
* History tracking of all change requests, including cost and schedule impacts.
  1. **Issue Resolution Plan:**

Submit an Issue Resolution Plan thirty (30) business days after contract execution.

The plan must include:

* Standard process for identifying, tracking, and resolving issues.
* Risk management strategies to prevent issues from occurring.
* Metrics for measuring resolution success.
  1. **Risk Management and Mitigation Plan:**

Submit a Risk Management Plan thirty (30) business days after contract execution.

The plan must include:

* Risk identification and prioritization.
* Mitigation strategies and contingency plans.
* Tools for tracking and reporting risk status.
  1. **Testing Plan:**

Submit a Testing Plan within forty-five (45) business days of contract execution.

The plan must include:

* Test cases and data.
* Roles and responsibilities for testing.
* Approach for User Acceptance Testing (UAT) prior to Go-Live.
* Regression testing procedures for updates.
  1. **Training Plan:**

Submit a Training Plan within forty-five (45) business days of contract execution.

The plan must include:

* Initial and ongoing training strategy.
* Train-the-trainer model.
* Curriculum overview and delivery methods (virtual, in-person, on-demand).
* Maintenance of training materials.
  1. **Requirements Plan:**

Submit a Requirements Plan within forty-five (45) business days of contract execution.

The plan must include:

* Approach for gathering and validating requirements.
* Traceability matrix to ensure all requirements are met.
* Process for addressing new requirements before implementation.
  1. **Data Security Plan:**

Submit a Data Security Plan sixty (60) business days prior to commencement of services.

The plan must include:

* Steps to ensure compliance with StateRAMP, NIST 800-53, FERPA
* Encryption standards for data at rest and in transit.
* Secure destruction of data when required.
  1. **IT Business Continuity and Disaster Recovery Plan:**

Submit a comprehensive ITBCP sixty (60) business days prior to commencement of services.

The plan must include:

* Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO).
* Disaster recovery testing schedule and reporting.
* Roles and responsibilities during outages.
  1. **End-of-contract Transition Plan:**

Submit a Transition Plan at least one hundred eighty (180) business days prior to contract end.

The plan must include:

* Approach for transferring all data, documentation, and system components.
* Knowledge transfer sessions for State personnel.
* Timeline for transition activities.
  1. **Communication Plan**

Sumit a Communications Plan within thirty (30) business Days of contract execution.

The plan must include:

* Methods and frequency for project communications (e.g., email, meetings, reports)
* Identification for key stakeholders and roles
* Escalation procedures for critical issues
* Schedule for status meetings and reporting requirements.

## **Reporting**

The Contractor shall furnish all reports required by the State under this Contract in a timely, complete, and accurate manner. Reporting requirements may evolve during the contract term to align with State and Federal obligations. The Contractor must maintain flexibility to accommodate new reporting needs as directed by DWD and CHE.

**11.1 Monthly Status Reporting**

* Submit a monthly status report within five (5) business days after the last day of the month.
* The report shall include:
  + Current status of major scheduled tasks
  + Recent accomplishments and setbacks
  + Objectives for the next reporting period
  + Staffing changes
  + Key decisions made
  + Release summary and testing status
  + Change control summary
  + Configuration management summary
  + Defects identified and resolution status
  + Training summary
  + Outstanding issues and action items

**11.2 Service Levels Report**

* Provide a monthly report on adherence to Service Level Agreements (SLAs).
* Include:
  + Proof of performance for each SLA
  + Summary of any service levels not met
  + Remediation plan for non-compliance

**11.3 Program-Specific Reporting**

* The Contractor shall support reporting requirements defined by business units for:
  + **Adult Education (AE):** NRS performance indicators, Title II compliance reports, enrollment and outcome tracking.
  + **Career and Technical Education (CTE):** Perkins V accountability reports, CLNA documentation, credential attainment.
  + **Eligible Training Provider (ETP):** WIOA Title I performance reports, provider eligibility audits, program cost and outcome data.
* These reports may include:
  + Scheduled submissions to Federal systems (e.g., NRS, Perkins reporting portals)
  + State dashboards and public-facing data
  + Ad hoc reports requested by DWD, CHE, or Federal entities

**11.4 Ad Hoc Reports**

* Respond to ad hoc reporting requests within timelines specified by the State:
  + **Type 1:** 1–2 business days turnaround
  + **Type 2:** 5 business days turnaround
  + **Type 3:** 10 business days turnaround
* Emergency requests may require completion in less than 24 hours.

**11.5 Full-stack observability tool**

* **The vendor is expected to learn and use a full-stack observability tool**
* The team is to become acclimated with the SOI tool and use it proficiently to investigate and diagnose. SOI currently uses AppDynamics.

## **Data Migration**

The Contractor shall develop and execute a secure Data Migration Plan approved by the State. Migration will include all in-scope data and attachments from the current Inters system, estimated at 1.2 TB, with historical data migrated back to 2002 (later date may be optional).

The Contractor shall accommodate migration for each solution (AE, CTE, ETP) independently. Migration planning and execution must enable any one solution to migrate and go live without dependency on the others.

* All PII and PHI must be encrypted in transit and at rest, with audit logging and role-based access.
* The plan must include mapping, validation, rollback procedures, and reconciliation reports.
* Lower environments must use masked data unless otherwise approved.

## **Implementation**

The State does not prescribe a specific approach (phased, pilot, or big bang). The Contractor shall propose an Implementation Plan for each solution (AE, CTE, ETP). Solutions may go live independently with no dependency risk.

The plan must include:

* Milestones and cutover steps
* Readiness criteria
* Communication and training alignment
* Backout procedures
* The Contractor shall minimize downtime and ensure a smooth transition from the incumbent vendor.

## **Testing**

The Contractor shall conduct testing, including user acceptance testing in accordance with the Testing Plan approved by the State. Testing shall be conducted both prior to initial go-live and prior to the release of any additional enhancements and updates throughout the Contract term. DWD & CHE shall be provided an opportunity to test all upcoming changes in the UAT environment prior to implementation into production.

The Contractor shall deliver a Testing Plan approved by the State and conduct testing prior to go-live and for all future releases. Testing must include:

* Functional, integration, regression, performance, security, and accessibility testing
* User Acceptance Testing (UAT) with full State participation
* Data conversion validation
* The State may engage a third-party testing provider (e.g., iLab); the Contractor shall fully cooperate.
* Go-live requires zero Severity-1 or Severity-2 defects and formal State acceptance.

## **Readiness Review and Go-Live**

At least thirty (30) business days before the Contractor System becomes operational, the Contractor must pass a readiness review for State approval. The Contractor must show that all systems are operating as expected and that all DWD requirements are included. Any exceptions to the readiness review timeline and due dates stated within this Section or within the Scope of Work must be approved by the State, in writing, at least sixty (60) business days prior to the commencement of Contractor program operations. The Contractor must establish that their systems are operational and ready for full-time service.

## **Maintenance and Operations (M&O)**

16.1 After the System is live and operational, the Contractor shall continue to provide M&O support for the System. These duties shall include:

1. Contractor shall perform System enhancements, releases, and maintenance as needed;
2. Contractor shall conduct enhancements and changes in line with the Change Control Plan approved by SOI;
3. Contractor shall provide prompt and accurate release notes to the State ahead of any scheduled enhancement/release;
4. Contractor shall make SOI aware of all changes to production at least one 5 business days prior to planned implementation. SOI will have ultimate authority to approve or deny changes before they are made in production;
5. Contractor shall coordinate all maintenance windows with the State to minimize any impact on operations;
6. Contractor shall communicate anything scheduled or known that might impact System downtime to the State as soon as the Contractor becomes aware or at least seven (7) calendar days in advance before the performance of that activity;
7. Contractor shall provide a history of maintenance and support releases to the State upon the State’s request;
8. Contractor shall maintain a HelpDesk to support front end System issues and technical assistance questions. Such HelpDesk shall be available at a minimum within the State's traditional business hours of operation;
9. Contractor shall continuously update the training materials contemplated to reflect the most up-to-date System information and provide periodic refresher training as requested by the State;
10. Contractor shall support the State with any ad-hoc report or query development requests, in a mutually agreed upon format and timeframe; and
11. The Contractor shall be required to ensure that all its systems are available, on-line and operational in accordance with the service levels contemplated by this contract.

**16.2 Outage Notifications**

In the case of an unplanned System outage, the Contractor’s account manager or another designated staff member will generate outage notifications to all state administrators and designated staff via an outage email distribution list. The email will include a description of the issue and end user impact. Notifications will be sent in thirty (30) minute intervals until the issue is resolved. Upon resolution, a service restored email notification will be sent to the State Administrators. The Contractor will provide a Root Cause Analysis to the State Administrator within forty-eight (48) hours of the outage event resolution.

**16.3 Backup and Recovery**

a. The system must support automated, scheduled backups of configuration and data.

b. Backup files must be encrypted and stored in a secure, administrator-defined location.

## **End-of-Contract Transition Requirements**

No less than one hundred eighty (180) calendar days prior to the end of the Contract period, the Contractor shall develop and submit to SOI an End-of-Contract Transition Plan covering the transition of the System. End-of-Contract Transition Plan shall be a comprehensive document detailing the proposed schedule and activities associated with the transition tasks, including the approach and schedule for transfer of all project artifacts and documentation created, maintained, and updated throughout the Contract term. As part of the transition plan, the Contractor shall provide a copy of non-proprietary system components or database(s) used. End-of-Contract Transition Plan is subject to SOI review and approval.

**What is to be expected from a technical perspective when the contract ends?**

* + An official off-boarding plan for approval by each team will be expected when the time comes to end services with a timeframe defined by each SOI team. The plan should include knowledge transfer sessions with designated SOI personnel, walkthroughs of the system architecture, deployment procedures, and maintenance routines. The vendor will submit a closeout plan (for each system) as requested. Again, the official plan is subject to approval by SOI. Labor rates for closeout activity will be no higher than rates for non-closeout work.

## **MULTI-TENANT ARCHITECTURE**

CHE-CTE & DWD is interested in their solution being built to accommodate multi-tenant architecture. This is not a hard requirement but of sufficient interest to warrant a mention. If your firm can deliver single or multi-tenant, CHE requests both architectures be proposed as options in the response for CHE to consider.

* Key design principles include but are not limited to:
  + Isolation by Design
    - Strong boundaries for data, identity, compute, and networking.
    - Prevent cross‑tenant data access and “noisy neighbor” performance impacts.
  + Shared‑Nothing Code, Shared‑Smart Infrastructure
    - One codebase; shared platform services where safe and efficient.
    - Parameterize behavior via tenant configuration/feature flags.
  + Control Plane vs. Data Plane
    - Control plane: global services for onboarding, provisioning, routing, metering, billing, and policy.
    - Data plane: tenant workloads, storage, and runtime execution.
  + Tenancy‑Aware Everything
    - Every request, job, and data artifact is tagged with a Tenant ID.
    - Policies and telemetry filter by Tenant ID.
  + Security First
    - Zero‑trust, least privilege, encryption in transit & at rest, audited access paths.
    - Regulatory partitions (HIPAA, FERPA, CJIS, etc.) as needed.
  + Scalability and Resilience
    - Horizontal scaling, sharding/partitioning, rate limiting, per‑tenant SLOs.
    - Disaster recovery with per‑tenant restore and region failover.
* The proposed solution must be designed and developed as a multi-tenant SaaS application, using Microsoft .NET (preferably .NET 8 or later), hosted in IOT’s Microsoft Azure tenant, and leveraging IOT GitHub Enterprise for source control, code reviews, and CI/CD automation.
  + Vendor is expected to adhere to software development best practices for building scalable, secure, and maintainable multi-tenant applications, leveraging Azure-native services and .NET capabilities.
  + Architecture Design & Scalability
    - Use a multi-tenant architecture that supports secure, scalable, and efficient tenant onboarding and management.
    - A shared codebase to support all tenants, with logical data isolation and per-tenant configuration options in IOT GitHub Enterprise.
    - Design to run on Azure App Services, Azure Kubernetes Service (AKS), or Azure Container Apps, with support for horizontal scaling based on tenant demand.
    - Architecture to allow for tenant-specific configurations, such as feature flags, custom branding, and access control policies using Azure App Configuration or similar tools.
  + Data Isolation & Security
    - Tenant data must be logically isolated using Row-Level Security (RLS) in Azure SQL Database, or via schema-per-tenant design, based on scalability needs.
    - Vendors must explain their data partitioning strategy and justify the choice based on tenant count, performance, and operational complexity.
    - Use of Azure Key Vault is required for managing per-tenant secrets, connection strings, and encryption keys.
    - Application Authorization must implement AccessIN for Indiana customers while being modular for other Authorization standards for potential out of State customers.
    - All data in transit and at rest must be encrypted using TLS 1.2+ and AES-256 encryption, aligned with Azure security best practices.
  + Deployment & Environment Management
    - Code must be managed using GitHub Enterprise, with clearly defined branching strategies (e.g., GitFlow or trunk-based development).
    - CI/CD pipelines must be implemented using GitHub Actions, with automated testing, build, and deployment workflows.
    - Support for blue/green or canary deployments in Azure must be included to minimize downtime and enable safe feature rollouts.
    - Environment-specific configurations must be managed securely using Azure App Configuration or Azure Key Vault.
  + Tenant Onboarding and Lifecycle Management
    - Provide support for automated tenant provisioning through secure APIs or administrative interfaces.
    - Each tenant must be initialized with a base configuration (e.g., branding, roles, data schema), stored securely and managed centrally.
    - Support for self-service onboarding flows (optional) via web portal or integration with external systems
    - Tenant lifecycle operations (activation, suspension, deletion) must be audit-logged and reversible where applicable.
  + Monitoring, Logging & Auditing
    - Use Azure Monitor, Application Insights, and Log Analytics for centralized monitoring with tenant-level correlation.
    - All API calls, admin actions, and data access must be audit-logged with tenant context for traceability and compliance.
    - Define and enforce rate limiting and quotas per tenant using Azure API Management or custom middleware.
  + Compliance & Data Governance
    - The solution must adhere to applicable regulatory, WCAG accessibility, and security standards.
    - All tenant data must be exportable and deletable upon request, with secure, auditable workflows for managing data lifecycle events.
    - Ensure multi-region support for tenants, with data residency options configurable by region using Azure’s infrastructure.
  + Extensibility & Customization
    - The application should support tenant-specific feature toggles using tools such as LaunchDarkly or Azure App Configuration Feature Management.
    - Allow extensibility via webhooks, plugin architecture, or API gateways for tenant-specific integrations.
    - Support tenant-level overrides for templates, content, roles, and workflows without altering the core codebase.