**RFP 26-85723**

**TECHNICAL PROPOSAL**

**ATTACHMENT F**

|  |
| --- |
| **INSTRUCTIONS** |
| * Please supply requested information ***in the blue-shaded areas*** and indicate any attachments that have been included. * Document all attachments with which section and question they pertain to. * Request for Proposal (RFP) for Inters is a solicitation issued by the State of Indiana in which organizations are invited to compete in a formal evaluation process. Your proposal will be evaluated by a team of State of Indiana employees, and your organization’s score will reflect that evaluation. The technical proposal can only be based on the information you provide in this Attachment F. A competitive proposal will thoroughly address all components of the State’s Scope of Work (Attachment F) and follow the section numbering used in the SOW. Please limit your response to 50 pages or less (not including appendices). Use the response boxes provided; you may reference exhibits/appendices if they are clearly labeled in the response box |

1. **Introduction**
   1. Provide an executive summary of your technical proposal and an overview of your solution, including how it supports AE, CTE, and ETP needs across DWD and CHE. Confirm you have reviewed the SOW introduction and understand the State’s goals.

|  |
| --- |
|  |

1. **Overview**
   1. Confirm your understanding of, and agreement with, the requirements outlined in Section 2 of SOW. Describe how you will address these challenges and align with the overview in SOW.

|  |
| --- |
|  |

1. **Definitions**
   1. Confirm that you have read and understand all definitions listed.

|  |
| --- |
|  |

* 1. Please list any additional terms and definitions used by your company or industry that you would like the State to consider incorporating in the contract. The State will not accept terms and definitions introduced after award, during contract finalization, and implementation

|  |
| --- |
|  |

1. **Adult Education (AE) Student Management System**
   1. Explain how your solution satisfies the AE Purpose in the SOW.

|  |
| --- |
|  |

Describe in detail how you meet each Key requirement.

**Explicitly detail your experience with NRS and Title II reporting**.

|  |
| --- |
|  |

1. **Eligible Training Provider (ETP) & OCTS Management System**
   1. Explain how your solution satisfies the ETP & OCTS purpose in the SOW.

|  |
| --- |
|  |

* 1. Describe in detail how you meet each key requirement.

|  |
| --- |
|  |

1. **Career and Technical Education (CTE) Student Data Collection System**
   1. Explain how your solution satisfies the CTE purpose in the SOW.

|  |
| --- |
|  |

* 1. Describe in detail how you meet each key requirement.

|  |
| --- |
|  |

1. **Desired Contractor Qualifications**
   1. Confirm and demonstrate how you meet the desired qualifications (NRS/Title II experience; integration with state platforms as required.

|  |
| --- |
|  |

1. **General Expectations for All Solutions**
   1. Describe how your solution complies with Security & Compliance.
      1. Please describe the practices you will put in place to best ensure data security and privacy, including, but not limited to sensitive data that must be protected: Personally Identifiable Information (PII) and Protected Health Information (PHI).

|  |
| --- |
|  |

* + 1. Confirm and describe the laws and regulatory standards your solution will comply with:
* FERPA
* ETP – WIOA Title 1
* ETP – WIOA Title 1 and 20 CFR Part 680
* OCTS – Indiana Code 22-4.1-21-10

|  |
| --- |
|  |

* + 1. Describe your firm’s approach and agreement to comply with:
* The system must comply with applicable laws and standards (e.g., NIST 800-53).
* All data in transit and at rest must be encrypted using industry-standard practices.
* Execute all sessions and REST type web services (internal and external) via HTTPS utilizing SSL certificates.
* Encrypt data while at rest and in transit in accordance with encryption standards meeting FIPS 140-2 with future ability to meet FIPS 140-3.
* Address security issues such as SQL injection, cross-site scripting, broken authentication, and session management.
* Protect the confidentiality of all customer data based on federal and state laws (e.g., 20 CFR 603, FERPA) and in accordance with NIST 800-53, current version).

|  |
| --- |
|  |

* + 1. Can the proposed product or solution integrate with Access Indiana (<https://www.in.gov/inwp/applications/authentication/>)?

|  |
| --- |
|  |

* + 1. 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.

|  |
| --- |
|  |

* 1. Describe how your solution complies with Data Ownership

|  |
| --- |
|  |

* 1. Describe how your solution complies with Ensuring Data Security and Privacy

|  |
| --- |
|  |

* 1. Describe how your solution complies with User Experience

|  |
| --- |
|  |

* 1. Describe how your solution complies with Integration

|  |
| --- |
|  |

* 1. Describe how your solution complies with Scalability & Maintenance

|  |
| --- |
|  |

* 1. Describe how your solution complies with Training & Documentation

|  |
| --- |
|  |

* 1. Describe how your solution complies with AI Technologies and SOI requirements.

|  |
| --- |
|  |

1. **Project Management Requirements**
   1. Confirm your understanding of, and agreement with, the requirements outlined in Section 9 of SOW. Provide a document to describe your company’s project management approach and methodology for this project.

|  |
| --- |
|  |

* 1. Confirm understanding of 9.10 in SOW. Provide examples and characteristics of what successful development tracking means to your firm and what pitfalls your team has learned to avoid through experience. Outline what you propose for SOI.

|  |
| --- |
|  |

* 1. Confirm understanding of 9.11 in SOW.

|  |
| --- |
|  |

1. **Plans and Procedures**
   1. Confirm your understanding of, and agreement with, the requirements outlined in section 10 of the SOW. Provide high-level descriptions and timelines for each plan in the SOW.

|  |
| --- |
|  |

1. **Reporting**
   1. Confirm your understanding of, and agreement with, the requirements outlined in Section 11 of SOW.

|  |
| --- |
|  |

* 1. Describe your approach for managing and maintaining the following reports, including how you will ensure all reports are submitted in an accurate and timely manner.

|  |
| --- |
|  |

1. **Data Migration**
   1. Describe your company’s overall data migration strategy, plan, and methodology. Include data extraction, cleansing, mapping, and conversion, and testing.

|  |
| --- |
|  |

* 1. Describe what tools or platforms will you use for migration so to include the archive and retrieval capabilities for a cost effective solution? How do you protect sensitive data during migration?
  2. Describe your proposed storage architecture for approximately 1.2 TB of data, including tiering, archiving strategy, replication for disaster recovery, and expected performance for data access and retrieval. Explain how your design scales over time and supports compliance/security requirements.
  3. Provide a detailed cost breakdown for storing and managing 1.2 TB of data, including costs for base storage, archiving, replication, retrievals, and any additional fees.

|  |
| --- |
|  |

1. **Implementation**
   1. Confirm your understanding of, and agreement with, the requirements outlined in section 13 of the SOW. Describe your company’s implementation strategy (Pilot, phased rollout, “big bang”, etc.). Provide details for the following listed in the SOW.

|  |
| --- |
|  |

* 1. Describe your firm’s approach to launch of new solutions and implementation support.

|  |
| --- |
|  |

1. **Testing**
   1. Confirm your understanding of, and agreement with, the requirements outlined in Section 14.0 in SOW.
   2. Describe your comprehensive testing strategy, including an approach to testing prior to initial go-live as well as testing prior to the release of enhancements

|  |
| --- |
|  |

* 1. Describe how you will ensure that DWD & CHE has the opportunity to test all upcoming changes in the UAT environment prior to implementation into production.

|  |
| --- |
|  |

1. **Readiness Review and Go-Live**
   1. Confirm your understanding of, and agreement with, the requirements outlined in Section 15 of SOW.

|  |
| --- |
|  |

* 1. Describe your process for conducting readiness reviews prior to go-live, ensuring the System, staff, and data are prepared for transition to production.

|  |
| --- |
|  |

1. **Maintenance and Operations (M&O)**
   1. Confirm your understanding of, and agreement with, the requirements outlined in Section 16 of SOW.

|  |
| --- |
|  |

* 1. Describe your approach to maintaining and operating the System after Go-Live including ongoing support. Your response must:

Describe your HelpDesk support.

Describe your approach to enhancements and releases, including how you will ensure the State is provided accurate release notes and is aware of changes to production.

|  |
| --- |
|  |

* 1. Outline your process of notifying the State of unplanned outages in line with the expected communication timelines in Section 16.2 of SOW. Describe your process for timely resolution and Root Cause Analysis.

|  |
| --- |
|  |

* 1. Outline your process for backup and recovery process. Provide a high-level example of a disaster recovery plan.

|  |
| --- |
|  |

1. **End-of-Contract Transition Requirements**
   1. Confirm your understanding of, and agreement with, the requirements outlined in Section 17 of SOW.

|  |
| --- |
|  |

* 1. Submit an example of a successful offboarding plan your firm has executed with this response.

|  |
| --- |
|  |

1. **Service Levels** 
   1. Can you provide high availability systems? What is considered high availability?

|  |
| --- |
|  |

* 1. What are your company’s service levels for hosting, help desk, etc.?

|  |
| --- |
|  |

* 1. How often are the service levels reviewed, and will the State be provided with service level results for each period?

|  |
| --- |
|  |

* 1. Provide details and describe service levels for incident response. Include how incidents will be handled and communicated to the State.

|  |
| --- |
|  |

* 1. Please provide proposed corporate service levels for the State’s review.
  2. Describe your firm’s approach and agreement to comply with non-disruptive production updates where possible.

|  |
| --- |
|  |

1. **Documentation**
   1. Describe your firm’s approach to documentation:

* The vendor shall be responsible for providing and continually maintaining comprehensive documentation for all components as deemed necessary by SOI. This includes, but is not limited to:
  + Technical documentation (architecture, data models, APIs, system configuration)
  + User documentation (user guides, training materials, FAQs)
  + Administrator documentation (installation, configuration, and maintenance procedures)
  + Change logs and version history
* All documentation must be in editable formats (e.g., Word, Markdown, HTML) and updated throughout the development lifecycle, including post-deployment changes to the satisfaction of SOI.
* A detailed knowledge transfer session must be conducted with State personnel prior to project closeout.

|  |
| --- |
|  |

* 1. Confirm and describe how your firm will provide a data dictionary:
  + The vendor shall be responsible for developing and delivering a comprehensive data dictionary. The data dictionary must define all data elements used within the system, including but not limited to:
  + Field names
  + Data types
  + Field lengths
  + Default values
  + Validation rules
  + Acceptable value ranges or enumerations
  + Relationships between data elements (e.g., foreign keys, dependencies)
* Include metadata for each data element, such as:
  + Source system (if applicable)
  + Business definition and purpose
  + Sensitivity classification (e.g., PII, PHI, public)
  + Usage context (e.g., reports, APIs, user interfaces)
* Be delivered in a machine-readable and human-readable format, such as Excel, CSV, or a structured database schema export, and must be updated throughout the development lifecycle.
* Be reviewed and approved by SOI prior to system acceptance.
* Be maintained and updated by the vendor during the maintenance period to reflect any changes to the data model.
* The vendor will report on completeness of the data dictionary on a routine basis as requested and subject to approval by SOI

|  |
| --- |
|  |

1. Application Infrastructure
   1. Confirm and describe where the application’s data will be stored:

All application and data components are to be stored in infrastructure owned, operated or licensed by SOI or SOI approved cloud environments. See accompanying attachments including Infrastructure Overview Attachment N for additional information to be reviewed and responded to.

|  |
| --- |
|  |

1. Software Development Lifecycle Approach (SDLC)
   1. Confirm and describe software engineering practices and standards to be used. It is possible requirements may differ for each team, DWD-AB, DWD-ETP, CHE-CTE.

* Use Infrastructure as Code (IaC) and CI/CD pipelines for deployments. Adhere to SOI standards outlined in this document and attachments.

|  |
| --- |
|  |

* 1. Confirm and describe how security is to be integrated into the SDLC.
* It is critical that the DevOps methodology fosters automation and continuous monitoring to deliver secure, high-quality software faster via DevSecOps. The approach is to be proposed to SOI and implemented by the vendor. SOI currently uses the Veracode platform for vulnerability scanning, static and dynamic scans (SAST and DAST).

|  |
| --- |
|  |

* 1. Confirm and describe preferred DevOps platform and approach. It is possible requirements may differ for each team, DWD-AB, DWD-ETP, CHE-CTE.
* Current recommendation is SOI’s AzureDevOps instance. In 2025 SOI launched ServiceNow’s Strategic Portfolio Management Suite. This may influence use of and integration with ADO for each team.
* Key requirements include but are not limited to:
  + All work is to be captured in Feature, User Stories, etc.
  + Create dashboards to be approved by SOI for real-time work tracking
  + CI/CD pipelines for application deployments will be created and maintained in the Azure DevOps environment.
  + The pipeline should include development, quality assurance, user acceptance testing, staging and production environments where necessary.
  + CI/CD pipelines for the Azure infrastructure resources will be scripted and run through CI/CD pipelines in the Azure DevOps environment.

|  |
| --- |
|  |

* 1. Confirm that your team will utilize the development infrastructure provided by SOI:
* A virtual desktop environment via AWS Workspaces. Development is not to be conducted on physical, local devices. Describe whether and how your team uses such with other customers and what successes and challenges have arisen.

|  |
| --- |
|  |

1. MULTI-TENANT ARCHITECTURE
   1. Confirm your understanding of section 19 in SOW. 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 & DWD to consider.
   2. Confirm whether your solution can be developed as a single application platform that could serve multiple customer organizations (tenants), while ensuring each tenant’s data, configuration, identity, and experience are isolated and secure. The solution should optimize operational efficiency by sharing infrastructure and code, while allowing per‑tenant customization, scaling, and governance.

* Describe your firm’s depth of experience with successful development and support of multi-tenant solutions.
* Vendor Response Requirements
  + High-level architecture diagram showing the multi-tenant structure and use of Azure services.
  + A succinct description of tenant data isolation strategy, including performance and security trade-offs.
  + An explanation of how GitHub Enterprise will be used for source control, branching, code reviews, and CI/CD.
  + Descriptions of how the solution will handle compliance, disaster recovery, and data governance within Azure.
  + A demonstration of experience with multi-tenant .NET applications on Azure, including sample projects or case studies in the last 5 years.

|  |
| --- |
|  |

1. Configuration Management
   1. Describe how auditing of admin and config changes is to be handled: The system must log all administrative actions unless otherwise defined, including but not limited to login attempts, configuration changes, and user management. SOI welcomes proven, and successful practices the vendor has adopted.

|  |
| --- |
|  |

* 1. Confirm and describe how your firm will handle system auditing. It is likely requirements will differ for each team, DWD-AB, DWD-ETP, CHE-CTE. Example audit trails may include but are not limited to.
* Service eligibility audit trail for each customer.
* General audit capabilities around key functionalities such as account creation, modification, disabling, and termination actions then notify, as required, the appropriate users that hold specific roles.

|  |
| --- |
|  |

1. Role Based Access control
   1. Confirm and describe how you will support role-based access. It is possible specific role requirements will differ for each team, DWD-AB, DWD-ETP, CHE-CTE.

* The system must support role-based access control (RBAC). Each team has further defined roles and permissions in functional requirements. Expect team-specific needs to evolve over time.

|  |
| --- |
|  |

1. Password Management
   1. Confirm and describe password management and user retention. It is possible requirements will differ (and evolve) for each team, DWD-AB, DWD-ETP, CHE-CTE.

* All user-password authentication mechanisms must comply with applicable state standards and align with the IOT Vendor Engagement security standards, including the agency‑specific security and regulatory controls from the Security & Regulatory Controls list.
  + **Encryption Requirements**
    - Passwords must be protected using strong encryption both at rest and in transit, in accordance with industry best practices and the IOT: IOT Vendor Engagement standards.
  + **Password Composition & Validation Rules**
    - The password must not be identical to the user’s username.
    - Passwords shall be 8–20 characters in length and include at least:
      * one lowercase letter
      * one uppercase letter
      * one numeric character
      * one special character from this set:! @ # $ % ^ \* .
  + **Password Lifespan & Reuse Restrictions**
    - Passwords must be changed no sooner than every 10 days and no later than every 90 days.
    - Users may not reuse any of their previous 5 passwords.
  + **Session & Account Inactivity Controls**
    - All internal system sessions must automatically timeout after a configurable period of inactivity, as defined by the agency’s session management policy (see IOT Vendor Engagement guidance).
    - User accounts that remain inactive for more than six months must be automatically disabled.
    - Account deletion must be a logical delete, retaining all historical data and profile information as required by agency retention policies.
  + **Auditing & Reporting Requirements**
    - The system must provide audit reporting for:
      * stale (inactive) accounts
      * account lockouts
      * session timeouts and related authentication events
    - All reporting must align with IOT Vendor Engagement control requirements and agency standards listed in the Security & Regulatory Controls inventory.

|  |
| --- |
|  |