Request for Innovative Solutions

(RFIS)

This Request for Innovative
Solutions (RFIS) invites qualified
vendors to demonstrate novel
methods and technologies for
achieving an IDEC Data &
Analytics Hub

**Please respond by submitting
your information via e-mail to:
Illinois Department of Early Childhood
DEC.procurement@illinois.gov
by:**

RFIS Issued November 17, 2025

RFIS Questions Due November 26, 2025 at 12:00 p.m. Central Time

IDEC Response to Questions by December 3, 2025 at 12:00 p.m. Central Time

RFIS Response Due Date December 10, 2025 at 12:00 p.m. Central Time

1 Introduction

Services for young children are currently housed in three separate agencies: the Illinois State Board of Education (ISBE), the Illinois Department of Human Services (DHS) and the Illinois Department of Children and Family Services (DCFS) ("transferring agencies"). On October 24, 2023, Governor J.B. Pritzker issued Executive Order 23-09, which sunset the Office of Early Childhood Development that had existed within the Office of the Governor and sought to create a new Department of Early Childhood. On June 25, 2024, Governor Pritzker signed SB 1 (P.A.103-0594) statutorily creating the Illinois Department of Early Childhood (IDEC). Under the Department of Early Childhood Act (Act), programs from the three transferring agencies will transition to IDEC on July 1, 2026. These programs will be unified to improve ease and availability for families and providers seeking state resources, including:

- The Early Childhood Block Grant at ISBE, which funds Preschool for All and the Prevention Initiative programs
- The Child Care Assistance Program, Home-Visiting programs, Head Start, and Early Intervention services at DHS
- Day care licensing currently managed by DCFS.

The Act contains a partial exemption to the Illinois Procurement Code allowing IDEC to expedite the purchase of required products and services when IDEC makes a good faith determination that, to implement the mandates of the Act, it is necessary and appropriate to enter a contract on an accelerated basis. Contracts that may be entered under the exemption include:

> "… those necessary to design and build integrated, operational systems of programs and services. The procurements may include, but are not limited to, those necessary to align and update program standards, integrate funding systems, design and establish data and reporting systems, align and update models for technical assistance and professional development, design systems to manage grants and ensure compliance, design and implement management and operational structures, and establish new means of engaging with families, educators, providers, and stakeholders…." 30 ILCS 500/1-10(b)(25).

Due to the impending transition of early childhood services from the transferring agencies to IDEC on July 1, 2026, IDEC has determined it is necessary to design and build an integrated, operational system for programs and services, in order to: align and update program standards, integrate funding systems, design and establish user-friendly data and reporting systems, align and update models for technical assistance and professional development, and establish new means of engaging with families, educators, providers, and stakeholders. For these reasons, IDEC has made a good faith determination that it is necessary and appropriate to enter a contract for an IDEC

Data & Analytics Hub on an expedited basis under the exemption provided in 30 ILCS 500/1-10(b)(25). However, the selection process will be conducted in a manner substantially in accordance with the requirements of Article 50 (ethics) and Sections 5-5 (Procurement Policy Board), 5-7 (Commission on Equity and Inclusion), 20-80 (contract files), 20-120 (subcontractors), 20-155 (paperwork), 20-160 (ethics/campaign contribution prohibitions), 25-60 (prevailing wage), and 25-90 (prohibited and authorized cybersecurity) of the Procurement Code. Illinois General Assembly - FullText Illinois Procurement Code.

2 Process Overview

To support transparency and ease of participation, the following table outlines the key milestones and sequence of activities for this Request for Innovative Solutions (RFIS). This summary includes important dates, submission instructions, and the overall process from initial questions through to vendor selection and project launch. Participants are encouraged to review this timeline carefully and plan accordingly. This is an exploratory RFIS which may lead to an invitation to a vendor to negotiate a contract for a Data and Analytics Hub. This RFIS does not constitute a solicitation as defined in the Illinois Procurement Code and does not commit IDEC to contract with any vendor.

This service will be contracted in phases, with the first phase of delivery occurring between March through June of 2026 and a second phase occurring beginning in the summer or early fall of 2026 (separate contract). This RFIS is intended to identify potential vendors to provide the services and is intended to cover the first phase of the project. It is not known if a RFIS will be conducted for the second phase; depending on performance, proposal alignment to needs, price, and internal factors, a different vendor may be contracted for the second phase. This RFIS is intended to determine potential solutions and vendors for the first delivery phase and to then engage in contract negotiations for the required services with the vendor most aligned to the needs of IDEC.

Milestone	Date	Details
RFIS Issued	November 17, 2025	Request for Innovative Solutions released by IDEC
Deadline for Questions	November 26, 2025	Submit questions by 12:00 p.m. Central Time to: DEC.procurement@illinois.gov
Responses to Questions Posted	December 3, 2025	IDEC posts responses to questions on its website

RFIS Response Due	December 10, 2025	Submit RFIS response by 12:00 p.m. Central Time to: DEC.procurement@illinois.gov
Review of Submissions Completed	December 19, 2025	IDEC completes review of all responses
Interviews / Presentations	January 5-7, 2026	Selected participants invited to present
Finalists Selected	January 9, 2026	Finalists notified and asked to submit pricing
Pricing Due	January 14, 2026	Finalists submit pricing proposals
Vendor Selected	January 23, 2026	If a solution/vendor is identified, IDEC finalizes vendor selection and begins contract discussions
Contract Negotiations Finalized	Mid-February, 2026	If agreement is reached, contract terms finalized
Onboarding Activities Begin	Late February 2026	Early onboarding, background checks, and planning activities
Project Start Date	Early March, 2026	Stage 1 of IDEC Data & Analytics Hub implementation begins

3 PURPOSE AND AUTHORITY

Pursuant to Public Act 103-0594 and 30 ILCS 500/1-10(b)(25), IDEC may enter contracts necessary to design and build integrated, operational systems of programs and services under an accelerated schedule. To inform such an expedited procurement, IDEC is issuing this Request for Innovative Solutions (RFIS) to obtain industry input and identify qualified solution partners capable of rapidly and cost-effectively building out the IDEC Data & Analytics Hub. This process is not a solicitation conducted pursuant to the Illinois Procurement Code; however, it will be carried out in a manner consistent with applicable ethical, transparency, and oversight provisions of the Code and will be used to help select a vendor to provide a state-of-the-art solution for the requested services. This is an exploratory RFIS which may lead to an invitation to a vendor to negotiate a contract for a Data and Analytics Hub. This RFIS does not commit IDEC to contract with any vendor.

a. Any vendor proposed solution for the IDEC Data & Analytics Hub must, at a minimum:

i. Be fully compliant with applicable **state and federal requirements** (Appendix E);

ii. Integrate with the **existing infrastructure** managed by the Illinois Department of Innovation and Technology (DoIT); and

iii. Support a phased implementation approach, with Stage 1 (March –June 2026) focused on establishing core architecture, initiating data governance, ingesting all required data sources, and enabling two-way data exchange with two critical applications.

b. This RFIS invites participants to submit the following:

i. **Non-price information** about the participant's knowledge of and experience with building **cloud-based data platforms** using **Microsoft Azure Commercial Cloud**, including:

- Data lake house architecture (e.g., Medallion model: Bronze, Silver, Gold)
- Secure, auditable data ingestion and transformation pipelines
- Governance, metadata management, and compliance frameworks

ii. An outline of how your organization would approach delivering the scope detailed in this document, including:

- Team structure and key roles
- Experience in early childhood, education or related human services field
- Proposed phases and timeframes for implementation
- Anticipated risks and mitigation strategies
- Key assumptions about IDEC readiness or contributions
- Any additional innovative ideas or value-added services

c. Procedural Details

IDEC will invite participants who it determines demonstrate an understanding and expertise with setting up Data Lakehouse and Analytics systems to engage in discussions that may result in a contracting opportunity for setting up the IDEC Data & Analytics Hub. Not all participants who submit a response to the RFIS will be invited to engage in additional discussions and the determination of participants to invite to discuss a solution is solely within the province of IDEC and not subject to protest or review.

The State of Illinois does not pay for any information provided in this RFIS, nor is it liable for any cost incurred by the participant. Participants are invited to provide non-proprietary, non-price information within the RFIS's scope. In addition to the specific information requested, participants may provide general information about industry trends and innovations, products, services or industry best practices that are not specifically tailored to meet the need. All information received through this RFIS will be available for public review and may be shared with interested stakeholders and consumer groups.

IDEC will answer questions about this RFIS. All questions should be submitted to DEC.procurement@illinois.gov according to the schedule in Section 2. Do not discuss this RFIS, directly or indirectly, with any other State official or employee. Potential participants who do not comply with this requirement will not be eligible to participate in future discussions with IDEC on the topic. Please see 30 ILCS 500/50-39 and 2 Ill. Admin. Code 1620.825.

A response to the RFIS is due by participants according to the schedule in Section 2. Participants who are invited to engage in further discussions with IDEC about potential contracting opportunities will occur according to the schedule in Section 2.

4 Overview

a. Context

IDEC has begun receiving millions of records from three transferring agencies across 60+ distinct data sources into a single DoIT-hosted Azure commercial cloud environment that was initially designed to operate at a smaller scale. The current need is to upscale and optimize this environment to support full-scale data migration and integration with new and existing technologies, ensure secure and auditable data flows, and establish a master data management and governance structure. Data acquisition, initial staging / ingestion and preparedness for data integration are already underway. The vendor proposed solution will accelerate and scale those initiative efforts to support IDEC's "Day 1" readiness in July 2026, along with additional advances in analytics, user experience, and application design in the years that follow.

b. Objectives

- Scale Azure-based infrastructure to support required levels of secure, compliant, and performant data ingestion, storage, and processing.
- Establish governance, role-based access control, and monitoring mechanisms.
- Enable batch and real-time data interfaces with data lifecycle management.

15 In-Scope Activities

c. Infrastructure & Storage

- Expand Azure environment from ~21 GB to ~500 GB with data lifecycle management.
- Recommend improvements to a landing zone already in place for inbound data by agency and category (70+ unique sources).

d. Data Ingestion & Processing

- Design a scalable and modular ingestion architecture compatible with State target data lake.
- Establish secure, monitored pipelines (one-time + ongoing) to ingest, apply transformation, normalization, and aggregation data set, as required.
- Support batch interfaces (initially via SFTP, but the vendor should recommend improved processes here; some applications will require near real-time ingestion pipelines).

- Configure and deploy ingestion pipelines to extract data from multiple source systems into the data lake.
- Enable Azure Data Factory (ADF) orchestration by building and scheduling end-to-end data pipelines to automate the flow from ingestion through transformation to outbound delivery.
- Outbound Data Distribution Configuration of secure data delivery mechanisms to third-party systems via:
  - SFTP (e.g., scheduled file drops with encryption),
  - Direct data connections (e.g., JDBC/ODBC to external databases),
  - APIs (e.g., RESTful endpoints or webhooks).
- Design and implement an efficient (cost effective) event-driven data architecture leveraging for near-time data flow.
- Establish data validation and error-handling mechanisms.
- Establish error-handling alert automation.

e. Security & Access

- Work with State to Configure identity and access management to implement granular Role-Based Access Control (RBAC) for:
  - 15–30 external users
  - 5–10 internal users
- If service accounts are needed, they should be configured for least privilege.
- Document all security controls and access requirements.
- Secure data outflows to comply with State Information Security requirements.
- Establish Key Vaults and Secrets as needed.
- Provide written Security processes for data governance or data quality agents that are required for installation on sources data sets that ensure no data is exposed.
- Use Azure Private Links, Managed VNets, and FIPS 140-3 Level 2 encryption.

f. Monitoring & Compliance

- Configure monitoring, auditing, and alerting (e.g., Azure Monitor, Log Analytics).
- Implement audit logging and data retention policies.
- Activate Microsoft Purview for data governance, lineage, and compliance.
- Set up monitoring dashboards and alerts for ingestion pipeline health and performance or SQL Server views/reports for sync status monitoring. Configure SQL Server alerts for job failures. Implement performance monitoring for long running processes.
- Enable logging for traceability and troubleshooting.

g. Architecture & Environments

- Implement a Medallion Architecture (Bronze, Silver, Gold layers).
- Stand up Development, QA, and Production environments.
- Configure API Management Service and build up to 5-10 API and database connections.
  - Develop REST API endpoints for external system access.
  - Implement Enterprise standards for authentication and authorization.
  - Create integration error handling and logging. Make operation table available to collect errors in production.

h. Data Quality & Validation

- Create validation rules to ensure no data loss.
- Implement standardization, validation, and transformation rules in accordance with industry best practices and early childhood user needs.
- Build and test alerting for pipeline failures and data load summaries.
  - Conduct unit, integration, and performance testing of ingestion pipelines.
  - Document and perform end-to-end testing of data flows, including data integrity checks and delivery confirmation to third parties.
  - Validate transformation logic against expected business outcomes.
  - Validate data completeness, accuracy, and timeliness post-ingestion.

i. Analytics & Visualization

- Implement Power BI Premium for interactive operational dashboards and reports from semantic data sets.
- Build 10 dashboards with varying complexity, where public-facing dashboards only feed from aggregated containerized data. Requirements to be provided by IDEC for the contents and business objectives of the dashboards. Vendor to propose an approach for building fit-for-purpose dashboards and setting up standard designs for growing the dashboard over time.
- Create a semantic data model secured with granular security enforced by role.

5 Out-of-Scope Activities

- Real-time streaming ingestion (e.g., Event Hubs, Kafka) unless added later.
- Complex analytics/reporting dashboards beyond initial setup.
- Extensive data transformation or enrichment beyond validation.
- End-user application development (e.g., portals).
- Agency onboarding/training (except data access and technical integration guidance).

- Custom AI/ML model development or content extraction.

6 Assumptions

- Some initial data is batch-based; transferring agencies and application vendors will use agreed protocols (SFTP, API) and other initial data will more real-time, automated integrations.
- Data structures are stable with minor variations.
- No public or citizen access is expected.
- Azure subscription and basic services are pre-established.
- Third-party vendors and users not authorized by IDEC will not have direct data access.
- The State will provide internal resources to support the implementation, including strategic data and technology leadership, data engineering capacity, information security, project management, business analysis, and cloud operations support for setting up the base applications, infrastructure, and firewalls.
- Data may include 2.3M PDFs; only metadata will be used for identification.
- The State's legal and security teams will provide timely guidance.
- IDEC will be responsible for the procurement of required licenses and contracts for applications and cloud infrastructure.

7 Proposed Solution Requirements

- Implement Azure SQL Hyperscale and Microsoft Purview.
- Design a simple, yet efficient, scalable, and documented Modern Cloud Data Lakehouse.
- The Phase 1 build should include some parallel discovery and business analysis by the vendor to develop more specific requirements for the Phase 2 part of the solution.
- Ensure anything implemented in Phase 1 has proper documentation and includes documentation and handoffs if needed between phase 1 and phase 2.
- Based on more specific requirements developed in Phase 1, a separate contract would be designed for the building and configuring of:
  a. Ingestion/transformation processes.
  b. Batch processing controls.
  c. Business and Gold layer notebooks.
  d. Endpoints for downstream integrations.
  e. Configure SSO for multiple identity providers.
  f. Configure Power BI with a semantic model and dashboard design.

8 Additional Requirements

a. Additional Technical Considerations and Requirements

The following requirements are ones that would be helpful for the overall design and implementation strategy but are not the highest priority when it comes to meeting timeline and budgetary considerations, particularly for Phase 1 of this project.

1. Additional Data Ingestion & Processing Requirements
   a. Ensure ingestion supports various formats (e.g., JSON, CSV, XML, relational data) and handles schema drift where applicable.
   b. Implement connectors and adapters for each source system.
   c. Design and implement transformation logic to cleanse, enrich, and normalize ingested data according to business rules.
   d. Develop reusable transformation components to support multiple data use cases and formats.
   e. Ensure data is formatted and packaged according to third-party specifications.
   f. Use tiered storage (Hot → Cool → Archive) for cost efficiency.
2. Additional Event-Driven Architecture Requirements

   a. Design Change Data Capture and tracking approach
   b. Define polling intervals and batch processing strategies
   c. Configure Event Grid to receive data from specified source systems and trigger downstream processing. If using MS SQL, create Agent Job configurations to create polling jobs for change detection, implement incremental change logic, and create filtering logic for relevant data changes.
   d. Enable Change Data Capture on target databases and tables, configure retention policies, and implement clean up jobs for change tracking tables. If using an Azure approach, develop Azure Functions to handle event triggers, perform data retrieval, and apply necessary transformations.
   e. Azure Functions (if using):
      i. Implement publish/subscribe mechanisms to route transformed data to designated external systems or consumers.
      ii. Ensure secure, scalable, and fault-tolerant integration across all components of the event pipeline.
      iii. Develop consumption tier functions for external integrations.
      iv. Implement retry policies and circuit breakers
      v. Configure Function app settings and connection strings, to be also present in an operational table to later monitoring.
   f. If recommending a SQL Server model
      i. Develop and document transformation and mapping logic for data processing.
      ii. Implement conflict detection and resolution procedures.
      iii. Develop formal reconciliation reports for sync accuracy to be stored in an ACID compliant database for audit traceability.
   g. Provide documentation and operational runbooks for the event-driven architecture, including trigger logic, transformation rules, and delivery endpoints.
   h. Document Error Handling and retry logic.
   i. Define monitoring and Alerting thresholds.
3. Additional Analytics and Visualization Requirements
   a. Enable data literacy effort for IDEC personnel to enable self-service analytics in Power BI Premium.

b. Collaboration with State Personnel

The selected vendor will be expected to work closely with the State's infrastructure team, including personnel from both IDEC and DoIT, throughout the project. DoIT will retain responsibility for provisioning and securing the core Azure environment, while the Vendor will focus on configuring and managing the data platform components according to IDEC user requirements.

Key expectations include:

- **Cloud Environment**: DoIT will continue to provision the Azure Commercial Cloud environment using Terraform but may need assistance developing the necessary infrastructure as code. Manual setup is not permitted.
- **Networking**: ExpressRoute is already in place. DoIT team will manage network design, routing, and secure entry/exit points.
- **Azure Services**: DoIT will deploy base instances of services (e.g., Azure Data Factory, SQL, PowerBI). The vendor will configure data flows, access controls, and analytics.
- **Microsoft Purview**: The vendor will set-up IDEC's data catalog within the existing statewide Purview instance. DoIT will not configure or manage Purview for this project.

The following requirements will only be partially met in phase 1 of the project, but should be considered in the scoping for phase 1:

c. Medallion Architecture

- **Bronze Layer**: Raw data capture with validation for loss.
- **Silver Layer**: Cleansing and transformation rules linked to data owners.
- **Gold Layer**: Enriched data with endorsement and advanced transformations.

d. Testing & Alerting

- Create test processes for each layer.
- Implement alerting for pipeline failures.

e. Documentation

- Environment configuration management and monitoring
- Metadata, dynamic SQL, and integration documentation.
- Monitoring, orchestration, and API usage.
- Deliver comprehensive documentation covering pipeline architecture, transformation logic, and delivery configurations.
- Security, access control, and change management.
- Power BI design and modification procedures.
- Version control and notebook standards.

9 STAGED APPROACH FOR PHASE 1

IDEC expects all proposals to follow a **staged implementation approach** that delivers measurable value and critical capabilities at each milestone. The approach should be structured to allow for incremental wins, risk mitigation, and continuous alignment with IDEC's evolving needs.

a. Phase 1 - Stage 1: Onboarding, Planning, and Kickoff (March - Mid-April 2026)

This initial stage is essential to ensure the vendor is fully oriented, aligned with IDEC's goals, and integrated into the broader project ecosystem. The vendor will work closely with IDEC, DoIT staff, and Clarity Partners to understand the existing environment, avoid duplication of efforts, and establish a collaborative foundation for success.

Key Activities:

- **Onboarding**
    - Complete background checks, set-up virtual machines, provide system access, and other onboarding activities
- **Knowledge Transfer**
    - Review existing architecture, documentation, and in-progress work
        - Provide detailed documentation of ingestion architecture, pipelines, and operational procedures.
    - Participate in technical walkthroughs with DoIT staff and Clarity Partners
    - Understand Terraform-based provisioning and Azure data lake and IAM network setup
    - Conduct knowledge transfer sessions with State teams.
- **Stakeholder Alignment**
    - Define roles, responsibilities, and communication protocols
    - Establish governance and decision-making structures
- **Project Planning**
    - Finalize detailed project plan, timeline, and deliverables for Stage 2 (under the management of the IDEC Data Project Manager, who will manage this project)
    - Identify dependencies, risks, and mitigation strategies
    - Confirm resource availability and team onboarding
    - Provide regular status sessions and risk assessments in writing
    - Leverage official State project reporting tools to make progress visible.

Deliverables:

These deliverables will be done by the IDEC Data PM, but the vendor will contribute to the following:

- Onboarding and orientation documentation
- Finalized project plan and timeline
- Risk register and mitigation plan
- Stakeholder engagement and communication plan

b. Phase 1 - Stage 2: Foundation & Critical Capabilities (April - June 2026)

This foundational phase will operate under **strict budget constraints** and must focus on establishing the foundational architecture and delivering the following key outcomes:

- **Core Architecture Setup**: Under the direction of IDEC and the DoIT Enterprise Cloud Operations, Data and Architecture Teams, deploy essential components of the Azure-based data platform, including storage, networking, identity management, and security configurations.

- **Data Governance Initiation**: Under the direction of IDEC and the DoIT Enterprise Data Team, implement the minimum viable governance framework, including metadata management, lineage tracking, and access control policies.

- **Data Ingestion**: Under the direction of IDEC and the DoIT Cloud Operations, and in collaboration with Clarity Partners, successfully ingest all required data sources from external agencies, ensuring secure, auditable, and validated pipelines.

- **Two-Way Integration**: Under the direction of IDEC and the DoIT Enterprise Data, Cloud Operations, and Information Security Teams, and collaboration with Vendor and IDEC application implementation teams, establish and validate **bi-directional data exchange** (Event Driven Architecture described above) between the data hub and **two critical applications**, enabling operational use of the ingested data.

- **Monitoring & Compliance**: Under the direction of IDEC and the DoIT Cloud Operations team, set up basic monitoring, alerting, and audit logging to ensure visibility and compliance from day one.

This stage must be designed to **de-risk future phases** by validating core assumptions, demonstrating early value, and enabling stakeholder confidence.

11 Future Phases

Subsequent phases will be defined and proposed by the responding vendors based on their understanding of IDEC's long-term goals. These phases should build upon the foundation established in Stage 1 and may include:

- Expansion of real-time data capabilities, to include master data management for sites, guardians, and providers
- Advanced analytics and reporting
- Broader application integrations
- Enhanced data quality and enrichment

Full-scale governance and compliance automation. Vendors are encouraged to propose a **logical, value-driven roadmap** that aligns with IDEC's strategic objectives and resource constraints.

12 Mandatory Requirements for Participants in RFIS Process

To ensure that only qualified and capable vendors are considered, IDEC requires that all participants in the RFIS process meet the following **mandatory qualifications**. These criteria are designed to ensure the selected Vendor can deliver a secure, scalable, and compliant Azure-based data platform that supports large-scale data ingestion, governance, and integration.

12.1 Organizational Qualifications

- The Participant must have experience working in early childhood, education or related human services field.
- The Participant must have been in continuous operation for a minimum of **five (5) years**.
- The Participant must have at least **five (5) years of experience** delivering **enterprise data management solutions**, including Azure-based cloud-based data ingestion, transformation, governance, and secure storage.
- The Participant must have experience implementing **data platform solutions** in a **public sector or government environment**, with a focus on compliance, security, and stakeholder coordination.
- The Participant must have successfully delivered at least **one (1) large-scale Azure cloud data platform implementation**, involving:

- Migration of multi-agency or multi-source data
- Secure, auditable data pipelines
- Role-based access control and identity integration
- Integration with downstream applications or services

12.2 Technical and Project Experience

- The Participant must have demonstrated experience designing and implementing solutions using **Microsoft Azure services**, including but not limited to:
    - Azure Data Factory
    - Azure SQL (including Hyperscale)
    - Azure Storage (Blob, tiered storage)
    - Azure Monitor and Log Analytics
    - Microsoft Purview
    - Microsoft Power BI Professional
- The Participant must have experience implementing **data governance frameworks**, including metadata management, lineage tracking, and data classification.
- The Participant must have experience establishing **secure data exchange mechanisms**, including SFTP, APIs, and private endpoints, in compliance with government security standards.

12.3 Key Staff Qualifications

- The Participant's **Key Staff**, collectively across all roles and project phases, must have experience leading and managing **large-scale technology implementations**, where "large-scale" is defined as a project with a **minimum budget of $500,000**.

- The Participant's Key Staff must demonstrate expertise in:
    - Early Childhood, Education or related Human Services field
    - Cloud data architecture and orchestration
    - Data quality and validation frameworks
    - Power BI or equivalent visualization platforms
    - Agile or phased delivery methodologies

- Deploying and managing cloud resources using Infrastructure as code via Terraform

12.4 Subcontracting

- Subcontractors are allowed.
- A subcontractor is a person or entity that enters into a contractual agreement with a total value of $100,000 or more with a person or entity who has a contract pursuant to which the person or entity provides some or all the goods, services, real property, remuneration, or other monetary forms of consideration that are the subject of the primary State contract.
- All contracts with subcontractors where the annual value of the subcontract is greater than $50,000 will be required to include Illinois Standard Certifications completed by the subcontractor.
- The selected vendor will be required to identify subcontracts with an annual value of $100,000 or more that will be utilized in the performance of the contract, the names and addresses of the subcontractors, and a description of the work to be performed by each.
- If the annual value of any subcontracts is more than $100,000, the Vendor must provide to the State the Financial Disclosures and Conflicts of Interest for that subcontractor.

13 How to Respond to this RFIS

The responses to this RFIS should be submitted in the format described below.

13.1 Section 1: Please submit a Cover Page with:

a. Organization Name

b. Organization Address

c. Organization Representative/Point of Contact

d. Contact information for the organization representative

e. Affirmation or acknowledgment that Participant meets the mandatory requirements for RFIS responders

f. Affirmation or acknowledgment of requirements to meet Illinois Department of Innovation and Technology (DoIT) information technology requirements (see Appendix A-C)

g. Explanation of Proposed AI Use and relevant controls (Appendix D)

h. Appendix of additional information (if desired)

13.2 Section 2: Scope of information requested

This RFIS is intended to assist IDEC in better understanding the capabilities, approaches, and considerations involved in building, integrating, and maintaining an Azure **cloud-based data platform** that supports secure, auditable, and scalable ingestion of data from multiple external agencies, with robust governance and integration with downstream applications.

13.2.1 Industry Overview

Please provide a general overview of the early childhood, education and/ or related human services sectors in which your organization has experience operating, including but not limited to:

1. The problem statement(s) for the end user that data project solved
2. The types of **data platform and integration services** typically offered
3. The **types of clients or entities** commonly served (e.g., government, healthcare, education, etc.)

4. The **typical scale and capacity** of services delivered (e.g., volume of data handled, number of users supported, geographic reach)

13.2.2 Industry Pricing Structures

Please describe the **standard pricing models** used in your industry for services relevant to this initiative. This may include, but is not limited to:

- Initial platform setup and configuration
- Data migration and integration
- Identity and access management setup
- Ongoing platform maintenance and support
- Change requests and enhancements
- Optional services such as analytics, visualization, or AI/ML integration

Please do not include actual pricing—only describe the types of cost structures typically used.

13.2.3 Implementation Timeline Capabilities

Provide a descriptive statement of your organization's ability to implement **cloud-based data platform solutions** on an **expedited timeline**. Include any relevant examples of past projects where:

- A phased approach was used to deliver early wins
- Critical capabilities were delivered within a constrained timeframe
- Timelines were maintained despite complexity or scale

13.2.4 Experience Delivering Similar Solutions

Provide a brief statement demonstrating your organization's ability to deliver and implement **secure, scalable, and compliant data platform solutions**, particularly in public sector or multi-agency environments. In your response, please highlight:

- Relevant experience, certifications, and technical capabilities
- Program and quality management practices
- Whether the implementation was completed **on time and on budget**, prior to any change orders or amendments

13.2.5 Experience with Large-Scale Government Systems

Provide a brief statement identifying other **large, complex enterprise systems** your organization has implemented for **state or federal government clients**. In your response, please include:

- The nature and scope of the system(s)
- Whether the implementation was completed **on time and on budget**
- Any notable challenges and how they were addressed

13.2.6 Approach to Delivering the Scope

Please provide a high-level outline of how your organization would approach delivering the scope of work described in this RFIS. Your response should reflect a **phased implementation strategy** that prioritizes early wins and critical capabilities, particularly those outlined for **Stage 1 (March–June 2026)**.

Your outline should include:

- How your team would be structured to support this engagement
- Proposed phases and timeframes for implementation
- Key milestones and deliverables for each phase
- Anticipated risks and mitigation strategies
- How your approach ensures collaboration with IDEC and the DoIT infrastructure team
- Any additional ideas or innovations that would add value to the IDEC Data & Analytics Hub initiative

13.3 Section 3: Illinois Department of Innovation and Technology Requirements

Illinois Department of Innovation and Technology (DoIT) Requirements are attached as appendixes A-C. Any participant selected for further interviews must comply with all DoIT information technology requirements. Participant shall identify affirmatively their ability to meet these standards.

13.4 Section 4: Artificial Intelligence Policy

The DoIT AI Policy and IDEC contract language is attached as appendix D. Any participant selected for further interviews must comply with the AI Policy. Participant shall identify affirmatively their ability to comply with this Policy and shall complete the Vendor certification identifying how, if at all, the proposed solution uses Artificial Intelligence Systems.

13.5 Section 5: Procurement Code Requirements

While all of the provisions of the Procurement Code do not pertain to the selection of a Vendor for the IDEC Data & Analytics Hub, certain provisions of the Procurement Code are applicable including the requirements of Article 50 (ethics), Section 5-5 (Procurement Policy Board), Section 5-7 (Commission on Equity and Inclusion), Section 20-80 (contract files), Section 20-120 (subcontractors), Section 20-155 (paperwork), Section 20-160 (ethics/campaign contribution prohibitions), Section 25-60 (prevailing wage), and Section 25-90 (prohibited and authorized cybersecurity) of the Procurement Code. Illinois Procurement Code (30 ILCS 500). Participants shall identify affirmatively their ability to comply with these provisions of the Procurement Code and submit a business enterprise utilization plan prior to contract execution (appendix F).

14 Presentation/Discussion

a. Vendors may be contacted after receipt of information, to schedule a WebEx call to discuss IDEC's need for a Data Hub. IDEC will contact the individual listed as the point of contact. Vendors are not required to give a presentation, but all invited vendors will be given the opportunity. IDEC will engage vendors in discussion of the vendor's experience, knowledge of data lake house implementations, and presentation (if any). A maximum of one (1) hour will be allocated to each invited vendor. Vendors are not required to use the entire time, but all will be given the same time. Notification of this invitation will be emailed to the contact person listed in your response.

b. IDEC will try to accommodate the vendor's requested time slots, but time slots will be filled on a first-received basis to prevent partiality.

Illinois Department of Innovation and Technology (DoIT)
Information Technology Requirements and Additional IDEC Requirements

Appendix A:	Authority to Operate/ Authority to Connect Packet
Appendix B:	Cloud Hosted Security Requirements
Appendix C:	DoIT Standard Terms and Conditions
Appendix D:	DoIT AI Policy and IDEC AI Contract Language
Appendix E:	Federal and State Regulations That May Govern IDEC
Appendix F:	Business Enterprise Utilization Plan

Appendix A Authority to Operate/ Authority to Connect Packet

STATE OF ILLINOIS NIST and FISMA Compliance Document

Project Name:

Date:

Duration of Project:

Contractor/Business Associate Name:

Contractor/Business Associate Contact Information:

A. The departments and agencies within all branches of the Federal Government are required by Federal Information Security Modernization Act (FISMA) of 2014 to comply with OMB E-GOV guidance to provide information security for the information and information systems that support the operations and assets under their control. The Federal Office of Management and Budget (OMB) has published guidance for the executive branch in OMB Circulars A-123, Appendix D and A-130.

B. State of Illinois recognizes that FISMA compliance, effective information security management and continuous monitoring of information systems are paramount to the success of HFS IT systems. To establish an information security program in accordance with the FISMA, the Contractor must follow the National Institute for Standards and Technology (NIST) Guidelines of the NIST Risk Management Framework (RMF), as amended.

C. Requirements

a. The Contractor shall adhere to the following NIST and FISMA requirements.

i. The Contractor shall meet all NIST and FISMA requirements before the solution or projects approved for production.

ii. The Contractor shall define information system boundaries for authorization.

iii. The Contractor shall assess, review and evaluate the information systems to be implemented based upon security categorization in accordance with Federal Information Processing Standards (FIPS) Publication 199 Standards for Security Categorization of Federal Information and Information Systems. Additional guidance on defining the information type can be obtained from National Institute Technological Standards (NIST) SP 800-60.

iv. The Contractor shall select the baseline controls described in FIPS 200 and NIST SP 800-53 to develop a System Security Plan (SSP).

v. The Contractor shall meet security requirements regarding protecting the confidentiality, integrity, and availability of the system and the information processed, stored, and transmitted by the system.

vi. The Contractor shall perform continuous monitoring of the system in compliance with NIST SP 800-137.

b. Contractor shall provide the following System Security Plan (SSP).

D. The Contractor must develop a System Security Plan using the guidance from NIST Risk Management Framework (RMF) (NIST SP 800-18) to establish an information security program in accordance with the Federal Information Security Management Act (FISMA) and demonstrate compliance.

E. This SSP must be approved by the authorizing official within State of Illinois. The SSP must include but not limited to the following:

a. Description of how the system is to be compliant with all the Federal and State laws regarding the security and privacy of medical data and records, and of all protected health information (PHI), including:

i. The Code of Federal Regulations (at 45 CFR 95.621) which provides that State agencies are responsible for the security of all automated data processing systems involved in the administration of Department of Health and Human Services' programs, and which includes the establishment of a security plan that outlines how software and data security will be maintained. This section further requires that State agencies conduct a review and evaluation of physical and data security operating procedures and personnel practices on a biennial basis.

ii. The security and privacy standards contained in Pub. L. 104–191, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and adopted in 45 CFR Part 164, Subparts C and E, as follows: The security standards require that measures be taken to secure protected heath information that is transmitted or stored in electronic format. The privacy standards apply to protected health information that may be in electronic, oral, and paper form.

iii. The requirements in section 1902(a)(7) of the Social Security Act (the Act), as further interpreted in Federal regulations at 42 CFR 431.300 to 307.

iv. Description of the process Contractor will use to report security breach incidents (regardless of severity or loss of actual data) to State of Illinois within 4 hours.

b. Description of measures to secure data and software;

c. Description of how data is encrypted in transit and in storage;

d. Description of physical and equipment security measures;

e. Description of personnel security;

f. Description of software used for security;

g. Description of the user roles and the access capabilities of each role;

h. Description of how users are assigned certain roles;

i. Identification of the staff responsible for controlling the system security;

j. Description of contingency security procedures during a disaster recovery event;

k. Description of how the Contractor works with State of Illinois to conduct annual security review;

l. Password security

m. Audit trails for all data access;

n. Contractor will be responsible for all costs associated with Identify theft, resulting from security breach.

F. Security Risk Assessment. State of Illinois or an independent entity will perform a security control assessment. State of Illinois will provide the Contractor a copy of the approved security control assessment. Once the Contractor receives the approved assessment, the Contractor must then develop a Security Risk Assessment based on the applicable security controls. Guidance to conducting and documenting the Security Risk Assessment can be obtained in NIST SP 800-30.

G. Plan of Action and Milestones (POA&M). After State of Illinois reviews and approves the Security Risk Assessment, the Contractor should begin to develop a POA&M. The POA&M should be a living document that is based on the findings and recommendations of the security assessment report. The POA&M should describe the deficiencies in the security controls, address the residual risk and detail plans for remediation.

H. Authorization approval package.

a. After State of Illinois reviews and approves the POA&M, the Contractor must prepare a transmittal letter to request approval of the entire authorization package. The authorization package must include at a minimum the following documents.

i. Transmittal Letter

ii. Updated System Security Plan

iii. Security Assessment Plan (include the State of Illinois/independent security assessment)

iv. Security Assessment Report (include the State of Illinois/independent security assessment)

v. Security Risk Assessment

vi. Plan of Action and Milestones

vii. Supporting Documentation including but not limited to design documentation, "As Built" documentation, operational documentation, validation documentation, prior authorization documentation, and other artifacts associated with the implementation and monitoring of the security controls.

b. The authorizing official will determine the risk to the organizational operation and determine if the system is authorized to proceed. The authorizing official will deliver to the Contractor a letter of authorization specifying any limitations or restriction placed on the operation of the system. Additionally, this letter should establish end date for the security authorization.

c. If the authorizing official denies the authorization, State of Illinois will continue to work with the Contractor until an acceptable level of residual risk for the system is achieved. This work would include the continued remediation listed in the POA&M.

I. Life-Cycle Management. Contractor or Business Associate shall perform security system reviews and reauthorization of the system at the direction of State of Illinois. Contractor or Business Associate shall be responsible for meeting the following requirements:

a. Performing continuous monitoring of the security system. Contractor's continuous monitoring must include periodically selecting a subset of the baseline controls for assessment. Based on assessment of these controls, subsequent remediation actions must be identified and implemented. The ongoing remediation process should include updating key documents such as the SSP, SAR, and POA&M.

b. Prior to any system or environmental modifications, the Contractor must perform a security impact analysis. This must be included as a part of any change management or configuration management process. If the results of the modification indicate changes to security posture of the system, corrective actions should be initiated, and appropriate documents revised and updated. The updating of the documentation and continuous monitoring should provide near real-time risk management.

c. A monthly Security Status Report must be produced by the Contractor for State of Illinois. The Status Report should provide essential information regarding the security posture of the system as well as the effectiveness of the controls deployed. Ongoing monitoring activities should be detailed as well as ongoing remediation efforts to address know vulnerabilities. Additional guidance for the monitoring of system security can be obtained in NIST SP 800-137.

Appendix B: Cloud Hosted Security Requirements

State of Illinois Security Requirements:

1. Vendor will notify the State of Illinois' Chief Information Security Officer within 24 hours of knowledge of any information breach or other security incident which impacts State of Illinois data. Email notification must be sent to: DoIT.Security@illinois.gov with the subject line 'Breach Notification.' Vendor must provide an initial incident report within five (5) business days of the incident and a final incident report upon resolution. Reports must include a summary of the event, systems affected, root cause analysis, remediation steps, and any actions taken to prevent recurrence.
2. Vendor certifies it has undertaken independent third-party audit Statement on Standards for Attestation Engagements (SSAE-18) certifications and must provide the State of Illinois with a System Operation Controls report (SOC 2 type 2) at time of award and annually thereafter with applicable bridge/gap letter.
3. Vendor must engage with the State of Illinois' Third-Party Risk Management (TPRM) platform, currently ServiceNow, during onboarding and upon request for risk assessment and monitoring purposes. This engagement includes timely responses to questionnaires, document submissions, and other actions required to evaluate and manage vendor risk.
4. Vendor must ensure all hosted data pertinent to this contract shall remain located within the contiguous United States. No remote access to State of Illinois systems or data may occur from outside the United States without prior written authorization from the State.
5. Vendor must ensure encryption of State of Illinois data both at rest and in transit. This encryption must comply with encryption security controls as defined in the most current version of the Federal Information Processing Standard (FIPS) 140, using Advanced Encryption Standard (AES) encryption with a minimum key length of 256 bits. Vendor must provide proof of encryption. Vendor must provide the State of Illinois with the capabilities to manage encryption keys for data at rest. These capabilities must not rely on a proprietary format or platform that prevents interoperability, visibility, or control by the State.
6. Vendor must store data in a non-proprietary, readily accessible format, or Vendor must provide a solution, at no additional cost to the State of Illinois, to extract any State of Illinois data stored in Vendor's solution.
7. Vendor must only use State of Illinois data, for the purposes stated in this contract.
8. Vendor may not use any State of Illinois data in any non-production system or in any other system outside the application/service procured under this contract. Vendor is strictly prohibited from using State of Illinois data to train, fine-tune, or otherwise influence artificial intelligence or machine learning models, regardless of whether the data is anonymized or aggregated.

9. No replication of State of Illinois data to testing, development, sandbox, or non-production environments is permitted without prior written authorization from the State.
10. Vendor must provide a complete and current copy of all State of Illinois data, in a non-proprietary, structured, and machine-readable format (e.g., JSON, XML, or CSV), without delay upon request by the State. Vendor must ensure that all metadata and file integrity are preserved.
11. Vendor must provide a copy of all State of Illinois data (in a non-proprietary, structured, and machine-readable format such as JSON, XML, or CSV) to the State of Illinois prior to termination of contract. Vendor must assist in the secure transmission or migration of such data to an alternate State environment upon termination, at no additional cost to the State.
12. Vendor must ensure its system supports secure integration with the State of Illinois Identity and Access Management (IAM) platform, including ILogin or any successor service designated by the Department of Innovation & Technology, if credentialing is required for access to the system or its administrative functions. Integration shall apply to all interactive and administrative access and use industry-standard federated authentication protocols (e.g., SAML 2.0, OAuth 2.0, or OpenID Connect). Multifactor authentication (MFA) must be enforced for all privileged accounts. Vendor shall not create or maintain local user accounts for State personnel unless expressly authorized in writing by the State.
13. Vendor must provide a Software Bill of Materials (SBOM) for all products or services delivered under this contract. The SBOM must identify all components, including open source and commercial libraries, versions, licenses, and known vulnerabilities. SBOMs shall follow a recognized format (e.g., SPDX, CycloneDX, or SWID), include dependency trees, and align with NTIA minimum elements. The SBOM must be updated with each major release or upon request by the State of Illinois and made available to the State's designated vulnerability management repository.
14. Vendor must maintain a robust and reliable data backup system. Vendor must supply a description of backup methodology, and this methodology must meet defined Maximum Tolerable Downtime (MTD) and Return to Operations (RPO) requirements.
15. At the State's request, Vendor must provide a written disaster recovery methodology and provide documented proof of annual disaster recovery testing. Testing documentation must include the test scope, methods used, results, issues discovered, and remediation plans. Vendor must maintain records of these tests for a minimum of three (3) years and make them available to the State upon request.
16. Vendor must sanitize all media that contains or contained State of Illinois data using the most current revision of NIST Special Publication 800-88 (Guidelines for Media Sanitization). Vendor must certify in writing the sanitization method used, date and time of sanitization, and identification of the media sanitized. Certification must be signed by an authorized representative of the vendor.

17. Vendor must render all State of Illinois data hosted within its environment permanently inaccessible using crypto shredding or equivalent cryptographic sanitization methods approved by the State. Vendor must certify the successful completion of this process in writing and provide metadata or logs validating data destruction, upon request.
18. Vendor and/or its agents must not resell nor otherwise redistribute information gained from its access to the State of Illinois data.
19. Vendor must not engage in, nor permit its agents to engage in, the delivery, installation, or activation of adware, unauthorized software, or any form of marketing, telemetry, or user tracking features unless explicitly authorized in writing by the State of Illinois.
20. Vendor shall have a documented security incident policy and plan. Vendor must supply a copy at the request of the State of Illinois. Vendor must notify the State of any material changes to the plan within 30 days.
21. Vendor must comply with all United States Federal and State of Illinois laws, rules, and regulations. Vendor must cooperate fully with any federal or State audit or security review related to the systems, services, or data covered by this contract.
22. Vendor must comply with all the State of Illinois Enterprise Security Policies (https://doit.illinois.gov/initiatives/cybersecurity/policies.html).
23. Vendor program and project management personnel must ensure coordination of activities with the State of Illinois governance program. Vendor must comply with all policies, standards, and procedures defined by the State of Illinois Department of Innovation and Technology's Enterprise Portfolio Management Office.
24. When hosting or processing State of Illinois financial information, Vendor must provide an SSAE-18 SOC 1 Type 2 report annually, along with any applicable bridge or gap letters. Reports must cover the full audit period and describe controls relevant to financial data handling, segregation of duties, and fraud prevention. Reports must be provided upon contract award and annually thereafter.
25. Vendor must ensure that all information technology products, services, and digital content provided under this contract comply with the Illinois Information Technology Accessibility Act (30 ILCS 587) and the IITAA 2.0 Standards, which incorporate the Revised Section 508 Standards and the Web Content Accessibility Guidelines (WCAG) 2.1 Level AA. Accessibility compliance must be maintained throughout the system lifecycle, including during updates, upgrades, and new releases, and any material changes that affect accessibility must be remediated or mitigated in coordination with the State.

Security Appendix S1 – Minimum Logging Requirements

- Input validation failures (e.g., protocol violations, unacceptable encodings, invalid parameter names and values)
- Output validation failures (e.g., database record set mismatch, invalid data encoding)
- Authentication successes and failures
- Authorization (access control) failures
- Session management failures (e.g., cookie session identification value modification)
- Application errors and system events (e.g., syntax and runtime errors, connectivity problems, performance issues, third-party service error messages, file system errors, file upload virus detection, configuration changes)
- Application and related systems start-ups and shut downs, and logging initialization (starting, stopping, or pausing)
- Use of higher-risk functionality (e.g., network connections, addition or deletion of users, changes to privileges, assigning users to tokens, adding or deleting tokens, use of systems administrative privileges, access by application administrators, all actions by users with administrative privileges, access to payment cardholder data, use of data encrypting keys, key changes, creation and deletion of system-level objects, data import and export including screen-based reports, submission of user-generated content - especially file uploads)
- Legal and other opt-ins (e.g., permissions for mobile phone capabilities, terms of use, terms & conditions, personal data usage consent, permission to receive marketing communications)

Appendix C: State of Illinois Information Technology Standard Terms and Conditions

Microsoft Word - IT Standard Terms and Conditions v25.4.docx

Appendix D: DoIT AI Policy and AI Contract Language

Policy on the Acceptable and Responsible Use of Artificial Intelligence April 1, 2025

1. Vendor AI Use Certification

Pursuant to the State of Illinois Department of Innovation and Technology (DoIT) AI Policy (effective April 1, 2025), the Vendor must affirmatively certify whether an Artificial Intelligence (AI) System is utilized as part of any goods, services, or solutions offered under this contract. An AI System is defined as any software, system (physical or virtual, or application that uses AI in whole or part to perform tasks (examples include virtual meeting assistants, digital voice assistants, customer service chatbots, facial recognition software, and writing assistant services, among many types).

Vendor must check and certify one of the following statements:

☐ **NO,** Vendor certifies that no AI Systems, in whole or in part, are used, embedded, or included in any deliverable, product, or service provided under this contract.

☐ **YES,** Vendor certifies that AI Systems are used, embedded, or included in one or more deliverables, products, or services provided under this contract. Vendor shall provide a written disclosure describing:

- The nature and function of each AI capability;
- Whether the AI System will have access to or process State or Protected Data or any other data protected under law or regulations (including, but not limited to, HIPAA, PII, CJIS, etc.);
- Any third-party or proprietary AI components included in the Vendor's solution;
- How human oversight ("human-in-the-loop") is maintained;
- Bias mitigation and privacy controls in place.

This certification and disclosure shall become a material part of the contract. The State reserves the right to reject or prohibit any unauthorized AI use.

---

2. Prohibited Uses of AI

AI Systems used under this contract shall not:

- Spread false or misleading information, deceiver users, or manipulate public opinion;

- Make autonomous decisions without documented human oversight;
- Discriminate against protected classes or violate human rights;
- Access protected, sensitive, or confidential information without controls in place and prior written authorization from the Agency Head and 30-day notice to DoIT;
- Use State data to train, refine, or improve AI models without express written permission.

---

3. Use of State Data in AI Systems

Vendor shall not use, transmit, or process any State data — including operational, training, or telemetry data — for any AI-related purpose unless:

- Authorized in writing by the Agency Head;
- Advance written notice is provided to DoIT at least 30 calendar days prior to such use;
- The data remains within a private, segregated environment and is not incorporated into a public or commercial AI model.

---

4. Compliance and Remedies

Non-disclosure or misrepresentation of AI use constitutes a **material breach of contract**. The State reserves the right to terminate the agreement, seek damages, or pursue any other remedy allowed under Illinois law.

Appendix E: Federal and State Statutes That May Govern IDEC

Family Educational Rights and Privacy Act (20 U.S.C. §1232(g)) ("FERPA"),
Health Insurance Portability and Accountability Act, (42 U.S.C. §1320d-6) (HIPAA)
45 CFR Part 160, Part 162, and Part 164
Federal Information Security Management Act of 2002 (44 U.S.C. §3514) (FISMA)
Medicaid, 42 U.S.C. §1396a(a)(7), 42 C.F.R. 431.300-307
Temporary Assistance for Needy Families (TANF) (42 U.S.C. §602(a)(1)(A)(iv))
Supplemental Nutrition Assistance Program (SNAP) (7 U.S.C. §2020(e)(8)), 7 C.F.R. 272.1(c)
Public Assistance Programs, 45 C.F.R. 205.50
The Privacy Act of 1974 (5 U.S.C. §552a)
Alcoholism and Substance Abuse, 42 C.F.R. Part 2
Children's Online Privacy & Protection Act (15 U.S.C. § 6501-6506) ("COPPA")
Children's Internet Protection Act (47 U.S.C. § 254) ("CIPA")
Privacy Act of 1974 (5 U.S.C. § 552a)
Individuals with Disabilities Education Act (20 U.S.C. § 1400) ("IDEA"),
34 C.F.R. 303
Social Security Act (42 U.S.C. §§ 1320d-2 through 1320d-7)
Health Information Technology for Economic and Clinical Health Act, (HITECH)
Payment Card Industry Data Security Standard (PCI DSS)
Illinois Freedom of Information Act (5 ILCS 140) (FOIA)
Illinois Identity Protection Act (5 ILCS 179)
Substance Use Disorder Act (20 ILCS 301)
Data Processing Confidentiality Act (30 ILCS 585)
Illinois Information Technology Accessibility Act (30 ILCS 587)
Performance Evaluation Reform Act (105 ILCS 5/24A-1 *et seq.)* ("PERA)
Illinois School Student Records Act (105 ILCS 10) ("ISSRA"),
Student Online Personal Protection Act (105 ILCS 85)
Illinois Public Aid Code (305 ILCS 5/11-9)
89 Ill. Adm. Code Part 50, 89 Ill. Admin. Code 10.230
Early Intervention Services Act (325 ILCS 20)
Illinois Department of Early Childhood Act (325 ILCS 3)
Child Care Act of 1969 (225 ILCS 10)
Children's Privacy Protection and Parental Empowerment Act (325 ILCS 17/1)
Mental Health and Developmental Disabilities Code (405 ILCS 5)
Illinois Controlled Substance Act (720 ILCS 570/318)
Biometric Information Privacy Act, 740 ILCS 14/1 (BIPA)
Mental Health and Developmental Disabilities Confidentiality Act (740 ILCS 110)

Illinois Personal Information Protection Act (815 ILCS 530) (PIPA)

Appendix F: State of Illinois Business Enterprise Program for Minorities, Women, and Persons with Disabilities Utilization Plan

U-Plan V.25.1