



**STATE OF TENNESSEE
Administrative Office of the Courts**

REQUEST FOR INFORMATION

For

Tennessee Data Platform: Integration Hub and Data Repository

RFI #30227-00654

July 23, 2026

1. Statement of Purpose

The State of Tennessee, Administrative Office of the Courts (TN AOC), is undertaking a strategic initiative to modernize statewide court technology and data management. This Request for Information (RFI) is issued to gather market intelligence, industry input and systems integrator vendor capabilities regarding the design, implementation, and support services of an integrated statewide Data Platform. The envisioned Data Platform will consist of a robust Integration Hub, a Centralized Data Repository (TnDR), a web-based Data and Analytics Portal (TnPortal), and a Statewide Reporting and Analytics Solution (TnRAS), all hosted within a secure Microsoft Azure environment.

The purpose of this RFI is to inform the State's procurement strategy by identifying vendor's best practices, infrastructure and systems integrator capabilities, operational considerations, and support models necessary to deliver a scalable, extensible, and sustainable Data Platform. The TN AOC seeks to enable reliable integration of court data from multiple sources, provide secure and efficient access to centralized data, support advanced analytics and reporting, and ensure ongoing operational support and maintainability by AOC IT.

The State appreciates the input and participation of interested parties in this process, and values recommendations that address solution architecture, integration patterns, data governance, security and compliance, solution ownership, and operational independence for the TN AOC.

The State will only consider solutions that ensure all developed code, configurations, and intellectual property are exclusively owned by the State and are delivered in non-proprietary, maintainable formats, with no third-party vendor-owned or proprietary dependencies.

For the avoidance of doubt, TN AOC intends to procure all required software infrastructure licenses (including, but not limited to, the Integration Hub, Centralized Data Repository, and related Azure services) separately from this RFI process. Respondents should focus their input and recommendations on systems integration, implementation, and support services, and should not propose or assume the resale or provision of software licenses as part of their response.

2. Background

The Tennessee Judiciary is advancing a strategic modernization initiative to transform its fragmented, court-by-court data landscape into a unified, standardized statewide environment. Historically, court data has been dispersed across multiple legacy Case Management Systems (CMS), with integration solutions

managed independently by individual courts or jurisdictions. This fragmentation has resulted in inconsistent data standards, limited interoperability, and significant challenges for comprehensive statewide reporting, analytics, and long-term data governance.

To address these challenges, TN AOC is pursuing the adoption of a cloud-native Data Platform as a foundational component of its Target State Design. This Data Platform will directly support core statewide applications, including CMS and eFiling, and will enable unified, secure, and reliable management, access, provisioning, and exchange of court data across Tennessee's trial courts. The solution is expected to enhance data accessibility, transparency, and operational efficiency for authorized stakeholders.

The Data Platform will facilitate Tennessee's transition from disparate, locally managed court data systems to a scalable, compliant, and future-ready statewide infrastructure hosted in Microsoft Azure. The Data Platform will also support the State's multi-year rollout of a new statewide CMS and eFiling solution. This initiative will ensure interoperability, robust security, and data governance in accordance with State and Federal requirements, supporting the modernization and sustainability of Tennessee's judicial technology ecosystem.

In support of this vision, TN AOC seeks a systems integrator vendor with demonstrated experience in Data Platform implementation in judicial environments. The vendor will be expected to design, implement, and support the following components and services:

- Data Platform Components:
 - Integration Hub
 - TnDR
 - TnRAS (design in scope for vendor but development to be done by the State)
 - TnPortal (design in scope for vendor but development to be done by the State)
- Data Platform Services:
 - Access Court Data
 - Manage Court Data
 - Provision Court Data
 - Exchange Court Data
- Data Migration & Ongoing Data Feed Implementation Services

The TN AOC will retain responsibility for data governance, CMS validation, and stewardship of statewide reporting and analytics capabilities. The selected systems integrator vendor will architect and implement the core technical components, including integration pipelines, data transformation and mapping, and foundational cloud infrastructure necessary to implement the statewide Data Platform.

Please see **Appendix A: Solution Architecture Scope** for detailed technical expectations and **Appendix B: Scope of Systems Integrator Services** for detailed services-related expectations.

3. Desired Outcomes / Success Criteria

The State seeks systems integrator vendor input on approaches that would support the following outcomes for the future statewide court Data Platform:

- A secure, centralized data environment that improves consistency, accessibility, and usability of court data across jurisdictions.

- Standardized ingestion, transformation, and storage of data from multiple legacy Case Management Systems.
- Improved support for statewide reporting, analytics, and internal business intelligence development.
- A scalable architecture capable of onboarding additional court types, integrating with additional justice partners, and adapting to future modernization efforts, particularly the multi-year, phased rollout of the statewide CMS and eFiling solution.
- Compliance with CJIS, State security requirements, and sound audit, recovery, and access-control practices.
- A supportable operating model that allows the TN AOC to assume long-term administration and maintenance following implementation.
- All code, configurations, and intellectual property developed for the Data Platform must be owned by TN AOC. The Data Platform must be delivered in non-proprietary, maintainable formats (e.g., C#, .NET, open standards), and must not include any vendor-owned or proprietary solution components. This ensures the TN AOC can independently support, maintain, and enhance the Data Platform over its lifecycle.

For purposes of this RFI, the State is particularly interested in systems integrator vendor recommendations regarding practical implementation sequencing, key risks, dependencies, and the measures a future project should use to determine whether each phase has been successfully completed.

4. Estimated Scale and Volume

The State is seeking systems integrator vendor input on architecture and implementation approaches capable of supporting a statewide judicial Data Platform operating across multiple court systems, jurisdictions, and court types.

At a minimum, respondents should assume the future environment may involve:

- Data ingestion from 15+ legacy Case Management Systems.
- Integration across General Sessions, Criminal, Civil, Chancery, Probate, Juvenile, and other court domains as applicable.
- A phased implementation approach that begins with foundational infrastructure, proceeds through General Sessions onboarding, and then expands to broader Trial Court integration.
- High-volume concurrent ingestion from numerous jurisdictions, particularly during later implementation phases and statewide scaling activities.
- An eventual statewide footprint of approximately 400 courts across the full implementation lifecycle.

Because exact transaction volumes, record counts, interface frequency, and source-system readiness may vary, the State requests that respondents identify the scale, growth, and performance assumptions used in developing their recommendations, timelines, and rough-order-of-magnitude pricing.

5. Communications

1. Please submit your response to this RFI to:

Brandon Bowers, Chief Technology Officer
Tennessee Administrative Office of the Courts
511 Union Street, Suite 600
Nashville, TN 37219

615-741-2687

[Brandon L Bowers@tncourts.gov](mailto:Brandon_L_Bowers@tncourts.gov)

2. Please feel free to contact the Tennessee Administrative Office of the Courts with any questions regarding this RFI. The main point of contact will be Brandon Bowers, Chief Technology Officer.
3. Please reference the RFI Number with all communications related to this RFI.

6. RFI Schedule of Events

All times listed below are in Central Time, and all dates are State business days.

Event	Time	Date
1. RFI Issued		7/23/26
2. Written Questions and Comments Deadline	10:00 AM	7/30/26
3. State Response to Written Questions	5:00 PM	8/6/26
4. RFI Response Deadline	10:00 AM	8/20/26
5. Conduct Vendor Demo Presentation (Optional)	TBD	TBD

The State reserves the right to revise this schedule at its discretion.

7. General Information

1. Respondents must have successful implementations of large-scale Data Platform and integration for justice or court agencies' data.
2. Responding to this RFI will not create any contract rights. Responses to this RFI will become property of the State.
3. The State may use the information received through this RFI to support strategy development, budgeting, and procurement next steps.
4. The RFI responses will not be released while the State is reviewing responses and considering alternatives.
5. All official responses to written questions, the questions and answers log, and any additional notices or updates related to this RFI will be posted at the following website: <https://tncourts.gov/tennessee-statewide-court-information-systems-technology-solution>
6. The State will not pay for any costs associated with responding to this RFI.
7. Respondents are encouraged to keep responses concise while providing enough detail to respond comprehensively to the questions included in this RFI.
8. Respondents may include attachments, diagrams, sample artifacts, or supplemental materials if such materials help clarify the response.

9. Any assumptions, exclusions, or exceptions that materially affect a respondent's feedback should be clearly identified.
10. The State may, at its discretion, seek written clarifications, conduct follow-up discussions, or request demonstrations or presentations.

8. Informational Forms

The State is requesting the following information from all interested parties. Please complete the following forms.

RFI Number: 30227-00654

TECHNICAL INFORMATIONAL FORM

8.1. Respondent Legal Entity Name

Vendor Response	
------------------------	--

8.2. Respondent Contact Person

Field	Vendor Response
Name	
Title	
Address	
Phone Number	
Email	

8.3. Requested General Information

Category 1: Corporate Experience & Cloud Pedigree

A. Brief Description of Experience Providing Similar Scope of Services

Please demonstrate that your organization has successful implementations of large-scale data platform and integration for justice or court agencies' data.

Please also describe your experience providing statewide or large-scale data integrations, particularly within judicial, criminal justice, public safety, or other complex government environments. Include experience in extracting, migrating, standardizing, and managing data across multiple legacy court Case Management Systems and jurisdictions. Additionally, include your experience using court-relevant standards (e.g., NIEM, ECF) in the exchange of justice data.

Vendor Response	
------------------------	--

B. Microsoft Azure and Similar Experience

Describe your experience serving as a Microsoft Certified Partner, if applicable, and summarize your experience designing and deploying cloud-native integration hubs, enterprise data platforms, or centralized data repositories in Microsoft Azure.

Vendor Response	
------------------------	--

Category 2: Technical Architecture & Data Strategy

C. Recommended Azure Services and Architecture

Identify the Azure-native services you would typically recommend for a statewide Integration Hub and Data Repository of this scale, and explain the reasoning, tradeoffs, and major risks associated with your preferred approach.

Vendor Response	
------------------------	--

D. Data Segregation Strategy

Explain your recommended data management strategy for organizing and securing data across different court types (e.g., General Sessions/Chancery) and jurisdictions (e.g., County 1/ County 2), including whether you would favor separate physical data marts, a shared logical model, semantic-layer segmentation, or other approaches. Include governance and performance considerations.

Vendor Response	
------------------------	--

E. Data Mapping and Transformation Logic

Describe your approach to ETL or ELT transformation logic when a legacy CMS vendor cannot natively map exported data to the State's standard data taxonomy.

Explain your data mapping approach when documentation for the legacy source data is limited or unavailable.

Explain any alternative approaches you would consider for data mapping in addition to traditional manual field-by-field mapping.

Vendor Response	
------------------------	--

F. Data Quality, Error Handling, and Master Party Management

Explain how your integration approach would identify, log, isolate, and process malformed, inconsistent, duplicate, or incomplete records without halting ingestion. Include your approach to master party management or duplicate identity resolution across systems. Additionally, please detail if and how Artificial Intelligence (AI) or Machine Learning models will be utilized within these workflows to automate error detection, pattern recognition, or identity resolution.

Vendor Response	
------------------------	--

G. High-Volume Ingestion and Pipeline Performance

Describe how you would architect API- and SFTP-based ingestion pipelines to support high transaction volumes, manage rate limits, prevent bottlenecks, and maintain high availability during peak usage periods. Include any AI-driven mechanisms you might employ for predictive load balancing, anomaly detection, or automated performance tuning of the data pipelines.

Vendor Response	
------------------------	--

H. Transition from Batch to Event-Driven Processing

Explain how you would design the platform so it can evolve from legacy batch-based integration methods to near-real-time or event-driven exchanges in the future, without major rework.

Vendor Response	
------------------------	--

I. External Partner Exchanges

Describe how your architecture would support potential future bidirectional exchanges with external justice partners, including secure outbound and inbound data flows, routing, translation, and auditing. Please describe any AI applications your architecture could leverage to facilitate intelligent routing, automated data mapping/translation between different external standards, or anomalous behavior detection during these exchanges.

Vendor Response	
------------------------	--

Category 3: Security, Access, & Compliance

J. Security and Disaster Recovery

Describe how you would design the underlying data architecture to support internal TN AOC Power BI and similar tools and secure jurisdiction-based access, including row-level security and other access control considerations. Note if and how AI tools could be embedded within the data layer to assist internal staff with automated semantic layer generation, advanced reporting optimization, or dynamic access monitoring.

Vendor Response	
------------------------	--

K. Support for Internal TN AOC Reporting and Access Controls

Describe your approach to designing a secure data architecture that enforces jurisdiction-based access controls, including row-level security and other access control mechanisms. Please provide examples of how you have implemented such controls in environments requiring compliance with the FBI CJIS Security Policy. Additionally, describe your experience with maintaining compliance with CJIS background investigation and similar requirement for your firm's staff.

Vendor Response	
------------------------	--

Category 4: Implementation, Support, & Handover

L. Estimated Timeline by Phased Approach

Based on your experience, provide an estimated implementation timeline broken down by your phased approach, including likely dependencies, sequencing concerns, and key bottlenecks the State should consider. Following responses in the table below, develop a Gantt chart with estimated start dates and completion dates per activity phase.

This Phased approach must mirror what is quoted under section 8.3.2 ROM.

Appendix B Scope of Service Activity	Vendor Response
SI Project Management & Service Enabling	
Integration Hub Stand Up	
TnDR Stand Up & Schema Determination	
Data Platform Services Stand Up	
Data Migration & Ongoing Feeds to TnDR	
TnRAS — Statewide Reporting & Analytics	
TnPortal — Web-Based Data & Analytics Access	
Service Desk Support	
Post Implementation Support	

Optional: Deployment of an Agentic AI Engine for complex, multi-step querying and automated synthesis of statewide court data, enabling advanced, hands-off analytical reporting and natural language accessibility.	
--	--

Gantt Chart

Vendor Proposed Project Timeline	
---	--

M. Readiness Approval

What specific technical criteria would you recommend for an Approval Gate for exiting the initial General Session court deployment phase (i.e., to ensure that the Data Platform is ready to scale to Trial Courts)? Additionally, based on best practice, how would Readiness be measured and confirmed?

Vendor Response	
------------------------	--

N. Training, Hypercare, and Transition to State Support

Describe your recommended approach for training, knowledge transfer, operational handoff, and transition to State support, including a hypercare period for a project of this type.

How do you measure the success of knowledge transfer to ensure state administrators are fully self-sufficient post-implementation? Please define the specific Key Performance Indicators and metrics you recommend for evaluating operational readiness and the successful phasedown of systems integrator vendor support.

Vendor Response	
------------------------	--

Category 5: Innovation (Optional)

O. Optional AI-Enabled Query Capabilities

Provide your perspective on the maturity and security viability of optional AI-enabled natural language querying capabilities, such as Azure AI Foundry, for justice data environments. Include any prerequisites that should be in place before such functionality is considered.

Vendor Response	
------------------------	--

8.3. Requested Cost Information

Please note that pricing provided in response to this section is for planning and budgetary purposes only and does not constitute a binding bid.

8.3.1. Pricing Approach

Describe the fixed firm pricing structure you would consider for this implementation, given your experience with similar projects. Time and Materials is not considered by the State.

Vendor Response	
------------------------	--

8.3.2. Rough-Order-of-Magnitude (ROM) Pricing by Phase

Cost Category	Appendix B Scope of Service Activity	Vendor Response for ROM
Implementation Services	SI Project Management & Service Enabling	Est. \$
Implementation Services	Integration Hub Stand Up	Est. \$
Implementation Services	TnDR Stand Up & Schema Determination	Est. \$
Implementation Services	Data Platform Services Stand Up	Est. \$
Implementation Services	Data Migration & Ongoing Feeds to TnDR	Est. \$
Service - Recommendations	TnRAS — Statewide Reporting & Analytics	Est. \$
Service - Recommendations	TnPortal — Web-Based Data & Analytics Access	Est. \$
Implementation Services	Service Desk Support	Est. \$
Implementation Services	Post Implementation Support	Est. \$

Optional Capability	Optional AI-Enabled Query Capability / Agentic AI Deployment	Est. \$
Other Costs	Annual non-Azure costs, if any	Est. \$

8.3.3. Pricing Assumptions, Volume Assumptions, and Exclusions

Please identify any pricing assumptions, scale or volume assumptions, exclusions, licensing considerations, support model assumptions, or other factors that would materially affect cost estimates.

Vendor Response	
------------------------	--

8.4. Additional Considerations

Please provide input on alternative approaches or additional considerations that might benefit the State for this project. This may include suggested sequencing changes, key risks, market constraints, recommended evaluation considerations, or other information that would improve the project success.

Please also include any suggested alternatives to the approaches included in Appendix A and Appendix B.

Vendor Response	
------------------------	--

8.5 Performance Management Considerations

Please provide input on recommended approaches, metrics, or alternative strategies for performance management, including the establishment and monitoring of Service Level Agreements (SLAs) and Service Level Requirements (SLRs) as described in Appendix B, Section 10. The State welcomes suggestions for additional performance measures, reporting methods, or best practices that would help ensure accountability, continuous improvement, and the long-term success of the Data Platform implementation.

Vendor Response	
------------------------	--

APPENDIX A: Solution Architecture Scope

1. Solution Architecture Scope

The Solution Architecture Scope articulates the foundational architecture that will drive the design and implementation of the Data Platform—including the Integration Hub and TnDR. This modernization effort is designed to promote transparency, inclusivity, and efficiency in the administration of justice, ensuring that Tennessee’s general sessions, juvenile and trial courts can adapt to evolving judicial and technical needs while maintaining robust security, regulatory compliance, and effective data governance. By establishing a unified, standards-based architecture, the TN AOC will empower stakeholders statewide with consistent, reliable access to court data, support advanced analytics and interoperability, and lay the groundwork for sustainable innovation across the judicial branch.

1.1 Current State Environment

Tennessee's court technology landscape currently operates under a fragmented and federated model, where courts employ their own solutions and capabilities. In alignment with legislative goals, there is a concerted effort to unify the court’s data under a single, statewide solution that enhances data aggregation, data management, interoperability, analytics, and overall efficiency.

While the existing systems have served their purpose, the current technological environment presents an opportunity for enhancement to better support TN AOC's strategic vision. This vision includes implementing a cohesive statewide Data Platform that facilitates seamless data integration, storage, and supports data analytics for informed decision-making. By transitioning to a more unified approach, Tennessee aims to modernize its court technology data management infrastructure, ensuring it meets the evolving needs of the court system and its stakeholders.

Integration Hub Current State

Currently, the court technology landscape in Tennessee lacks a statewide Integration Hub to facilitate secure, standardized data exchange among court CMS, external agencies, and statewide applications. Data integrations are managed on a court-by-court basis, often relying on point-to-point connections, custom scripts, or manual processes. This results in complex, brittle integrations that are difficult to scale, maintain, and secure. There is no common sophisticated middleware orchestration layer or event-driven architecture to support near real-time or batch data flows between local legacy CMS, statewide applications (e.g., statewide reporting), or external partners (e.g., law enforcement, probation). The absence of a centralized Integration Hub hinders interoperability, increases operational risk, and complicates efforts to modernize the judicial technology ecosystem.

TnDR Current State

At present, Tennessee does not operate a centralized statewide data repository for court case-level operational and analytical purposes. Court data is stored and managed locally within individual legacy CMS solutions, resulting in fragmented data silos and inconsistent data standards across jurisdictions. There is no consistent unified mechanism for aggregating, validating, storing, archiving, or reporting statewide court data in a standard manner, which impedes comprehensive analytics, transparency, and cross-jurisdictional data sharing. Data extracts for statewide reporting are typically manual, ad hoc, timely, and subject to local variations in schema, quality, and completeness.

1.2 Future State Capabilities

In establishing the foundational infrastructure required for the Data Platform, the systems integrator vendor is required to create and implement a set of Data Platform Services which will allow the Data Platform to support TN AOC’s statewide court technology modernization goals. These services will underpin the operational and analytical needs of Tennessee’s courts by enabling integration across statewide eFiling, Case Management System, TnDR, TnRAS, and TnPortal applications.

The Data Platform Services will be implemented leveraging configurable, out-of-the-box features of the selected Data Platform tools, and will be architected, integrated, and validated by the systems integrator. Key capabilities include:

- Secure, scalable management of court data across jurisdictions.
- Near real-time and batch data ingestion, transformation, and storage in TnDR.
- Robust data exchange and interoperability via Integration Hub, supporting internal court systems and external justice partners.
- Comprehensive support for statewide reporting and analytics (TnRAS) and web-based data access (TnPortal).
- Enforcement of access controls, data privacy, and compliance with all relevant federal, state, and local regulations.
- The Systems integrator will ensure that the Data Platform and Data Platform Services are fully integrated with the statewide CMS, providing the foundation for a unified, transparent, and efficient court technology environment.

1.3 Target State Design

The Target State Design addresses current state gaps and challenges by presenting a unified, comprehensive court system technology solution architecture that supports TN AOC's strategic vision and goals. This design builds a foundation of capabilities, allowing Tennessee to grow and modernize further over time.

This design lists several foundational data management components that underpin the architectural landscape — specifically, TnDR, paired with an Integration Hub.

This creates a flexible, scalable data management environment for court technology, which:

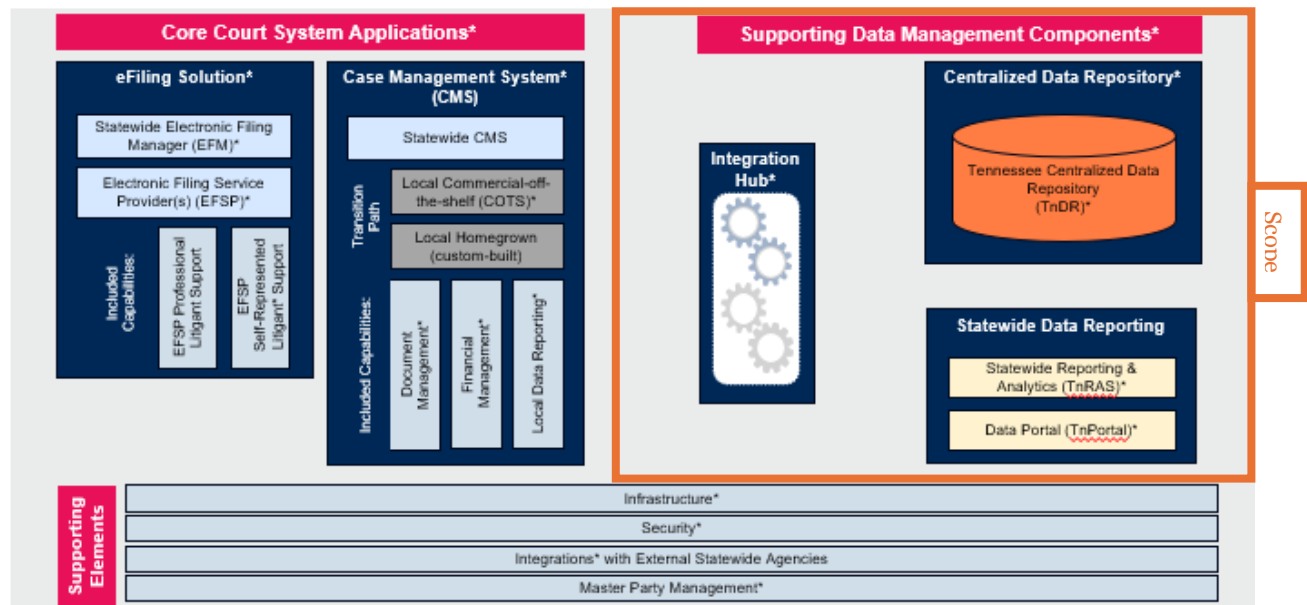
- I. Allows for the incremental replacement of legacy CMS while enabling TN AOC to realize benefits more quickly.
- II. Enables access to data from statewide CMS in a single, easily accessible Centralized Data Repository via the Integration Hub.
- III. Is scalable and designed to incorporate additional data elements for data-driven decision-making.
- IV. Facilitates efficient data exchange and isolates components to prevent disruptions in one system from affecting the entire court technology environment systems.
- V. Equips TN courts with improved reporting capabilities, allowing them to access and utilize local and statewide data for decision-making.

It is also important to note that the statewide CMS, Integration Hub, TnDR, TnRAS, and TnPortal will feature modular architecture and open APIs. This will enable local integrations to be executed either directly at the statewide CMS level (as determined by TN AOC only) or through the Integration Hub (preferred) to meet court-specific requirements and enhance system interoperability.

Finally, the statewide CMS is expected to contain its own database(s) capable of integrating seamlessly with the Integration Hub, feeding data to and from TnDR, ensuring efficient data exchange and synchronization across all courts while maintaining local data autonomy.

The following diagram outlines the target state design.

Figure 1: Target State Design for Court Technology Solution



1.4 State Responsibilities / Project Prerequisites

The following activities are expected to be completed by the State prior to primary implementation and are not anticipated to be systems integrator vendor deliverables.

Prerequisite	Description
Azure Procurement Readiness	Provision of Azure licensing, subscriptions, credits, or related items needed to support implementation startup.
Data Taxonomy Provision	Delivery of the State's finalized data taxonomy and standard definitions for use in design and mapping.
CMS Business Rules Definition	Provision of business rules and source-system expectations that define how CMS platforms are expected to transmit data to the Integration Hub.
Source System Readiness	Coordination with legacy courts and CMS vendors to support standardized exports (preferred) or other interface methods through API or SFTP methods.

2. Data Platform Scope Categories

The Data Platform Scope Categories define the key architectural and functional domains that will guide delivery of the Data Platform. These categories encompass the foundational cloud infrastructure, data integration and pipeline development, system testing and validation, transition and operational handover, and optional innovative capabilities. Together, they establish a comprehensive framework for implementing a secure, scalable, and future-ready statewide court Data Platform.

Category 1: Foundation & Cloud Infrastructure

- **Azure Environment Architecture Design:** Comprehensive documentation of the target Microsoft Azure infrastructure, including the foundational layout for the Integration Hub and centralized Data Repository.
- **Security & Access Implementation:** Configured identity and access management controls, integrating with Microsoft Entra ID for role-based security, alongside CJIS-aligned encryption protocols for data at rest and in transit.
- **Base Data Repository Deployment:** A fully deployed, foundational repository that is ready to begin receiving and harmonizing structured court data.

Category 2: Data Integration & Pipeline

- **Data Ingestion Interfaces:** Secure API and SFTP pipelines designed for data extraction from legacy Case Management Systems (CMS).
- **Transformation & Mapping Logic:** ETL/ELT pipelines that extract, validate, route, and map legacy source data against the State's finalized standard Data Taxonomy.
- **Error Handling & Party Management Systems:** Automated logging to identify, isolate, and process malformed or duplicate records without halting high-volume ingestion.

Category 3: System Testing & Validation

- **Performance & Load Testing Validation:** Documentation proving the Data Platform's capacity to maintain high availability and manage concurrent, high-volume ingestion and access from an eventual footprint of approximately 400 courts.
- **Phase Approval Gate Reports:** Documented fulfillment of predefined exit criteria metrics, specifically validating the success of the initial deployment to General Sessions courts before scaling to broader Trial Courts.

Category 4: Transition & Operational Handover

1. **Knowledge Transfer Documentation:** Comprehensive system administration, architecture, and maintenance manuals, along with a structured, hands-on and measurable knowledge transfer program to enable self-sufficient AOC ownership.
2. **Hypercare Support:** Dedicated support and issue resolution logging during the post-implementation transition period(s).

Category 5: Optional Innovative Capabilities

- **Agentic AI Engine Deployment:** Implementation and security configuration of an Azure AI Foundry component to enable natural language querying and automated synthesis of statewide data.

3. Data Platform Services

The following four tables outline the Data Platform Services, including a brief description of each. These services are to be designed and created by the Systems integrator as part of the project scope. These services provide the mechanisms by which data is exchanged between TnDR and the CMS and eFiling solution (both legacy and new statewide) solutions as well with other applications including but not limited to TnRAS, TnPortal and other interfacing systems at both the state and local levels.

Manage Court Data

Core Service	Service Description
Ingest Case Updates into TnDR	Receives near real-time case update messages (e.g., filings, dispositions) from the statewide CMS and applies changes to the central repository. Ensures update ordering, deduplication, and transactional integrity for each case update.
ETL Load Case Data into TnDR	Executes scheduled batch jobs to extract full or incremental data from the legacy and/or statewide CMS, transform to the TnDR schema, and load into the repository. Supports historical backloads and schema-driven mapping.
Manage Ingestion Exceptions	Detects, logs, and routes errors for both streaming and batch ingestion processes. Provides dashboards and alert workflows to resolve data format issues, connection failures, or schema mismatches.
Manage Master Party Records	Creates and updates consolidated “master party” records by matching and merging individual person and organization entities. Tracks lineage and supports de-merge operations.
Provide Person Match Suggestions to Statewide CMS	Exposes a matching service that returns potential duplicate parties when users create or modify records in the statewide CMS. Reduces duplicate entries by suggesting existing master IDs.
Manage Statewide Code & Reference Tables	Hosts and version-controls statewide lookup tables (e.g., charge codes, jurisdiction lists). Distributes point-in-time and current versions via APIs for downstream systems’ validation.

Access to Court Data

Core Service	Service Description
Apply Court Order Seal to Case Records in TnDR	Replicates seal status from the legacy and/or statewide CMS to TnDR when a court order is issued. The seal is initiated and managed in the legacy and/or statewide CMS, and TnDR replicates the access restriction by preventing sealed records from appearing in queries or reports unless the user has explicit permissions.
Apply Court Order Partial Seal to Case Records in TnDR	Replicates partial seal status from the legacy and/or statewide CMS to TnDR for specific case sections or attachments as ordered by the court. The partial seal is initiated in the legacy and/or statewide CMS, and TnDR replicates the access restriction to those specific sealed elements, ensuring compliance with the originating court order.
Redact Fields	Replicates field-level redaction status from the legacy and/or statewide CMS to TnDR. Redaction rules are initiated in the legacy and/or statewide CMS, and TnDR replicates the access restriction, ensuring that only authorized users can view redacted fields according to the originating system’s rules.

Restrict Data by Originating Jurisdiction	Enforces jurisdiction-based access controls within TnDR. Access rules are defined and managed in legacy and/or statewide CMS, and those rules are replicated in TnDR (e.g., restricting users to records from their own jurisdiction unless elevated privileges are granted). This includes special handling for sensitive data per jurisdictional policy.
--	--

Provision Court Data

Core Service	Service Description
Initial Bulk Load into TnDR	Executes one-time bulk extracts of existing legacy CMS data for new jurisdictions joining the centralized data repository. Includes data validation, reconciliation reports, and reconciliation support.
Initial Bulk Load of Historic Data from TnDR to New Statewide CMS	Executes a one-time, large-scale migration of select historic case, party, and hearing data from the TnDR into the new statewide CMS. This process includes data extraction, transformation to meet the statewide CMS schema requirements, validation for completeness and accuracy, and loading into the statewide CMS.
Provide Historic Case & Party Data to eFiling	Publishes read-only historic case and party snapshots via APIs to the eFiling portal. Enables attorneys and filers to access prior case context alongside new submissions.
Provides Data to Statewide Reporting (TnRAS)	Enables TnRAS to access case and party data directly from TnDR for statewide reporting purposes.
Provide Data Exports	Generates ad hoc or scheduled extracts of consolidated TnDR data. Supports CSV, JSON, and direct database replica options.

Exchange Court Data

Core Service	Service Description
Manage Exchanges: CMS ↔ TnDR Data	Provides data exchange between the legacy and/or statewide CMS and TnDR, including protocol translation, authentication, and end-to-end entity mapping. Includes monitoring and retry logic.
Manage Exchanges: CMS ↔ AOC Systems	Provides data exchange between the statewide CMS and other related AOC applications (e.g., fee payment), applying business rules and data transformations as defined by AOC integration policies.
Manage Exchanges: CMS ↔ External State Systems	Provides standardized data exchange interfaces with external agencies (e.g., law enforcement, driver services) via secure APIs or message queues. Enforces data contracts and audit logs per regulatory requirements.

Manage Exchanges: CMS ↔ Local Clerk System	Provides data exchange interfaces between the statewide CMS and local court systems (e.g., ADR, jury management), including event subscription and transformation capabilities.
Manage Exchanges: CMS ↔ Local Agency	Provides data exchange between the statewide CMS and county-level non-court agencies (e.g., probation, juvenile services), applying consent and jurisdiction rules.
Manage Exchanges: Local Legacy CMS ↔ Local Agency	Provides data exchange between individual court legacy CMS instances and local agencies (e.g., law enforcement, social services). Supports synchronous calls and event-driven notifications.

5. Compliance Standards

The Systems integrator shall ensure all systems and components comply with the following:

- FBI CJIS Security Policy — for systems handling criminal justice information.
- NIST SP 800-53 — for federal-grade information security controls.
- HIPAA — for systems processing protected health information (PHI).
- State of Tennessee IT Security Policies and Standards.
- Tennessee Public Records Act.
- Local Court Rules and Data Governance Policies.
- ISO 27001 — as a best-practice framework for information security management.
- All other State and Federal compliance and regulatory standards.

APPENDIX B: Scope of Systems Integrator Services

Scope of Services

TN AOC seeks a Systems integrator with demonstrated experience in Data Platforms. That is, designing, implementing, and supporting cloud native Integration Hubs and Centralized Data Repositories, data migration services, and Statewide Data Reporting solutions within the complex judicial environment. The implementation services sought are for:

- **Data Platform**
 - **Integration Hub:** Implementing a secure, cloud native, scalable MS Azure middleware infrastructure enabling seamless data exchange between CMS, eFiling, TnDR, TnRAS, TnPortal, and external systems.
 - **TnDR:** Creating the authoritative, cloud native data repository for statewide court data, supporting ingestion, transformation, storage, and provisioning for operational and analytical purposes.
- **Data Migration Services:** Implementing comprehensive data migration and ongoing data feeds, facilitating the data ingestion from legacy CMSs to TnDR and supporting continuous data synchronization with the new statewide CMS.
- **Service Desk Support:** Establishing and operating a centralized Service Desk to provide support for all Data Platform implementation phases.
- Post-go-live, the Contractor will provide **Post Implementation Support Services**, which include:
 - Hypercare
 - Ongoing Operations & Maintenance (O&M) support services

Additionally, refer to each section below to find a list of implementation service deliverables required.

The following sections provide an example of the systems integrator vendor services the State anticipates will be provided by the systems integrator along with corresponding activities, and information related to required implementation services. Respondents are encouraged to provide in their RFI response any alternative implementation service delivery approaches which may benefit the State.

1. SI Project Management & Service Enabling — Activities and Deliverables

The systems integrator shall:

- Lead overall project management, including scope, schedule, budget, and risk management.
- Establish and maintain project governance, including escalation paths, stakeholder roles, and a detailed implementation roadmap.
- Track and report project status, KPIs, and performance metrics.
- Maintain a risk management register, updating risks and mitigations regularly.
- Design and document the Data Platform architecture, including environment sizing, infrastructure, and TCO. Maintain comprehensive technical documentation, including architecture diagrams, integration specifications, test plans, deployment guides, and API catalogs.
- Define and document event-based processing rules, access controls, monitoring/logging frameworks, and error handling strategies.
- Design and document ETL frameworks for ingesting, transforming, and loading data into TnDR.

- Develop and execute a comprehensive Quality Assurance (QA) Test Plan, subject to review and approval by TN AOC. The plan shall encompass unit testing, system integration testing, user acceptance testing (UAT), and any additional testing activities as directed by TN AOC. The QA process must validate both the technical implementation and the functional performance of the Data Platform Services, as described in Appendix A.
- Conduct integration and security testing, providing results and obtaining stakeholder sign-off.
- Monitor, measure, and report on all agreed performance measures, ensuring continuous adherence to Service Level Agreements (SLAs) and proactively identifying and addressing any deviations.
- Provide training and knowledge transfer sessions for TN AOC staff, with supporting materials focused on Data Platform Services usage and administration.
- Ensure that all code, configurations, documentation, and intellectual property developed for the Data Platform are delivered to TN AOC in non-proprietary, maintainable formats (e.g., C#, .NET, open standards). No vendor-owned or proprietary platforms or components may be used. All deliverables must be structured to enable TN AOC's full ownership, operational independence, and future maintainability.

Table 1: Project Management & Service Enabling Deliverables

#	Deliverable	Type	Description
1	Data Platform Project Governance Plan	One-time	Governance structure, escalation paths, stakeholder roles, implementation roadmap, project risks, assumptions, and benefits.
2	Data Platform Status Report	Recurring (weekly)	Tracks activities, progress, quality, and performance against SI-proposed KPIs and AOC-agreed metrics, including Data Platform Services adoption.
3	Data Platform Risk Management Register	Recurring (monthly)	Tracks all identified risks, mitigations, and status throughout the project.
4	Data Platform Architecture Report	Recurring (per phase/release, updated as needed)	Comprehensive design and documentation of the Data Platform (Integration Hub & TnDR), including: • Infrastructure, architecture, and environment sizing. • vCores, bandwidth, and total cost of ownership (TCO) analysis. • Architecture diagrams and system topology. • Integration specifications and interface definitions. • Test plans and deployment guides. • API catalog, versioning, and usage guidelines.

			• Event-based business rules for data processing. • Access control policies and access control matrix. • Monitoring, logging, and alerting framework. • Error handling strategies, retry logic, and escalation paths. • ETL framework design for ingesting, transforming, and loading data. • Data mapping documentation and maintenance. • Operational enablement of Data Platform Services (manage, access, provision, and exchange court data).
5	Data Platform QA Test Plan	One-time	A detailed and executable Quality Assurance Test Plan covering all components of the Data Platform Services as defined in Appendix A. The plan shall include unit testing, system integration testing, user acceptance testing (UAT), regression testing, and any additional testing activities required for optimal performance or as directed by TN AOC. The deliverable must demonstrate validation of both technical implementation and functional performance.
6	Data Platform Test Results & Stakeholder Sign-Off	Recurring (per integration release)	Results of integration and Platform QA testing, including Data Platform Services functionality, with formal stakeholder sign-off.
8	Performance Management Report	Recurring (monthly)	Comprehensive report detailing compliance with all SLAs/SLRs, including metrics, trends, and corrective actions for any performance deviations.
9	Data Platform Security & Compliance Assessment Report	Recurring (per major release)	Results of penetration testing, vulnerability assessments, and compliance checks for all Data Platform components, including services.
10	Data Platform Training & Knowledge Transfer Sessions	Recurring (per major release)	Instructor-led or recorded sessions with supporting materials for TN AOC staff, focused on Data Platform Services usage and administration.

2. Integration Hub Stand Up – Activities and Deliverables

The systems integrator shall:

- Configure a secure, scalable, and highly available cloud native Integration Hub (licensed from Microsoft) to enable data exchange between Local CMS/Statewide CMS, eFiling, TnRAS, TnPortal, TnDR, and designated external systems (e.g., LEA, Probation).
- Recommend and deploy appropriate cloud integration services in accordance with TN AOC's architecture, security, and compliance requirements.
- Establish and configure cloud resources, including network, compute, storage, and integration services, to support current and anticipated integration workloads.
- Implement baseline security measures, including IAM roles and policies, encryption, key management, and access controls, in accordance with industry best practices, the State of Tennessee policies and standards, and the FBI CJIS Security Policy, ensuring compliance for all systems handling criminal justice information.
- Configure connectivity between the Integration Hub and all required internal and external systems, including secure network paths, firewalls, and endpoints.
- Set up environment-specific variables, secrets management, and configuration parameters to support development, testing, and production operations.
- Establish initial administrative and user access controls, including RBAC and SSO integration as required.
- Verify the Integration Hub's successful provisioning and readiness through health checks, smoke tests, and validation of connectivity and security controls.
- Document all provisioning steps, configurations, dependencies, and references to cloud documentation and infrastructure-as-code artifacts, ensuring reproducibility and auditability.

Table 2: Project Management Deliverables

#	Deliverable	Type	Description
1	Integration Hub Platform Provisioning & Configuration Report	One-time	Comprehensive documentation of the provisioning and configuration of the cloud native Integration Hub. Includes: • Provisioned cloud services, regions, and service versions. • Resource sizing, scaling, and high availability settings. • Network and connectivity setup (VPC/subnet, security groups, endpoints, VPN, etc.). • Security baseline configuration (IAM roles, policies, key vaults, certificates, encryption, compliance). • Environment variables, secrets management, and system parameters. • Initial admin/user accounts, RBAC, and SSO integration. • Health checks and readiness verification.

			• Prerequisites and dependencies addressed (e.g., cloud resource enablement, permissions). • Reference to vendor cloud documentation and infrastructure-as-code artifacts (if used).
--	--	--	---

3. TnDR Stand Up & Schema Determination — Activities and Deliverables

The systems integrator shall:

- Configure a secure, scalable, and highly available cloud native TnDR to support operational and analytical needs.
- Recommend and deploy appropriate cloud database services in accordance with TN AOC's architecture, security, and compliance requirements.
- Establish and configure cloud resources, including compute, storage, network, and database services, to support current and anticipated data workloads.
- Implement baseline security measures, including IAM roles and policies, encryption, key management, and access controls, following industry and State of Tennessee best practices.
- Set up environment-specific configurations for development, testing, and production, including environment sizing and resource allocation.
- Conduct a data modeling exercise to design the initial TnDR schema, using the TN AOC data dictionary as the foundational reference.
 - Align the proposed TnDR schema with the statewide CMS schema to ensure consistency across operational and analytical systems.
 - Document the proposed schema, including entity relationships, data types, and metadata definitions.
 - Present the schema to TN AOC for review and formal approval prior to deployment.
- Deploy the approved TnDR data model and schema into the designated environments (e.g., dev/test/prod) as part of the initial repository setup.
- Configure automated backup and recovery processes to ensure data protection and business continuity.
- Establish initial administrative and user access controls, including RBAC and SSO integration as required.
- Verify the repository's successful provisioning and readiness through health checks, smoke tests, and validation of connectivity and security controls.
- Document all provisioning steps, configurations, dependencies, and references to cloud documentation and infrastructure-as-code artifacts, ensuring reproducibility and auditability.

Table 3: TnDR Stand Up & Schema Determination Deliverables

#	Deliverable	Type	Description
1	TnDR Cloud Provisioning & Configuration Report	One-time	Comprehensive documentation of the provisioning and configuration of the cloud native TnDR. Includes: • Provisioned cloud database services, regions, and service versions. • Resource sizing and environment setup, including dev/test/prod. • Network and connectivity configuration (VPC/subnet, security groups, endpoints, etc.). • Security baseline configuration (IAM roles, encryption, key vaults, access controls). • Initial admin/user accounts, RBAC, and SSO integration. • Deployment of initial data model and schema aligned with TN AOC data dictionary. • Configuration of automated backup and recovery processes. • Health checks and readiness verification. • Prerequisites and dependencies addressed. • Reference to vendor cloud documentation and infrastructure-as-code artifacts (if used).
2	TnDR Design Package	One-time	Documentation of the overall design for the centralized data repository, including: • Data model and schema aligned with statewide CMS and TN AOC data dictionary (approved by TN AOC). • Data quality and validation rules. • Data lineage and provenance documentation. • Data retention and archiving policy.

4. Data Platform Services Stand Up — Activities and Deliverables

All Data Platform Services future state capabilities will be delivered and deployed by the systems integrator vendor within the scope of this document. Data Platform Services will be required to support the initial and on-going ingestion of data from the various legacy CMS to TnDR, as well as to access that data through TnRAS and TnPortal, will be utilized in production initially by TN AOC.

Other Data Platform Services (e.g., Ingest Case Updates into TnDR) may not be utilized until TN AOC's statewide CMS vendor integrates these services with the new statewide CMS as it is configured and rolled out.

The systems integrator will support establishment of this integration with the new Statewide CMS under the requirements in Appendix B - Post Implementation Support Activities and Deliverables.

The systems integrator shall:

General Requirements and Sequencing

- Architect, configure, and enable Data Platform Services in a logical, phased sequence to ensure foundational ingestion and data management capabilities are operational before enabling downstream access, provisioning, and exchange services.
- Prioritize the development and validation of ingestion-related services (i.e., applicable services related to initial data ingestion into TnDR from legacy CMS) to establish a reliable service in TnDR before enabling the remaining access, manage, provision, and exchange Data Platform service functionalities.
- Ensure that each Data Platform Service is fully documented, tested, and validated prior to being released for use in subsequent operational phases or by downstream applications.
- Coordinate with TN AOC and other implementation teams to align service readiness with project milestones and the rollout of dependent systems (e.g., statewide CMS).
- For each Data Platform Service (Manage, Access, Provision, Exchange Court Data), complete a readiness assessment, obtain TN AOC acceptance, and issue a Data Platform Service-specific Certificate of Completion prior to enabling the service for operational use or subsequent project phases.

Data Platform Services

The systems integrator shall reference the Data Platform Services outlined in Appendix A and shall be responsible for the design, configuration, and deployment of each service to enable the defined future-state functionality. The required services include:

- Manage Court Data
- Access Court Data
- Provision Court Data
- Exchange Court Data

Each Data Platform Service must be delivered in a manner that ensures interoperability, scalability, and readiness for integration with the legacy CMS and/or Statewide CMS upon its production deployment.

Table 4: Data Platform Services Stand Up Deliverables

#	Deliverable	Type	Description
1	Manage Court Data Service Implementation Package	Recurring (per migration phase)	Complete implementation package for <u>Manage Court Data</u> service, as defined in Appendix A. This deliverable shall include the technical design, configuration, and deployment of service components required to support structured data ingestion, transformation, and governance.

			The package must also include executed unit tests validating service functionality, along with comprehensive technical documentation.
2	Access to Court Data Service Implementation Package	Recurring (per migration phase)	Complete implementation package for <u>Access to Court Data</u> service, as defined in Appendix A. This deliverable shall include the technical design, configuration, and deployment of service components required to support structured data ingestion, transformation, and governance. The package must also include executed unit tests validating service functionality, along with comprehensive technical documentation.
3	Provision Court Data Service Implementation Package	Recurring (per migration phase)	Complete implementation package for <u>Provision Court Data</u> service, as defined in Appendix A. This deliverable shall include the technical design, configuration, and deployment of service components required to support structured data ingestion, transformation, and governance. The package must also include executed unit tests validating service functionality, along with comprehensive technical documentation.
4	Exchange Court Data Service Implementation Package	Recurring (per migration phase)	Complete implementation package for <u>Exchange Court Data</u> service, as defined in Appendix A. This deliverable shall include the technical design, configuration, and deployment of service components required to support structured data ingestion, transformation, and governance. The package must also include executed unit tests validating service functionality, along with comprehensive technical documentation.
5	Manage Court Data Service Certificate of Completion	Recurring (per migration phase)	Formal certification signed by TN AOC confirming that the <u>Manage Court Data</u> services, as defined in Appendix A, have been fully implemented, functionally validated, and are ready for operational use. This certificate will be based on the successful completion of all required acceptance testing activities and will serve as the official sign-off for production readiness.
6	Access to Court Data Service Certificate of Completion	Recurring (per migration phase)	Formal certification signed by TN AOC confirming that the <u>Access to Court Data</u> services, as defined in Appendix A, have been fully implemented, functionally validated, and are ready for operational use. This certificate will be based on the successful completion of all required acceptance testing activities and will serve as the official sign-off for production readiness.
7	Provision Court Data Service	Recurring (per	Formal certification signed by TN AOC confirming that the <u>Provision Court Data</u> services, as defined in Appendix A,

	Certificate of Completion	migration phase)	have been fully implemented, functionally validated, and are ready for operational use. This certificate will be based on the successful completion of all required acceptance testing activities and will serve as the official sign-off for production readiness.
8	Exchange Court Data Service Certificate of Completion	Recurring (per migration phase)	Formal certification signed by TN AOC confirming that the <u>Exchange Court Data</u> services, as defined in Appendix A, have been fully implemented, functionally validated, and are ready for operational use. This certificate will be based on the successful completion of all required acceptance testing activities and will serve as the official sign-off for production readiness.

5. Data Migration & Ongoing Feeds to TnDR — Activities and Deliverables

The systems integrator shall:

Section A: Data Migration Overview

- Develop and submit a Comprehensive Data Migration Plan for TN AOC approval, covering:
 - Phase 1A: General Sessions Courts: Initial bulk-load strategy and load from existing local legacy CMS databases
 - Phase 1B: Other Trial Courts: Initial bulk-load strategy and load from existing local legacy CMS databases
 - Phase 2A: General Sessions Courts: Interim ongoing data feeds from legacy CMS databases.
 - Phase 2B: Other Trial Courts: Interim ongoing data feeds from legacy CMS databases.
 - Phase 3: Event-based data feeds from statewide CMS.
 - Coordination with TN AOC and the statewide CMS implementation team.
- Develop a Repeatable Migration Playbook incorporating operational best practices to guide all data migration phases and future onboarding waves.

Section B: Phase-Specific Activities

- Phase 1 A&B — Initial Bulk Data Load from Legacy CMS
 - Request and receive bulk data extracts from local legacy CMS for a specified time period and format, as determined by TN AOC.
 - Perform load and performance testing of TnDR under bulk ingestion conditions.
- Phase 2 A&B — Interim Data Feeds from Legacy CMS
 - Implement daily batch file transfers (e.g., via SFTP) from legacy CMS systems to TnDR through the Integration Hub.
 - Define and implement incremental delta-load logic, change data capture (CDC), or polling schedules.

- Coordinate onboarding of additional jurisdictions over time.
- Phase 3 — Statewide CMS Data Feeds
 - Collaborate with the statewide CMS vendor to implement event-based processing with near-real-time (e.g., via RESTful APIs) updates to TnDR.
 - Apply mapping and transformation rules from the statewide CMS schema to the standardized TnDR schema.
 - Continue jurisdiction onboarding and validation as statewide CMS rollout progresses.

Section C: Common Data Migration Activities Across Phases

- Collaborate with courts, legacy CMS vendors, or the statewide CMS vendor to obtain data extracts or enable data feeds.
- Apply mapping and transformation rules from source legacy CMS or statewide CMS schemas to the standardized TnDR schema.
 - Enforce the standardized TnDR data taxonomy for all incoming data; legacy naming conventions (e.g., TJIS) shall not be accepted.
- Conduct data profiling to assess the quality, completeness, and readiness of incoming data.
- Ingest data into TnDR via the Integration Hub, applying required transformations and cleansing*.
- Implement rollback procedures and transactional controls to ensure recoverability in case of failed loads.
- Execute validation and reconciliation processes across all migration phases, comparing source data (exports or feeds) to TnDR loads.
- Generate audit logs for all ingest operations, capturing timestamps, source identifiers, and processing outcomes.
- Conduct performance and scalability testing to validate responsiveness and throughput under expected load conditions.
- Obtain TN AOC stakeholder sign-off at defined milestones for each data migration phase.

**Data cleansing may be conducted by Clerks in the legacy CMS ahead of migration.*

Table 5: Data Migration & Ongoing Feeds to TnDR Deliverables

#	Deliverable	Type	Description
1	Data Migration Plan	One-time	A unified data migration strategy and process document covering every phase.
2	Data Migration Playbook	One-time	Repeatable, step-by-step operational guide for executing data migration, to be used in current and future phases.

3	Migration Risk Assessment & Mitigation Plan	Recurring (per migration phase)	Identification of migration risks with mitigation strategies and contingency plans.
4	Load & Performance Test Results	Recurring (per migration phase)	Documentation of load and performance testing outcomes for TnDR during/after migration.
5	Migration Validation & Reconciliation Report	Recurring (per migration phase)	Results of testing, validation, and reconciliation of migrated data, including data integrity checks.
6	Audit Log of Migrated Records	Recurring (per migration phase)	Detailed record of all migrated data with timestamps and source references for traceability.
7	Migration Certificate of Completion	Recurring (per migration phase)	Formal sign-off from TN AOC stakeholders per data migration phase.

6. TnRAS — Statewide Reporting & Analytics — Activities and Deliverables

The systems integrator shall:

- Recommend and document a best-practice architecture for TnRAS, including data modeling for analytics, role-based access control, performance optimization, and self-service analytics capabilities.
- Develop and deliver sample dashboard/report designs, user interface mockups, and reference implementations that demonstrate integration with TnDR for real-time and scheduled data sourcing, and address both internal and public access requirements.
- Provide comprehensive technical and user documentation for the proposed reporting and analytics solution, including guidance on dashboard/report development, data refresh strategies, and best practices for ongoing maintenance and enhancement.

7. TnPortal — Web-Based Data & Analytics Access — Activities and Deliverables

The systems integrator shall:

- Recommend and document a best-practice architecture for a secure, responsive, web-based portal (TnPortal) that will provide internal and potential public access to court data and analytics.
- Develop and deliver sample portal designs, user interface mockups, and reference implementations that demonstrate integration with TnDR for data sourcing and with TnRAS for analytics and reporting.
- Recommend and document a best-practice architecture for TnPortal, including authentication and authorization, audit logging, user activity tracking, accessibility, responsive design, and integration patterns with TnDR and TnRAS.

8. Service Desk Support — Activities and Deliverables

The systems integrator shall:

- Establish and operate a centralized Service Desk to provide Tier 2 support for all Data Platform implementation components, including Integration Hub, TnDR, TnRAS, and TnPortal, as well as all integration, migration, and interoperability services delivered by the SI.
- Provide multi-channel user support (phone, email, web portal/ticketing system) during defined business hours (determined by TN AOC), with on-call escalation procedures for critical incidents outside standard hours.
- Configure and maintain an IT Service Management (ITSM) or equivalent ticketing system to log, track, and manage all incidents, service requests, change requests, and inquiries related to SI-implemented Data Platform services.
- Categorize, prioritize, and assign all incoming tickets according to a proposed documented severity matrix, ensuring alignment with agreed Performance Measures for response and resolution times.
- Acknowledge all incidents and service requests within the defined SLA response times and provide initial triage and troubleshooting for Data Platform service issues.
- Diagnose and resolve Tier 1 and Tier 2 incidents and service requests within the agreed SLA resolution times, including but not limited to:
 - Integration and data exchange failures.
 - Data migration errors.
 - ETL process exceptions.
 - API connectivity issues.
 - User access and permissions problems.
 - Reporting and analytics service issues.
 - Portal usability or accessibility defects.
- Escalate unresolved or complex issues to Tier 3 support, TN AOC technical teams, or product/infrastructure vendors as appropriate, and coordinate cross-team incident resolution.
- Communicate incident status, progress updates, and closure notifications to affected users and stakeholders throughout each ticket's life cycle.
- Maintain and update a comprehensive knowledge base and self-service support portal, including documentation of common issues, troubleshooting guides, FAQs, and SI-specific operational procedures.

- Generate and deliver regular Service Desk performance reports to TN AOC, including metrics on incident volume, categorization, response/resolution times, first contact resolution rates, root cause analysis, and user satisfaction.
- Conduct root cause analysis and post-incident reviews for recurring or Defect Level 1 or 2 incidents, providing recommendations for process improvement and preventive actions.
- Support user onboarding and offboarding processes, including provisioning, de-provisioning, and permissions management for Data Platform services as implemented by the SI.
- Facilitate training sessions and user orientation on Service Desk processes, ticketing system usage, and self-service resources for Data Platform services.
- Ensure all Service Desk activities comply with TN AOC security, privacy, and regulatory requirements, including FBI CJIS Security Policy, HIPAA, and State of Tennessee IT security policies.
- Continuously review, assess, and improve Service Desk processes and procedures, incorporating feedback from TN AOC, end users, and lessons learned from incident management.

Table 8: Service Desk Support Deliverables

#	Deliverable	Type	Description
1	Service Desk Implementation Plan	One-time	Detailed plan for establishing Service Desk operations, including staffing, processes, escalation paths, and ITSM/ticketing system configuration.
2	Service Desk Operations Manual	One-time (updated as needed)	Comprehensive documentation of Service Desk procedures, ticketing workflows, severity matrix, escalation, and reporting protocols.
3	Service Desk Ticketing System Setup	One-time	Configuration and deployment of an ITSM/ticketing system for incident, service request, and change management.
4	Incident Management & Resolution Report	Recurring (monthly)	Monthly report detailing incident volume, categorization, response/resolution times, first contact resolution rates, and SLA/SLR compliance.
5	Root Cause Analysis & Post-Incident Review	Recurring (monthly)	Documentation of root cause analysis and corrective actions for Defect Level 1 or 2 or any recurring incidents.
6	Service Desk Performance Dashboard	Recurring (monthly)	Real-time dashboard or monthly summary of key Service Desk metrics, including SLA/SLR adherence and user satisfaction scores.

7	Knowledge Base & Self-Service Portal	Recurring (monthly updates)	Creation and maintenance of a searchable knowledge base, FAQs, troubleshooting guides, and self-service support resources for Data Platform services.
8	User Onboarding & Offboarding Support	As needed	Execution and documentation of user provisioning, de-provisioning, and permissions management for SI-implemented Data Platform services.
9	Service Desk Training & Orientation Sessions	As needed	Delivery of training and orientation for TN AOC staff and end users on Service Desk processes, ticketing system usage, and self-service resources.
10	Incident Closure Notification	Per Incident	Formal notification to users and stakeholders upon incident resolution and service restoration.
11	Service Desk Continuous Improvement Plan	Quarterly	Periodic review and update of Service Desk processes, incorporating feedback, lessons learned, and best practices.

9. Post Implementation Support — Activities and Deliverables

The systems integrator shall:

- Deliver a post-implementation support plan, covering:
 - Hypercare support immediately post go-live (2 months). During Hypercare, the systems integrator vendor is responsible for promptly resolving any newly discovered defects as well as actively managing and remediating any outstanding non-blocking defects identified during User Acceptance Testing (UAT), utilizing a punch list, defect tracker, or other agreed-upon mechanism.
 - Ongoing Operations and Maintenance (O&M) support following the hypercare term (12 months).
 - Data Platform Services enabling and operational support.
 - Ongoing Service Desk Support.
 - Training and Knowledge Transfer.
 - The plan must include clear procedures for defect prioritization, tracking, communication, and resolution to ensure a smooth transition to steady-state operations.
- Provide post-implementation support to ensure that all deployed Data Platform Services (e.g., Manage, Access, Provision, Exchange Court Data) are successfully integrated with the statewide CMS as it is configured and rolled out. This includes:
 - Collaborating with the statewide CMS vendor to validate service interoperability and data exchange functionality.

- Supporting the activation and testing of services that were deployed but not yet utilized during initial implementation (e.g., ingesting case updates into TnDR).
- Ensuring that all Data Platform Services deliver intended functionality and value to TN AOC and the Tennessee court technology ecosystem once the statewide CMS enters production.

Table 9: Post Implementation Support Deliverables

#	Deliverable	Type	Description
1	Data Platform Post-Implementation Support Plan	One-time	Plan to cover systems integrator support, maintenance, and warranty services after go-live. The plan must include a 2-month Hypercare support term, a 12-month operations and maintenance (O&M) support term, Data Platform Services enablement and operational support, ongoing Service Desk Support, and Training & Knowledge Transfer of the Data Platform Services. The plan must account for the resolution of any newly discovered defects, as well as actively managing and remediating any outstanding non-blocking defects identified during the implementation phase that have not been resolved.
2	Post-Statewide CMS Integration Enablement Report	One-time (upon CMS production rollout)	A comprehensive report documenting the successful activation and validation of all Data Platform Services integrated with the statewide CMS. The report shall include: ▪ A complete readiness assessment for each Data Platform Service (Manage, Access, Provision, Exchange Court Data). ▪ Results from integration and functional testing with the statewide CMS. ▪ Confirmation of schema alignment and data flow integrity. ▪ Stakeholder validation and formal acceptance. ▪ Any required configuration updates to support full production use.

10. Performance Management

TN AOC seeks to establish clear and comprehensive Performance Measures (e.g., Service Level Agreements (SLAs) and Service Level Requirements (SLRs)) for the Data Platform Implementation services. These Performance Measures are designed to ensure that the selected systems integrator delivers a Data Platform, Migration, and Statewide Reporting services that meet the highest performance, reliability, interoperability, and security standards.

The Performance Measures will define the expected service levels, including availability, support, and response times. At the same time, the SLRs will outline the technical and operational requirements necessary to support TN AOC's strategic vision for modernizing court operations.

Together, these Performance Measurements will serve as the foundation for a successful partnership, ensuring that the solution effectively addresses the diverse needs of Tennessee's Trial Courts and enhances the accessibility and efficiency of the state's court system.

A. Measurement Period

If the "Measurement Period" is designated as "monthly," it shall mean the period commencing 12:00 a.m. on the first day of each month and ending 12:00 a.m. on the first day of the following month; if the "Measurement Period" is designated as "quarterly," it shall mean the period commencing 12:00 a.m. on the first day of each quarter and ending 12:00 a.m. on the first day of the following quarter. If the "Measurement Period" is designated as "annually," it shall mean the period commencing 12:00 a.m. on the first day of each fiscal year and ending 12:00 a.m. on the first day of the following fiscal year.

B. Service Level Exceptions

In addition to scheduled downtime, the Contractor shall not be responsible for a failure to meet any Performance Measurement to the extent that such failure is directly caused by any of the following:

- a) Service outages and missed SLRs due to system components owned or controlled by TN AOC or a Clerk's Office.
- b) Service outages and missed SLRs due to system components owned or controlled by third-party service providers other than subcontractors engaged by the prime Contractor. The Contractor will conduct a Root Cause Analysis to determine the reasons for outages.
- c) Willful misconduct or law violations by TN AOC or third-party service providers, other than subservice providers engaged by the prime Contractor.
- d) Service or resource reductions requested or approved by TN AOC and agreed to by the parties through a Change Request; provided that, as part of such process, the Contractor has previously notified TN AOC in writing that the implementation of such Change Request would result in such failure to meet the SLR.

C. Changes to Service Level Requirements

The parties may agree to add or otherwise make changes to the SLR. When setting a new SLR, the process to set the performance target for the new SLR will include the following steps (as ordered):

- a) By mutual agreement between TN AOC and the Contractor; or
- b) Engaging a third-party to identify a commercially common target and measurement calculation aligned with the Agreement.

At TN AOC's request, the Contractor will provide TN AOC with the performance data recorded in connection with the Services to inform TN AOC regarding implementing such changes.

D. Service Level Monitoring and Measurement

The Contractor will continuously monitor the implemented Data Platform and the services provided to identify, report, and correct SLR failures and ensure that the Contractor is meeting or exceeding the SLRs as required herein. The Contractor will notify TN AOC immediately upon Knowledge of an actual or anticipated SLR failure. In this context, Knowledge means facts known by any Contractor personnel performing services under the Agreement.

E. Measurement Reporting

The Contractor will provide reports to TN AOC regarding their compliance with the SLRs. The Contractor will measure all data reasonably required by TN AOC to determine the Contractor's performance of the measured services against the applicable SLRs. Without limiting the foregoing, the Contractor will keep complete and accurate logs of all such data for no less than the duration of the Agreement.

The Contractor will provide TN AOC with performance monitoring reports in a web-based dashboard format that depicts the current conditions across the Solution.

On or before the 10th calendar day of each calendar month or as otherwise requested by TN AOC, the Contractor will deliver a Performance Measurement Report to TN AOC containing:

- a) For each measured SLR and with respect to the immediately preceding calendar month, all data relating to the provision of the service during the applicable month;
- b) For each measured SLR during the immediately preceding calendar month, details of the Contractor's performance as measured against the SLRs for such Service during the applicable month;
- c) Details of any Scheduled Downtime that the Contractor believes has impacted the measured Services during the applicable month; and
- d) Any other information reasonably requested by TN AOC.

For any SLRs with a measurement period of longer than a month, the provision of the second item listed above shall apply for the calendar month in which the final date of the measurement period for such SLR falls.

Upon TN AOC's request, the Contractor will provide TN AOC data and details for measured SLRs in an approved form and format containing:

- a) All data relating to the provision of the measured SLR during the applicable day;
- b) Details of the Contractor's performance as measured against the SLRs during the applicable day;
- c) Details of any measured SLRs that were supposed to be performed during the applicable day that were not entirely performed as required; and
- d) Details of any measured SLRs that were supposed to have been performed during the previous day but were not entirely performed as required on that day, and the status of such measured services.

In generating data for dashboard reports provided by the Contractor, the Contractor will use, for each SLR, the measurement tools and methodologies needed to adequately measure each service level, or such other means as reasonably required by TN AOC, to confirm the Contractor's compliance with the SLRs.

The Contractor will also provide all the SLR data to TN AOC, upon request.

F. Service Problem Analysis

Notification of Problems

If the Contractor becomes aware of any problem, they must:

- a) Provide TN AOC with prompt notice of such a problem, no later than two (2) calendar days after discovery.
- b) Deliver a complete problem description to TN AOC, including its expected impact.
- c) Meet with TN AOC no later than four (4) calendar days after discovery to formulate and implement an action plan to minimize or eliminate the problem's impact.

Corrective Action Plan

If either party reasonably determines that a problem has occurred or is likely to happen, that party shall promptly notify the other party within two (2) calendar days. Concurrent with delivery or receipt of such notice, the Contractor shall:

- a) Immediately mitigate any harmful effects within control.
- b) Regularly update TN AOC on remedial progress and status.
- c) Demonstrate that all reasonable actions have been taken to prevent recurrence.
- d) Conduct a Root Cause Analysis within five (5) calendar days of problem resolution and report findings to TN AOC.
- e) Develop a Corrective Action Plan to address and prevent problem recurrence.
- f) Allocate necessary resources to resolve and prevent issues as outlined in the Corrective Action Plan.
- g) Upon TN AOC's acceptance of the Corrective Action Plan, promptly implement solutions, provide progress updates, and demonstrate preventive measures.

G. Additional Remedies

If the Contractor fails to identify and resolve any problems within its control that may impede or delay the timely delivery of the Statement of Work activities, TN AOC may:

- a) Require the Contractor to provide, at its sole cost, all additional resources necessary to resolve such problems.
- b) Equitably reduce the charges to account for delayed or incomplete tasks in the Statement of Work or services not received.

H. Performance Reimbursement

The Contractor shall reimburse TN AOC for failure to achieve SLR performance due to disruption of the Data Platform, Migration, or Statewide Reporting services.

TN AOC expects continuous improvement in the Contractor's service provision. At TN AOC's discretion, new SLRs may be added annually to reflect changing requirements and improvements.

SLRs have been set to meet TN AOC's minimum business requirements, with Service Level Reimbursements applicable for missed SLRs as follows:

- a) For each SLR failure during the same Measurement Period, 10% of the total monthly service charges, or a TN AOC pre-determined amount if the monthly service charge does not apply, will be reimbursed to TN AOC within thirty (30) calendar days of receipt of the applicable report. This applies to each SLR failure (e.g., 20% of the monthly charges for two (2) SLR failures).
- b) The maximum amount of Service Level Reimbursements in any contract year shall not exceed 20% of the total annual service charges, which is aligned with industry standards to reflect both risk and impact of service disruptions.
- c) If the Contractor fails to achieve twenty-five (25) or more SLRs within any rolling twelve (12) month period, they shall be deemed in default of the Agreement. Default conditions are defined as the inability to meet the minimum performance standards as outlined in the SLRs, with an opportunity for the Contractor to address issues before being officially deemed in default.

These Performance Measurements are designed to provide a framework for ensuring the proposed SaaS solution meets the operational and strategic needs of the TN AOC while maintaining high performance and security standards.

I. Performance Measurement Matrix

The following table identifies the Performance Measures for which the Contractor shall be responsible.

Table 16: Performance Measures

I D	Performance Measures	Service Measure	Performan ce Metric	Performan ce Target: SLA	Formula	Measureme nt & Reporting Period
1	Reporting	Schedule Adherence	Provision of reports within the defined timelines in the Agreement	100%	[Number of agreed actions that are completed within the target dates] ÷ [The total number of agreed actions in the Measurement Period] X 100%	Monthly
2	Incident Resolution	Time to Resolve	Tiers: Defect Level 1: ≤ 2 hours Defect Level 2: ≤ 4 hours Defect Level 3: ≤ 48 hours Defect Level 4: ≤ 120 hours	Defect Level 1: ≤ 2 hours 95% of the time Defect Level 2: ≤ 4 hours 95% of the time Defect Level 3: ≤ 48 hours 95% of the time Defect Level 4: ≤ 120 hours 95% of the time	[Number of defects resolved within the applicable time specified in the performance metric] ÷ [The total number of defects in the Measurement Period] X 100%	Monthly
3	First Contact Resolution	First Contact Resolution Percentage	Number of User contacts to the service desk during the Measureme	80%	[Number of User contacts to the service desk during the Measuremen	Monthly

			nt Period which are resolved by the initially contacted Service Desk agent and did not result in a call back		t Period which are resolved by the initially contacted Service Desk agent and did not result in a callback] ÷ [The total number of User contacts during the Measuremen t Period] x 100%	
4	Response	Time to Respond	Incident: ≤ 15 elapsed minutes Incident: ≤ 30 elapsed minutes	Incident Response within 15 minutes: ≥ 95% Incident Response within 30 minutes: 100%	[Number of Incidents responded to within time limits set by Performance Metric] ÷ [The total number of Incidents in the measuremen t period] X 100%	Monthly
5	Time to Notify Customer of Defect Level 1 or 2	Time to Notify	<15 minutes	98%	[Number of incidents within Performance Metric] ÷ [Total number of incidents during Measuremen t Period] x 100%	Monthly

6	Speed to Answer	Phone Response Time	≤30 seconds	80%	[Number of phone calls to the Service Desk during the Measurement Period that are answered by a Service Agent within the Performance Metric] ÷ [total number of phone calls to the Service Desk during the Measurement Period] x 100%	Weekly
7	Call Abandonment Rate	Phone Response Time	≤5%	100%	[Number of phone calls to the Service Desk during that Measurement Period that are abandoned from the queue before being answered by a Service Desk agent] ÷ [Total number of phone calls that entered the queue during the Measurement Period] x 100%	Weekly

8	Email and voicemail response rate	Response Time	≤4 hours	98%	Email response rate: [Number of emails received and responded to within the Performance Metric during the Measurement Period] ÷ [Total number of emails received during the Measurement Period] x 100% Voicemail response rate: [Number of voicemails received by the voicemail system during the Measurement Period and responded to by a Service Desk agent within the Performance Metric] ÷ [Total number of voicemails received by the voicemail system during the Measurement Period] x 100%	Weekly
---	--	----------------------	----------	-----	---	--------

9	Incident Closure Notice (via email and/or phone)	Elapsed Time after service restoration	<20 minutes following Incident Resolution	98%	[Number of Incidents Resolved, and service requests completed during the Measurement Period for which a closure notice was provided to the User within the Performance Metric] $\div$ [Total number of Incidents Resolved, and service requests completed during the Measurement Period] $\times 100\%$	Weekly
10	Release Documentation	Documentation received by TN AOC within the agreed time before Release date	Delivery of documentation within an agreed-upon time frame	100%	[Number of documentation releases within agreed timing] $\div$ [Total number of documentation releases during Measurement Period] $\times 100\%$	Monthly
11	Solution Interoperability	Interoperability	The system must integrate seamlessly with existing state and local justice partner applications,	100%	Successful integration will be verified through interoperability testing, with a target of 100%	Bi-Annual

			supporting data exchange through standardized APIs		successful data exchanges.	
12	Project Milestones & Deliverables	Milestone Adherence	Deliverables must be received on time	100%	[Number of deliverables received on or before the agreed due date] $\div$ [Total number of deliverables to be received during Measurement Period] $\times 100\%$	Per the deliverable due date. Aggregated for quarterly reporting
13	Change Management	Change Implementation	Approved changes must be implemented within agreed timeframes and with zero unplanned outages	100% of changes implemented within the agreed window; 0% unplanned outages	[Number of approved changes implemented within the agreed window and without unplanned outage] $\div$ [Total number of approved changes during Measurement Period] $\times 100\%$	Per change event. Aggregated for monthly reporting

Definitions

For purposes of this Contract, definitions shall be as follows and as set forth in the Contract:

Term	Definition
Acceptance	The State's formal acknowledgment that a delivered phase, work product, deliverable, or software product meets all specified requirements and performance criteria as outlined in the contract or as determined by TN AOC.
Agentic AI	An optional, specialized Artificial Intelligence component (Azure AI Foundry) that may be embedded to enable users to perform advanced natural language data querying without complex database syntax.
Agreement/Contract	A legally enforceable document that delineates the terms and conditions mutually accepted by the TN AOC and the Contractor. It establishes the obligations, rights, and responsibilities of each party, ensuring clarity and compliance throughout the procurement process. This document serves as the cornerstone of the partnership, providing the framework for service delivery, performance standards, and resolution of any disputes, thereby safeguarding the interests of all parties involved.
API (Application Programming Interface)	A set of protocols and tools for building and interacting with software applications, enabling integration and data exchange between systems and the Data Platform.
Approval Gate	A mandatory project milestone where the AOC evaluates the success of a completed phase against predefined metrics. The Contractor may not proceed to the subsequent phase without formal, written authorization from the AOC.
Azure (Microsoft Azure)	The chosen cloud infrastructure ecosystem hosting both the Integration Hub and Data Repository, selected for its government alignment and security capabilities.
Case Management System (CMS)	A court Case Management System or Solution (CMS) is a comprehensive software application designed to manage and track all information related to the life cycle of legal cases. This system integrates various functionalities with additional systems to support the administration of justice, ensuring that cases are processed efficiently and effectively from initial filing through to resolution.
Centralized Data Repository (TnDR)	A data repository is a centralized database designed to store, manage, and aggregate data from various systems across the state. A data repository enables comprehensive data integration, reporting, and analytics, providing a unified view of data. See also "TnDR."
Change Management	The process, procedures, and controls for managing changes to the Data Platform environment, including configuration, deployment, and upgrades, are to ensure minimal disruption and traceability.

Commercial off-the-shelf (COTS)	Ready-made software or hardware products available for purchase by the general public and used without significant customization, including those used to implement the Data Platform.
Contractor	The systems integrator vendor hired by TN AOC to provide the goods and/or services, and deliverables specified in this Contract. Contractor, systems integrator, and systems integrator vendor are used interchangeably.
Data Integration	The process of combining and synchronizing data from various sources into the Data Platform for unified management, analytics, and reporting.
Data Migration	The process of transferring data from legacy systems or sources into the new Data Platform, including mapping, transformation, validation, and reconciliation.
Data Platform	The cohesive data management solution composed of an Integration Hub and a Centralized Data Repository (TnDR), including TnRAS, TnPortal and all supporting services and integrations.
Data Platform Services	The set of services enabled by the Data Platform, which includes managing, accessing, provisioning, and exchanging court data in support of court operations and analytics.
Defect	Any bug, error, malfunction, or performance interruption that causes the Solution or Data Platform to fail to operate in conformance with specifications.
Defect Level 1	A Documented Defect that causes: (a) complete application failure or application unavailability (b) application failure or unavailability in one or more locations or (c) systemic loss of multiple essential system functions.
Defect Level 2	A Documented Defect that causes: (a) repeated, consistent failure of functionality affecting more than one user or (b) loss or corruption of data.
Defect Level 3	A Level 1 Defect with an existing circumvention procedure, or a Level 2 Defect that affects only one user or for which there is an existing workaround procedure.
Defect Level 4	A documented Defect that causes failure of non-essential functionality or a cosmetic or other documented Defect that does not qualify as any other service level defect.
Deliverable	A specific work product, report, or artifact to be provided by the Contractor to TN AOC as required by the contract, as listed in the Deliverables section.

Deliverable Expectation Document (DED)	Is a formal document, proposed by the systems integrator and subject to TN AOC's review and approval, which specifies the detailed requirements, acceptance criteria, quality standards, and review process for a project deliverable to ensure mutual understanding and objective evaluation between both parties.
eFiling Solution	The electronic submission of legal documents with courts, replacing paper-based methods with a digital solution, and integrating with CMS and the Data Platform.
ETL (Extract, Transform, Load)	The process of extracting data from source systems, transforming it to fit operational needs, and loading it into the target repository (TnDR).
Hypercare	A period of intensive support provided immediately after a system goes live to address issues, ensure stability of the Data Platform and its services, and facilitate user adoption.
Incident	Any event which is not part of the standard operation of a service, and which causes, or may cause, an interruption to, or a reduction in, the quality of that service, including the Data Platform.
Integration	The process of linking different systems and applications to enable seamless data sharing and workflow across the court technology ecosystem and Data Platform.
Integration Hub	A cloud-native centralized platform or middleware that facilitates secure, scalable, and standardized exchange of data between disparate systems, applications, and databases, serving as a core component of the Data Platform.
Knowledge Base	A repository of documentation, troubleshooting guides, FAQs, and support materials maintained by the Service Desk for end users and support staff of the Data Platform.
LEA	Law Enforcement Agencies
Master Party Management (MPM)	Refers to the practice of managing and maintaining a single, consistent set of data about all the "parties" involved in a transaction or case, across different systems within an organization, ensuring accuracy and eliminating duplicate information.
Operations & Maintenance (O&M)	Ongoing activities to keep the Data Platform and its components functional, secure, and aligned with TN AOC requirements after Go-Live.
Performance Management	The ongoing process of monitoring, measuring, and reporting on service levels, SLAs, and SLRs to ensure contract compliance and continuous improvement for the Data Platform.
Portal (TnPortal)	The secure, web-based portal providing internal and public access to court data and analytics, integrated with TnDR and TnRAS.

Post-Implementation Support	Support services provided after Go-Live include hypercare, O&M, service desk support, and knowledge transfer for the Data Platform.
Problem	Means any material problem, including any (i) Security Incident, (ii) failure to deliver any services, (iii) failure to deliver any service levels, (iv) situation that has negatively impacted or reasonably could negatively impact the maintenance of TN courts, information security, operations, and any policies, procedures, or services described in the Agreement, the Statement of Work or work authorization, or Applicable Laws; or (v) situation that has had or reasonably could have any adverse impact on the services.
Reporting & Analytics Solution (TnRAS)	The statewide reporting and analytics platform, delivering dashboards, reports, and self-service analytics sourced from TnDR.
Requirements	The functional, non-functional, technical, and compliance needs that must be met by the Solution and its components, including the Data Platform.
Risk Management	The process of identifying, assessing, tracking, and mitigating risks to the successful delivery and operation of the Data Platform and services.
Role-Based Access Control (RBAC)	A security approach that restricts system access to authorized users based on their roles within the organization, implemented across Data Platform components.
SaaS (Software as a Service)	A software licensing and delivery model in which software is accessed online via a subscription, rather than bought and installed on individual computers, as used for the Data Platform.
Scheduled Downtime	A planned and communicated period during which a system or service, including the Data Platform, is unavailable for maintenance or upgrades.
Service Desk	The centralized support function is responsible for handling incidents, service requests, and user support for the Data Platform and its services.
Service Desk Ticketing System	The Information Technology Service Management (ITSM) or equivalent tool used to log, track, and manage incidents, service requests, and changes related to the Data Platform.
Service Level Agreement (SLA)	A formal contract between the Contractor and TN AOC that defines the expected level of service, including specific performance metrics for the Data Platform.
Service Level Requirement (SLR)	Detailed technical or operational specifications outlining the necessary conditions and capabilities a service must fulfill to meet the SLA (e.g., metric measurement, formula, reporting period) as measured for the Data Platform.
Systems Integrator (SI) Vendor	The Contractor or systems integrator is responsible for designing, implementing, integrating, migrating, validating, documenting, training, and supporting the Data Platform services and its components.

Solution	The comprehensive statewide Data Platform and supporting data management components that will be procured and implemented under this Contract.
Stakeholder	Any individual, group, or organization with an interest in the successful delivery and operation of the Data Platform, including TN AOC staff, court personnel, and external partners.
Target State Design (TSD)	The conceptual and technical blueprint describing the future-state architecture, capabilities, and guiding principles for the court technology ecosystem, including the Data Platform.
Tennessee Administrative Office of the Courts (TN AOC or AOC)	The administrative entity providing support to the Tennessee Supreme Court and the entire State court system.
Tennessee Data Portal (TnPortal)	The dedicated web-based portal that will provide secure access to statewide court data and analytics for internal users (and external users if determined by TN AOC).
Tennessee Statewide Centralized Data Repository (TnDR)	Refers to the to-be-created Tennessee statewide “centralized data repository,” which is a single, consolidated cloud database where statewide data from multiple sources is collected, stored, managed, and accessed. This repository will provide a unified and consistent view of statewide court-related data.
Tennessee Statewide Reporting & Analytics Solution (TnRAS)	The statewide platform for comprehensive data reporting and analytics, leveraging insights embedded in the TnDR data.
Trial Courts	In Tennessee, Trial Courts are where civil and criminal cases are initially filed and heard, encompassing Circuit, Chancery, Criminal, General Sessions, Juvenile, and Municipal Courts. Circuit Courts manage a broad range of cases, including appeals and jury trials, while Chancery Courts focus on equity matters without jury trials. General Sessions Courts manage preliminary hearings, misdemeanors, traffic violations, and small claims, often serving as the first judicial contact for many individuals. Juvenile Courts address cases involving minors, focusing on rehabilitation and welfare, while Municipal Courts manage city ordinance violations and minor infractions. Trial Courts do not include the State of Tennessee Court of Appeals and Supreme Court.
User Acceptance Testing (UAT)	The process by which end users validate that a system meets business requirements and is ready for production use, including the Data Platform and its integrations.