



City of Dallas



Request For Information (RFI)

Project Title: AI-Assisted Digital Evidence Analysis Platform

Solicitation Number: BD26-00031278

1. Introduction

1.1.Purpose of the RFI

The Dallas Police Department (“DPD” or “the Department”) is issuing this Request for Information to identify commercially available platforms that apply artificial intelligence to the analysis of digital case evidence (recorded audio, video, images, documents, and spreadsheets) in support of criminal investigations. This RFI is issued for information-gathering and planning purposes only. It is not a solicitation, and no contract will be awarded from responses to it.

1.2.Background

DPD investigations involve growing volumes of digital evidence: body-worn and surveillance video, jail telephone recordings, mobile device extractions, scanned documents, financial records, and call detail records. Manual review of this material is a significant constraint on case throughout. The Department maintains existing systems of record, including Axon Evidence.com, and is interested in platforms that ingest evidence from those systems rather than replace them. This evidence constitutes Criminal Justice Information (CJI), so any solution must conform to the FBI CJIS Security Policy as administered by the Texas Department of Public Safety. The Department must also be able to document the capabilities and limitations of any AI system it deploys, consistent with Texas H.B. 149 (the Texas Responsible Artificial Intelligence Governance Act).

1.3.Non-Binding Nature

This RFI is for informational purposes only and is not a solicitation or guarantee of future procurement. Responses to this RFI will not result in contractual obligations for the City of Dallas, nor will they provide any advantage or disadvantage in any subsequent procurement process.

2. Meeting Schedule, Questions, and Inquiries

Proposers may view pre-solicitation meeting details, site visit details, and submit their questions electronically through the City solicitation portal,

<https://dallascityhall.bonfirehub.com/opportunities/>

During the solicitation process proposers are required to limit their communication regarding this project to the Buyer referenced herein. A pre-solicitation meeting will be held by the City whereby the proposers will have an opportunity to ask the requesting department(s) questions and/or obtain clarification. The pre-solicitation meeting will be the only time when proposers and requesting department(s) will communicate directly, thereafter, all communication associated with this project shall be addressed to the assigned Buyer.

All questions shall be submitted electronically; the City will respond to all questions by way of an addendum which will be posted as part of the solicitation. The City, its agents, and employees shall not be responsible for any information given by way of verbal communication.

3. Information Requested — Platform Capabilities

Respondents should address each numbered item below, stating whether the capability is generally available today and describing how it works.

3.1 AI architecture and data containment

3.1.1 Identify each AI model the platform uses for transcription, computer vision, and language analysis; state who operates each model and where it runs. Indicate whether the vendor can certify in writing that all inference occurs within the vendor's own accredited security perimeter. If any evidence content is processed by a third-party AI service, including a government-cloud instance of a commercial service, state whether that service's terms permit prompt retention or provider human review (for example, default abuse monitoring).

3.1.2 State whether the vendor operates self-hosted models for evidence processing, meaning model weights running on infrastructure under the vendor's direct control, and describe how model updates are controlled and documented.

3.1.3 AI audit trail. Describe the log kept of AI interactions: who initiated each one, which model processed it, what evidence was involved, and when. This record should be retained for the life of the case and exportable on request.

3.1.4 All equipment, services, infrastructure, and other vendor's technologies, including outsourced platforms, must be in compliance with: the State of Texas - Covered Applications and Prohibited Technologies: <https://dir.texas.gov/information-security/covered-applications-and-prohibited-technologies>.

3.1.5 FCC List of Equipment and Services Covered by Section 2 of The Secure Networks Act

3.2 Evidence type coverage

3.2.1 Audio and jail calls. Automatic transcription with word-level timestamps and speaker separation. Multilingual transcription of 90+ languages, including calls in which speakers switch language mid-call. Per-channel analysis of two-party correctional recordings at production volume, with telephony-provider metadata and warrant-return records layered on so that correspondence can be filtered and searched by that metadata. Describe safeguards for accuracy on poor-quality recordings, such as voice-activity detection ahead of transcription and use of more than one transcription engine with automatic fallback.

3.2.2 Video. Transcription of spoken audio, scene detection, object detection and tracking.

3.2.3 Images. Captioning and scene classification, object and license-plate detection, text recognition (OCR), and location mapping from EXIF data.

3.2.4 Documents and PDFs. Full-text extraction, including scanned and password-protected files, and question answering over document content. Ability to handle PDFs over 200,000 pages with full citations and verifiability.

3.2.5 Spreadsheets and CSV. The Department is interested in analytical capability, as distinct from text extraction: (a) automatic layout detection, including multi-tab workbooks and more than one data region per sheet; (b) plain-language queries computing totals, groupings, and

joins across data sets; (c) fuzzy matching that connects near-miss names, phone numbers, and identifiers across files.

3.2.6 Unified search. A single search across all evidence types combining keyword and semantic retrieval, with confidence filtering.

3.2.7 Scale and ingestion. State the largest case the platform supports in the ordinary course; the Department expects support for at least 5 TB and 3 million files in a single case, with standard processing complete within 24 hours of upload. Describe handling of nested archives and whether folder structure from the original upload is preserved for organizing and isolating review.

3.2.8 Call Detail Records with Cell-Site Location Information from all major cellular telephone companies to include, ATT, Dish Network, T-Mobile, & Verizon.

3.2.9 Digital Search Warrant Data Returns - ingestion of search warrant returns from all major social media, web, communication, and other electronic companies.

3.2.10 Banking Records (in PDF, image, and CSV formats) from all U.S. Domestically Chartered Commercial Banks to include the ingestion, categorization of line items, correlation of related accounts, diagram creation (graph and Sankey), the automated analysis of records using the net worth method, the expenditures method, and the bank deposits method.

3.2.11 Wizard type ingestion - allow investigators to use a combination of OCR, document recognition, and other methods to create the automated ingestion of repetitive organized and unorganized datatypes.

3.2.12 Dataset updates and workflows - a workflow and method to provide continuous updates to dataset ingestion changes, major changes and developments to digital search warrant data returns, and other evidence to include response times.

3.3 **Visual entity analysis**

3.3.1 Detection and clustering of the same face across the images in a case, so that investigators can view every appearance of a person.

3.3.2 A single entity model in which faces, license plates, vehicles, and text regions detected in images and video are searchable alongside transcripts and documents rather than isolated in separate views.

3.4 **Investigative assistance**

3.4.1 Natural-language question answering over case evidence. All AI-produced content (answers, summaries, and derived findings) must be traceable to its source evidence by design. Citations must be finer-grained than the file: the sentence or region of a page within a document, the spreadsheet row, or the audio or video timestamp, with cited rows keeping a stable identity across re-processing.

3.4.2 An assistant that retains an investigator's corrections and case context across sessions, so that knowledge accumulates over the life of a case rather than being restated in each conversation.

3.4.3 Automatic linking of people, phone numbers, vehicles, and locations into a case-level relationship view.

3.4.4 Deconfliction ability to automatically notify investigators of case overlaps to include any uniquely identifiable PII, numbers, social media identifiers, vehicles, Modus Operandi, and other forms of investigative leads.

3.4.5 Additional ability to import overlapping data into case file automatically without reingestion.

3.4.6 One click export for entire case that includes any and all utilization of the platform, all supporting documentation/evidence, and any and all related evidence in compliance with the Richard Miles and Micheal Morton Act.

3.4.7 Automated exportation of data onto forms provided by the department, courts, or other criminal justice related documents. This should include arrest warrant and arrest affidavit forms, search warrant forms, subpoenas, prosecution reports, and the ability to ingest any form to overlay exportable data in an automated workflow.

3.5 Security, compliance, and auditability

3.5.1 Alignment with FBI CJIS Security Policy v6.0 (the auditable baseline since October 1, 2025), as administered by the Texas Department of Public Safety, including the vendor's plan for the October 2027 full-compliance deadline and the CJIS Security Awareness training status of personnel with CJI access.

3.5.2 Documentation of AI capabilities, limitations, and intended use suitable for the Department's obligations under Texas H.B. 149, with sample plain-language text the Department could use to disclose AI use to the public.

3.5.3 Audit and integrity controls: attributable logging of evidence downloads and export-link redemptions; cryptographic integrity verification of evidence files (SHA-256 or equivalent); immutable originals, with AI outputs stored as labeled derivations; single sign-on with enforced multi-factor authentication.

3.5.4 Data-layer safeguards in production today, with time in service for each: tenant isolation between agencies enforced in the data layer rather than only in application code; column-level access controls distinguishing CJI from non-CJI fields; automatic malware screening of uploads, with quarantine that blocks flagged originals from download or streaming while preserving them for forensic purposes.

3.5.5 Available CJIS sponsor agency who can discuss user background checking and authentication protocols.

3.5.6 AI Sandboxing by design – all AI models applied to agency data must be provided through the cloud hosting service (e.g., Amazon Bedrock) or self-hosted open-source models. No criminal justice information sent to external parties, even with non-training contracts.

3.5.7 Ability to audit that the Detectives have verified the information prior to producing any reports or documents.

3.5.8 Support the use of Single Sign-on for client login (Okta preferred)

3.6 Interoperability

3.6.1 Ingestion of evidence exported from the Department's existing systems, including Axon Evidence.com, Peregrine, mobile forensic extractions (Cellebrite UFDR and Magnet

AXIOM exports, with their attachments), and correctional call platforms, without requiring their replacement.

3.6.2 Ingestion of data from department and vendor relational databases, NoSQL Databases, buckets, blobs, API's and other common datasets.

3.6.3 Ingestion of open data portals for the City of Dallas (including open GIS data), all surrounding available cities and counties, and State of Texas Open Data portals. <https://data.texas.gov/>

3.7 Support and product feedback

3.7.1 In-product mechanism for users to report a problem from the page where it occurred, transmitting the report and its session context to the vendor's engineering organization, with tracked resolution. Identify the support channel the Department would use.

3.7.2 A guaranteed response time along with a response framework that guarantees resolution of incidents or requests.

3.8 Executive Summary

3.8.1 Ability to create an executive summary for high profile cases. (PowerPoint, Google Slides, Apple Keynote, etc.).

3.8.2 Ability to edit and splice video to provide a video synopsis of the event.

4. Response Format

- Part A — Company introduction: contact information, company background, relevant law-enforcement deployments, references.

- Part B — Capability statement: item-by-item response to Sections 3.1 through 3.7, indicating whether each capability is generally available, in release, or planned (with date); key personnel.

- Part C — Experience: deployments of similar scope at comparable agencies, with outcomes.

- Part D — Business size & organization: business size standards and organization type.

- Part E — Scope-of-work comments: comments on the scope described in Section 3, and compliance documentation (CJIS alignment summary, H.B. 149 documentation sample, and the written certification described in 3.1.1 if available).

5. Administrative Provisions

Responses must be submitted electronically through the City of Dallas portal by the due date above, as a PDF named for the responding firm; no hard-copy submissions will be accepted. Questions must be submitted through the portal and are answered by posted addendum. Acknowledgement of receipt will not be made, and the City makes no implied or actual contract by issuing this RFI. Costs of response preparation are the responsibility of the respondents, and information received may or may not be used to develop a future solicitation. Do not submit material requiring a non-disclosure agreement. Responses are subject to the Texas Public Information Act.