REQUEST FOR PROPOSAL

Enterprise Land Records Processing, Title Plant Hosting, AI Keying, Abstracting, and Workflow Platform

RFP Number: WE-952-1543

Issued By: We Collective

Submission Email: rfps@wecollective.us

Initial Submission Due: 7/25/26 22:59 CST

Anticipated Budget Range: $5,000,000 to $10,000,000

Restricted Communications Notice: Vendors must follow the communication rules in this RFP. Unauthorized outreach will not improve a vendor's standing and may negatively affect responsiveness.

Document Contents

- RFP control sheet and placeholders
- Official communication and restricted contact rules
- Procurement process and shortlist schedule
- Executive overview and business objectives
- Scope of services and platform requirements
- Local AI Keyer, OCR, handwriting, and image enhancement requirements
- SFTP transaction, bot retrieval, intake, and audit requirements
- Title plant, search, order desk, abstracting, and reporting requirements
- Security, compliance, infrastructure, implementation, and acceptance criteria
- Vendor submission instructions, evaluation criteria, and response attachments

1. RFP Control Sheet

The following table establishes the primary administrative values for this procurement. Bracketed fields are intentionally left blank for completion by the issuing entity before publication.

Control Item	Value
RFP Title	Enterprise Land Records Processing and Title Plant Platform
RFP Number	WE-952-1543
Issuing Entity	We Collective, LLC
Issuing Entity Address	407 W. Covell Rd. Edmond OK 73012
Procurement Contact Email	rfps@wecollective.us
RFP Release Date	7/9/26
Initial Written Submission Due Date and Time	7/25/26
Shortlist Notification Date	8/25/26
Shortlisted Vendor Meeting Window	8/16-26 – 9/16/26
Final Presentation Due Date	3 weeks after
Anticipated Award Date	11/1/2026
Anticipated Implementation Start	1/1/2027
Anticipated Budget Range	$5,000,000 to $10,000,000
Proposal Validity Period	12/31/26
Submission Method	Email complete submission package to rfps@wecollective.us in pdf format. No other submission methods will be accepted.

2. Official Communication and Vendor Conduct Rules

These rules are mandatory. A vendor that cannot comply with the communication, submission, confidentiality, and procurement integrity rules may be found non-responsive or removed from consideration at the issuing entity's sole discretion.

2.1 Single Official Submission Channel

- **All initial RFP submissions must be sent to:** rfps@wecollective.us.
- The subject line should include: RFP Submission - WE-952-1543
- Vendors are responsible for confirming that all required files are complete, readable, and received before the stated deadline.
- The issuing entity is not responsible for blocked messages, late delivery, corrupted attachments, missing attachments, oversized files, or vendor email system failures.

2.2 Communication Blackout Prior to Shortlist

Before shortlist selection, vendors must not send questions, clarification requests, meeting requests, sales materials, informal proposals, calls, texts, social media messages, direct messages, or indirect communications to the issuing entity or its representatives regarding this RFP, except for the formal submission package sent to rfps@wecollective.us.

- No questions or emails will be responded to before the shortlisted vendor meeting stage.

- No phone calls, texts, direct messages, or informal discussions will be accepted before the shortlisted vendor meeting stage.
- No vendor will receive an advantage from attempting to communicate before the scheduled process allows questions.
- Continuing to reach out will not help a vendor receive an award and may be documented as a violation of the procurement process.
- The issuing entity may disregard, archive, or record prohibited communications without responding.
- Any attempt to influence, lobby, pressure, or bypass the stated process may result in disqualification.

2.3 Shortlisted Vendor Questions

After the initial written submission review, ten vendors will be selected for follow-up meetings. Questions will be addressed only during those scheduled meetings or through a formal written addendum issued by the issuing entity.

- Shortlisted vendors may ask questions during their scheduled meeting.
- The issuing entity may, at its discretion, summarize material clarifications and issue them to all shortlisted vendors in a written addendum.
- Oral statements are not binding unless later confirmed in a written addendum.
- After the scheduled meeting, each shortlisted vendor will be allowed three weeks to create a presentation and updated proposal response.
- Unscheduled questions after the meeting period may not be answered unless the issuing entity determines that a formal addendum is necessary.

2.4 Procurement Integrity Rules

- Vendors must not offer gifts, entertainment, compensation, referral payments, commissions, or any thing of value in connection with this RFP.
- Vendors must disclose any actual or potential conflicts of interest, including relationships with employees, consultants, subcontractors, or advisors connected to the issuing entity or the project.
- Vendors must not misrepresent product capabilities, staffing, intellectual property ownership, security posture, local infrastructure readiness, AI model maturity, document throughput, or implementation capacity.
- Vendors must identify all subcontractors and third-party technology providers expected to participate in the solution.
- Vendors must maintain confidentiality of the RFP materials, any related data, and any information learned through meetings or demonstrations.
- Vendors must not publicly announce, market, or reference participation in this RFP without written authorization.

2.5 Required Initial Submission Overview

As part of the initial written submission, each vendor must provide a concise but meaningful overview of the proposed project approach. This overview will be used to determine whether the vendor has the financial, staffing, technical, and operational capacity to be considered for the shortlist. Vendors must not submit questions, clarification requests, or separate communications with this overview; questions will be reserved for the scheduled shortlisted vendor meetings.

- Estimated budget or budget range for the proposed solution, including major assumptions, exclusions, payment milestone concepts, and whether the proposal is intended to cover the full program or only a defined phase.

- Estimated number of people assigned to the project, including the proposed team structure and the specific roles each person or group will perform.
- Required roles should be identified at a minimum for executive sponsorship, project management, solution architecture, infrastructure, AI/OCR and handwriting recognition, data engineering, application development, SFTP intake, bot retrieval automation, quality assurance, security/compliance, implementation, training, and post-launch support.
- Estimated time to complete in months, including the anticipated total duration and any recommended phases such as discovery, architecture, build, configuration, data migration, AI training, testing, pilot launch, production launch, and stabilization.
- Scope of work overview describing what services, deliverables, software components, infrastructure work, AI model work, integrations, document intake methods, bot retrieval work, testing, training, support, and project management services are included.
- Identification of major assumptions, dependencies, customer responsibilities, required access, required sample data, known risks, items excluded from scope, and any third-party technology or subcontractor dependencies.
- The initial overview does not replace the detailed proposal required from shortlisted vendors. It is intended to establish responsiveness, capacity, realism, and project fit before follow-up meetings are scheduled.

3. Procurement Process and Timeline

The procurement process is structured to first identify vendors with the technical, operational, and financial capacity to deliver an enterprise-scale land records and title plant platform, and then to allow a focused question-and-presentation phase for a smaller group of vendors.

Phase	Milestone	Target Date	Description
Phase 1	RFP issued	[INSERT DATE]	RFP released to vendors. Vendors review requirements and prepare initial written responses.
Phase 2	Initial written submission due	[INSERT DATE AND TIME]	Complete submissions must be emailed to rfps@wecollective.us. No questions will be answered before the shortlist stage.
Phase 3	Administrative and technical responsiveness review	[INSERT DATE RANGE]	Issuing entity reviews completeness, compliance, minimum qualifications, and technical alignment.
Phase 4	Selection of ten shortlisted vendors	[INSERT DATE]	Ten vendors will be selected for follow-up meetings. Selection does not guarantee award.
Phase 5	Shortlisted vendor meetings	[INSERT DATE RANGE]	Scheduled meetings will be used to answer questions, clarify scope, and allow the issuing entity to evaluate vendor understanding.
Phase 6	Presentation development period	Three weeks after each shortlisted vendor meeting	Shortlisted vendors prepare formal presentations and updated proposal materials.
Phase 7	Vendor presentations	[INSERT DATE RANGE]	Shortlisted vendors present final technical solution, implementation approach, staffing, risk controls, and commercial model.
Phase 8	Final evaluation and award	[INSERT TARGET DATE]	Issuing entity may select a vendor, enter negotiations, reject all proposals, or revise the procurement.

4. Executive Overview

The issuing entity is seeking proposals from qualified vendors to design, build, configure, deploy, train, support, and scale an enterprise platform for land records ingestion, title plant hosting, document processing, AI-assisted keying, abstracting workflows, order management, reporting, compliance, and secure search access.

The desired solution must operate as a high-volume records platform capable of supporting historical conversion, daily updates, direct electronic intake, automated document retrieval, local AI processing, human review, audit controls, and production search workflows. The platform must be suitable for mission-critical land records and title production environments where data accuracy, traceability, uptime, security, and operational scalability are essential.

The project is not limited to purchasing software licenses. The selected vendor must deliver a complete operating ecosystem, including infrastructure design, local server deployment, data model design, AI/OCR model training, SFTP transaction handling, bot-driven document retrieval, workflow configuration, migration tooling, quality assurance, reporting, support procedures, documentation, and long-term operational readiness.

5. Business Objectives

- Create a centralized platform for receiving, processing, indexing, searching, hosting, and auditing large volumes of land and court-related records.
- Deploy a local-server AI Keyer capable of trained extraction, handwriting interpretation, quality enhancement of poor scans, confidence scoring, exception handling, and continuous improvement through human review.
- Support high-volume processing of forty million records per month where the average document contains five pages, requiring the platform to process approximately two hundred million pages per month at sustained production throughput.
- Automate document intake through secure SFTP transactions, direct file drops, structured manifests, error handling, and bot-based retrieval from authorized source systems.
- Provide title plant search, legal description search, name search, instrument search, image viewing, chain-building, abstracting, examiner notes, quality flags, templates, reports, and export capabilities.
- Establish end-to-end traceability from source receipt through OCR, AI extraction, human review, approval, indexing, publication, search use, report generation, and audit reporting.
- Reduce manual keying, reduce duplicate effort, improve turnaround time, improve document quality, increase search reliability, and support scalable plant operations across multiple jurisdictions or record sources.
- Ensure data ownership, system security, access controls, operational resilience, disaster recovery, and compliance-ready reporting.

6. Anticipated Budget Range

The anticipated budget range for the full program is $5,000,000 to $10,000,000. This range is intended to cover enterprise design, implementation, infrastructure, configuration, training, conversion, AI/OCR enablement, integrations, support readiness, and operational launch activities. Vendors should structure their responses to demonstrate how their proposed approach can deliver the complete scope within the stated budget range.

The issuing entity may negotiate final scope, phasing, milestones, acceptance criteria, staffing, service levels, and commercial terms with the selected vendor. The issuing entity reserves the right to award all, part, or none of the scope.

7. Scope of Services

The selected vendor must provide a comprehensive solution that includes software, infrastructure design, implementation services, data conversion, AI/OCR training, integration development, operational controls, documentation, support procedures, and production launch assistance.

Scope Area	Required Work
Program Management	Project governance, work plan, risk register, decision log, implementation schedule, stakeholder meetings, status reporting, and launch readiness tracking.
Platform Architecture	Target-state architecture, data model, deployment model, network design, local server design, storage architecture, security architecture, backup architecture, and scaling plan.
Local AI Keyer	On-premises or locally controlled AI/OCR system with trained models, handwriting recognition, image enhancement, confidence scoring, validation workflows, and feedback-loop training.
Document Intake	SFTP transactions, bulk imports, manifests, checksum validation, source metadata capture, document normalization, duplicate detection, and error recovery.
Bot Retrieval	Authorized bot framework for retrieving documents from designated sources, managing credentials, schedules, retries, change detection, download receipts, source logs, and chain-of-custody evidence.
Title Plant Search	High-speed search by party, legal description, instrument number, document type, date ranges, book/page, subdivision, tract, parcel identifiers, aliases, and related record associations.
Abstracting and Workflow	Order desk, abstracting queue, chain-building, checklists, flags, notes, review workflows, examiner visibility, templates, document selection, export, and audit trail.
Reporting	Operational dashboards, ingestion reports, indexing reports, QA reports, missing record reports, review reports, throughput reports, exception reports, and compliance-ready reports.
Security and Compliance	Role-based access, privileged access controls, encryption, monitoring, logging, audit retention, incident response, data governance, and user activity reporting.
Training and Support	Administrator training, operator training, abstractor training, model reviewer training, support procedures, knowledge base, runbooks, and post-launch support.

8. Mandatory Platform Capabilities

Vendors must clearly describe whether each capability is available today, requires configuration, requires custom development, requires third-party tooling, or is not available. Responses must include technical detail sufficient to evaluate feasibility, effort, risk, and implementation complexity.

8.1 Core Platform Administration

- Central administration console for organizations, users, roles, permissions, record sources, plant settings, intake rules, queues, templates, integrations, notifications, and audit settings.
- Granular role-based permissions for administrators, plant managers, document intake operators, AI/OCR reviewers, indexers, abstractors, examiners, auditors, support users, and read-only search users.
- Ability to restrict access by jurisdiction, plant, office, customer group, document type, order type, record source, function, export privilege, and administrative privilege.
- Configurable workflow statuses, approval gates, escalation paths, quality-control queues, and exception queues.
- User activity logging, login history, document views, record edits, search activity, export activity, administrative changes, and override events.
- Support for single sign-on or enterprise identity integration if required by the issuing entity.

8.2 Order Desk and Work Intake

- Order creation, intake, assignment, routing, status management, priority levels, deadlines, internal notes, external notes, client references, and document attachments.
- Dynamic status boards, queue filters, bulk actions, reassignment, aging reports, overdue alerts, and operational dashboards.
- Order-to-abstracting workflow integration so searches, chain documents, review notes, compiled records, examiner comments, and exports are connected to the originating order.
- Support for different order types, jurisdictions, product types, custom fields, required checklists, default templates, and team routing rules.
- Ability to track every user action taken on an order, including changes to fields, assignments, status, notes, attachments, selected records, excluded records, reports, and exported files.

8.3 Title Plant Search and Record Access

- Search by grantor, grantee, party name, alias, normalized name, instrument number, document type, book/page, file date, execution date, legal description, lot/block, subdivision, section/township/range, tract, parcel identifier, and other configurable fields.
- High-speed search across very large record sets with filtering, sorting, pagination, saved searches, search history, and exportable result sets.
- Name normalization, alias handling, spelling variants, entity suffix handling, punctuation normalization, OCR confidence handling, and configurable search expansion rules.
- Legal description parsing and matching, including subdivision, block, lot, metes and bounds references, section-township-range values, and jurisdiction-specific variations.
- Instrument association, related document links, chain assistance, release/satisfaction relationships, assignment chains, corrective documents, re-recordings, and source image viewing.
- Full document image viewer with page navigation, thumbnails, zoom, rotate, quality flags, page-level metadata, and reviewer annotations where appropriate.

8.4 Abstracting, Chain-Building, and Reporting

- Abstracting workspace with order details, search tools, selected records, excluded records, notes, examiner notes, flags, checklists, attachments, and chain-building functions.
- Ability to add records from search results into an abstracting chain while preserving source metadata and selected fields.
- Ability to identify possible missing instruments, unresolved releases, unreconciled assignments, broken chains, title gaps, duplicate records, conflicting legal descriptions, and low-confidence extractions.
- Configurable report templates that can generate title evidence, abstract reports, plant reports, search packets, exception reports, review reports, and internal production summaries.
- PDF generation, document package assembly, selected document ordering, cover sheets, signatures, template variables, and audit-linked export records.
- Versioning of reports and templates so prior delivered outputs can be traced back to the data and template version used at the time of creation.

9. Local AI Keyer, OCR, Handwriting, and Image Enhancement Requirements

The AI Keyer is a mandatory local-server requirement. Vendors must not propose a solution that depends on uncontrolled public model processing for production records. The issuing entity expects a locally deployed, locally governed, trained system that can process large volumes of scanned and electronically received documents while improving extraction quality over time.

9.1 Local Server and Deployment Requirements

- The AI Keyer must run on local servers, private infrastructure, or another locally controlled deployment approved by the issuing entity.
- The vendor must design and implement the compute architecture required for OCR, image enhancement, model inference, model training, queue processing, storage, audit logs, and monitoring.
- The vendor must specify GPU, CPU, RAM, storage, network, backup, redundancy, and scaling assumptions in its proposal without relying on public shared AI processing for protected production documents.
- The vendor must provide deployment automation, configuration documentation, monitoring dashboards, restart procedures, capacity planning, patching procedures, and operational runbooks.
- The local AI environment must support development, test, staging, and production separation, or another approved control model that prevents untested model changes from affecting production results.
- The vendor must provide a controlled release process for OCR engine updates, image preprocessing changes, extraction model updates, prompt logic updates, schema changes, and validation-rule changes.
- Customer records must not be used to train external models or public models unless explicitly approved in a written agreement executed by the issuing entity.

9.2 Required Processing Capacity

The solution must be engineered to process forty million records per month. The average document will contain five pages, meaning the system must be designed for approximately two hundred million pages per month. Vendors must explain the architecture, queue design, hardware, parallelization strategy, storage model, retry logic, and monitoring required to sustain this volume.

- The platform must support continuous high-volume intake, OCR, AI extraction, quality improvement, validation, human review, approval, indexing, publication, and reporting without manual file handling bottlenecks.
- The vendor must describe peak-load handling, backlog recovery, queue prioritization, concurrent workers, load balancing, retry policies, failure isolation, and exception routing.
- The vendor must provide a performance testing plan that simulates production-scale records, large page counts, mixed document quality, multiple source batches, duplicate files, corrupted files, missing manifests, and reprocessing events.
- The vendor must identify expected throughput bottlenecks and how they will be solved through additional compute, distributed workers, batching, model optimization, preprocessing optimization, database indexing, caching, or workflow changes.
- The platform must provide real-time and historical dashboards for pages processed, records processed, error rates, exception rates, queue age, average processing time, throughput by source, reviewer workload, approval rates, model confidence, and reprocessing rates.

9.3 Image Quality Enhancement

The vendor must provide automated image enhancement before OCR and AI extraction. The system must improve the usability of poor scans, photographed pages, skewed pages, faint text, heavy noise, bleed-through, low contrast, poor cropping, shadowed scans, warped pages, mixed orientations, and multi-page documents with inconsistent image quality.

- Automatic page orientation detection and correction.
- Deskewing, dewarping, border cleanup, background normalization, contrast enhancement, binarization, denoising, sharpening, and shadow reduction.
- Detection of blank pages, duplicate pages, unreadable pages, rotated pages, truncated pages, mixed-size pages, and pages requiring human review.

- Page segmentation for stamps, marginal notes, handwriting, signatures, legal descriptions, book/page references, indexing stamps, and notary blocks.
- Image quality scoring before and after enhancement so reviewers can understand whether enhancement improved extractability.
- Ability to preserve original image files and enhanced derivative files with traceable links between both versions.
- Manual reviewer tools to view original versus enhanced image, override enhancement settings, request reprocessing, and flag records for specialized review.

9.4 OCR, Handwriting Recognition, and AI Extraction

The AI Keyer must combine OCR, handwriting recognition, document classification, field extraction, validation, normalization, and human review. Vendors should explain their approach to printed text, cursive handwriting, mixed handwriting and typed text, historical documents, stamps, marginalia, indexing references, and jurisdiction-specific formatting.

Capability	Expected Vendor Responsibility
OCR and Text Recognition	Printed text extraction, multi-column handling, page layout analysis, stamp recognition, book/page recognition, legal description reading, and confidence scoring.
Handwriting Recognition	Recognition of handwritten names, dates, legal references, marginal notes, book/page references, initials, notary information, and cursive or historical handwriting where feasible.
Document Classification	Classification by instrument type, recording category, source, jurisdiction, page grouping, cover sheet detection, continuation page detection, and exception category.
Field Extraction	Extraction of grantor, grantee, parties, instrument date, recording date, instrument number, book/page, document type, legal description, subdivision, block, lot, section, township, range, parcel identifiers, consideration references, related instruments, and other configurable fields.
Normalization	Normalization of dates, names, entity suffixes, legal descriptions, instrument references, book/page formats, capitalization, punctuation, and jurisdiction-specific data patterns.
Validation	Schema validation, required-field checks, cross-field consistency checks, duplicate detection, source manifest comparison, legal description parsing checks, confidence thresholds, and exception routing.
Human Review	Reviewer queues, side-by-side source image and extracted data, confidence highlighting, field edits, reviewer notes, supervisor approval, and audit trail.
Continuous Improvement	Feedback loop from reviewer corrections into training datasets, benchmark sets, model evaluation, prompt or model updates, and controlled production deployment.

9.5 Model Training and Governance

- Vendor must create a model-training plan using representative document samples approved by the issuing entity.
- Training must account for modern scans, historical scans, handwritten content, low-quality images, inconsistent record formats, multiple jurisdictions, multiple document types, and source-specific indexing conventions.
- Vendor must establish ground-truth datasets, benchmark datasets, reviewer-correction datasets, and regression test datasets.
- Vendor must define minimum accuracy targets, confidence thresholds, field-level scoring, document-level scoring, and escalation criteria for human review.
- Vendor must support active learning or equivalent processes so corrected records can improve future extraction performance without compromising auditability.

- Vendor must maintain model version history, training dataset lineage, evaluation results, release notes, rollback procedures, and approval records for each model update.
- Vendor must provide tools for subject-matter experts to review difficult examples, correct extractions, approve training examples, and identify recurring source problems.
- Vendor must ensure that model training, evaluation, and production inference remain segregated enough to preserve reliability and prevent unapproved changes.

9.6 Quality Assurance and Exception Handling

- Configurable confidence thresholds by field, document type, source, jurisdiction, and workflow stage.
- Exception queues for low-confidence fields, missing required fields, inconsistent parties, invalid dates, unmatched legal descriptions, unreadable pages, duplicate documents, conflicting book/page references, and records requiring supervisor review.
- Dual-pass or multi-pass extraction options where the system can compare results from different OCR/model strategies and flag disagreements for review.
- Reviewer productivity tools including keyboard shortcuts, field-level highlighting, original image zoom, enhanced image comparison, history of similar corrections, and batch approval where appropriate.
- Quality dashboards for accuracy sampling, reviewer disagreement, source quality, recurring errors, model drift, reprocessing volume, and field-level error patterns.
- Ability to lock approved records from uncontrolled edits while permitting controlled correction workflows with traceable approvals.

10. SFTP Transaction and Document Intake Requirements

The platform must be able to receive documents through secure SFTP transactions and other controlled intake methods. Intake is not simply file transfer; the selected vendor must implement a full transaction framework that validates, normalizes, tracks, reconciles, and audits every document package received.

10.1 SFTP Intake Framework

- Dedicated SFTP locations or folders by source, jurisdiction, customer, plant, batch type, and processing purpose.
- Support for structured batch manifests that identify source, document count, page count when available, recording date ranges, expected file names, hashes, metadata fields, and delivery timestamp.
- Checksum or hash validation to detect incomplete, corrupted, duplicate, or tampered files.
- Automated batch pickup, quarantine, validation, acceptance, rejection, reprocessing, and status reporting.
- Idempotent processing so the same file or batch cannot be accidentally processed multiple times without a controlled override.
- Configurable naming conventions and mapping rules for source files, image files, PDFs, TIFFs, text files, metadata files, and supplemental index files.
- Automated extraction of source metadata from manifests, file names, folder paths, embedded PDF metadata, OCR text, and associated index files.
- Error reports for missing files, extra files, invalid file types, invalid metadata, failed hash checks, unreadable files, unsupported images, and batch count mismatches.
- Outbound SFTP support for acknowledgments, processed records, rejected records, exception reports, status files, exported indexes, report packages, and reconciliation files.

10.2 Intake Processing Pipeline

Pipeline Stage	Required Capability
Receive	Detect incoming batch, capture delivery metadata, lock files for processing, and create a batch audit

Pipeline Stage	Required Capability
	record.
Validate	Validate folder, manifest, file types, counts, hashes, naming conventions, and required metadata.
Normalize	Convert or normalize images where needed, split or combine pages when required, assign document identifiers, and standardize file storage.
Preprocess	Run image enhancement, quality scoring, blank-page detection, orientation correction, and document boundary detection.
Extract	Run OCR, handwriting recognition, classification, AI field extraction, and validation rules.
Review	Route exceptions to human review, supervisor approval, or reprocessing queues based on confidence and validation outcomes.
Index	Publish approved metadata, document images, source references, and search fields to the title plant search environment.
Reconcile	Compare accepted records, rejected records, processed records, missing files, duplicate files, and final counts against source expectations.
Report	Produce batch-level reports, error reports, audit reports, throughput reports, and compliance reports.

11. Bot-Based Document Retrieval Requirements

The selected vendor must provide an authorized bot retrieval framework for collecting documents from designated source systems where automated retrieval is permitted. The bot framework must be designed for reliability, auditability, respectful source access, credential security, scheduling, reconciliation, and exception handling.

11.1 Bot Framework Requirements

- Configurable bots for approved source systems, including web portals, file drops, data feeds, image repositories, and other authorized retrieval channels.
- Credential vault integration or secure credential storage with rotation, access logging, encryption, and least-privilege controls.
- Scheduled retrieval by source, date range, instrument number range, document type, jurisdiction, batch type, or other source-specific parameters.
- Change detection for new records, corrected records, restored records, missing record ranges, replacement images, and updated index data.
- Download queue management, retry logic, throttling, source-specific rate controls, session recovery, page-level error capture, and evidence of attempted retrieval.
- Support for source-specific navigation, search forms, pagination, document viewers, bulk download tools, receipt pages, and image export mechanisms where authorized.
- Logging of source URL or access point, account used, query executed, timestamp, document identifiers, file names, download status, retry count, and final outcome.
- Capture of screenshots, receipts, metadata, or other evidence where needed to demonstrate collection path and support troubleshooting.
- Separation between bot configuration, bot execution, retrieved files, validation results, and downstream AI/OCR processing.
- Controls to prevent bots from violating source restrictions, bypassing security controls, or accessing records outside authorized scope.

11.2 Bot Monitoring and Exception Handling

- Operational dashboards showing bot status, source availability, last successful run, next scheduled run, documents retrieved, failures, retries, queue age, and source-level throughput.
- Alerts for login failures, source layout changes, unexpected page errors, missing search results, download failures, corrupted files, unrecognized formats, and repeated source errors.
- Version-controlled bot scripts or configurations with change approval, test execution, rollback capability, and release notes.
- Bot run history that allows auditors or operators to determine what was searched, what was retrieved, what failed, what was skipped, and what was later corrected.
- Manual override tools allowing authorized users to rerun a bot, retry a failed document, place a source on hold, update source credentials, or move retrieved files into an exception queue.
- Reconciliation reports comparing expected source ranges against retrieved records, accepted records, rejected records, and unresolved exceptions.

12. Data Model, Record Lifecycle, and Auditability

The selected vendor must design or configure a durable data model that preserves original documents, derived images, extracted text, structured metadata, field confidence, reviewer actions, source identifiers, order relationships, audit history, and published search indexes.

- Every record must have a unique platform identifier and retain source identifiers where available.
- Every file must retain original source metadata, receipt timestamp, source channel, batch identifier, file hash, and processing history.
- Every extracted field must support field-level metadata such as source page, source coordinates where available, extraction method, model version, confidence score, reviewer edits, and approval status.
- Every human edit must capture user, timestamp, before value, after value, reason code where required, workflow stage, and approval status.
- Every record must support lifecycle states such as received, validated, preprocessing, extraction, exception, review, approved, indexed, published, corrected, superseded, rejected, and archived.
- Records must support document grouping, page grouping, parent-child relationships, continuation pages, related instruments, re-recordings, corrections, and cross-reference links.
- The platform must support read-only audit views and exportable audit reports suitable for management, compliance, and external review.

13. Security, Privacy, and Infrastructure Requirements

The platform will handle sensitive operational data and large volumes of public-record-derived documents. The selected vendor must implement reasonable enterprise controls appropriate for high-volume, mission-critical records operations.

Area	Required Controls
Access Control	Role-based access, least privilege, user groups, administrative privilege separation, strong authentication options, session management, and access reviews.
Data Protection	Encryption in transit, encryption at rest where applicable, secure file transfer, controlled exports, secure secrets management, and protected backups.
Local AI Protection	Locally controlled model inference and training, restricted model access, model version governance, training-data controls, and prohibition on unauthorized external model training.
Monitoring and Logging	System logs, user logs, security logs, processing logs, bot logs, SFTP logs, model logs, audit logs, alerting, and log retention rules.

Area	Required Controls
Network Security	Firewall design, segmentation, private network paths where applicable, secure administrative access, IP restrictions where needed, and intrusion detection or equivalent monitoring.
Backup and Recovery	Backup schedule, retention, restore testing, disaster recovery objectives, local and redundant storage strategy, and documented recovery runbooks.
Vulnerability Management	Patch management, dependency management, vulnerability scanning, secure software development practices, and remediation tracking.
Incident Response	Incident escalation procedure, notice procedure, containment plan, evidence preservation, root-cause analysis, corrective action plan, and post-incident reporting.

14. Performance, Scalability, and Availability Requirements

- Support sustained processing of the required monthly record and page volume without uncontrolled manual intervention.
- Support parallel document intake, OCR, AI extraction, image enhancement, review, indexing, search, and report generation workloads.
- Support high-speed search over very large record sets with predictable response times and scalable indexes.
- Support growth across additional record sources, jurisdictions, users, plants, document types, and processing rules.
- Support operational monitoring of system health, queue age, failed jobs, processing throughput, disk capacity, database performance, search latency, and model performance.
- Provide capacity planning recommendations and an expansion strategy for additional hardware, compute workers, database nodes, storage volumes, and index partitions.
- Provide planned maintenance procedures, outage communication procedures, rollback procedures, and high-availability design options.

15. Implementation Workstreams

Workstream	Vendor Responsibility
Discovery and Requirements Confirmation	Confirm workflows, record sources, source formats, user roles, intake methods, document types, legal data fields, search expectations, reporting needs, security requirements, and implementation priorities.
Architecture and Infrastructure Design	Design local servers, compute clusters, storage, networking, backups, database architecture, search architecture, AI/OCR deployment, monitoring, and environments.
Data Model and Schema Design	Define record entities, document entities, page entities, extracted fields, legal description fields, party fields, audit entities, workflow entities, and reporting views.
SFTP and Intake Buildout	Configure SFTP folders, manifests, validators, file watchers, acknowledgments, error reports, batch dashboards, and reprocessing rules.
Bot Retrieval Buildout	Configure authorized bots, credentials, schedules, source-specific logic, retry rules, monitoring, receipts, and reconciliation reports.
AI Keyer Training and Deployment	Create training datasets, benchmark sets, image preprocessing, OCR/HTR models, extraction models, validation rules, reviewer queues, model governance, and production release process.
Search and Title Plant Configuration	Configure indexes, filters, legal description search, party search, aliases, instrument relationships, document viewer, saved searches, and search permissions.
Workflow and Reporting Configuration	Configure order desk, abstracting queues, chain tools, checklists, templates, quality flags, dashboards, and compliance reporting.

Workstream	Vendor Responsibility
Migration and Historical Loading	Load legacy data and images, normalize fields, reconcile counts, identify duplicates, run validation reports, and publish approved records.
Testing and Acceptance	Complete unit testing, system testing, integration testing, performance testing, security testing, user acceptance testing, data validation, and launch readiness sign-off.
Training and Go-Live	Train administrators, operators, reviewers, abstractors, examiners, support personnel, and managers; provide runbooks; support production launch.
Post-Launch Support	Provide hypercare, defect triage, queue monitoring, model tuning, knowledge transfer, and stabilization reporting.

16. Required Vendor Deliverables

- Project charter, project schedule, dependency list, risk register, issue log, decision log, and status-report template.
- Solution architecture document covering infrastructure, application architecture, database architecture, AI/OCR architecture, network architecture, security architecture, and deployment architecture.
- Data model documentation including table/entity definitions, field definitions, source mappings, indexes, audit fields, and reporting views.
- SFTP intake design including folder structure, manifest specification, validation rules, acknowledgment formats, exception report formats, and reconciliation procedures.
- Bot retrieval design including source configuration, credential handling, run schedules, retry logic, audit logs, rate controls, monitoring, and exception procedures.
- AI Keyer design including OCR/HTR approach, image enhancement approach, model architecture, training plan, validation rules, confidence scoring, human review workflow, and model governance plan.
- Security plan including access control, encryption, monitoring, logging, backup, disaster recovery, incident response, and vulnerability management procedures.
- Implementation runbook, deployment scripts or procedures, environment configuration guide, administrative guide, operator guide, reviewer guide, abstractor guide, and support guide.
- Test plans and test results for functional testing, integration testing, performance testing, SFTP testing, bot testing, AI/OCR testing, security testing, data migration testing, and user acceptance testing.
- Training materials, recorded training sessions if requested, knowledge-base articles, quick-start guides, and role-specific job aids.
- Go-live checklist, rollback plan, hypercare plan, support escalation matrix, and post-launch stabilization report.

17. Acceptance Criteria

Final acceptance will be based on mutually agreed milestones and objective acceptance criteria. At a minimum, vendors should expect acceptance criteria to include the following categories.

Acceptance Area	Minimum Acceptance Expectation
Functional Acceptance	Required modules operate according to approved requirements, workflows, permissions, configurations, reporting, and user roles.
Data Acceptance	Migrated, received, extracted, reviewed, indexed, and published records reconcile to approved source counts and validation reports.
AI/OCR Acceptance	AI Keyer meets agreed field-level accuracy, document classification, handwriting handling, image enhancement, confidence scoring, and exception routing standards.
Throughput Acceptance	System demonstrates capacity to process the required monthly record and page volume or an

Acceptance Area	Minimum Acceptance Expectation
	approved scaled performance test that proves capacity.
SFTP Acceptance	SFTP transactions validate manifests, handle errors, generate acknowledgments, reconcile batches, and process records through downstream workflows.
Bot Acceptance	Authorized bots retrieve documents reliably, log activity, handle errors, reconcile source ranges, and route retrieved documents into the intake pipeline.
Search Acceptance	Search results are accurate, performant, filterable, auditable, and usable by authorized users for production workflows.
Security Acceptance	Access controls, logging, local AI controls, backups, monitoring, and incident procedures satisfy agreed security requirements.
Training Acceptance	Administrators, operators, reviewers, abstractors, and support users receive usable training and documentation.
Operational Readiness	Support procedures, monitoring dashboards, runbooks, escalation paths, and hypercare procedures are in place before production launch.

18. Vendor Minimum Qualifications

- Demonstrated ability to deliver enterprise software for high-volume document processing, records management, legal records, title plant operations, workflow automation, or similarly complex domains.
- Demonstrated experience with OCR, handwriting recognition, image enhancement, AI-assisted extraction, human review workflows, and structured data validation.
- Demonstrated ability to deploy and support locally controlled infrastructure, including secure server environments, storage, monitoring, backups, and scaling.
- Demonstrated ability to build secure SFTP transaction frameworks, ingestion pipelines, file validation, batch reconciliation, and error handling.
- Demonstrated ability to build or operate authorized automation/bot frameworks for document retrieval, source monitoring, download management, and audit logging.
- Demonstrated project management discipline with formal schedules, risks, issues, documentation, testing, training, go-live support, and executive reporting.
- Ability to provide qualified staff for architecture, development, AI/OCR, data engineering, quality assurance, security, implementation, training, and support.
- Financial and operational capacity to complete a multi-workstream enterprise implementation and provide post-launch support.

19. Proposal Submission Requirements

Vendors must submit a complete initial written response by the due date listed in the control sheet. Submissions must be emailed to rfps@wecollective.us. The issuing entity may reject incomplete, late, unreadable, non-compliant, or materially evasive submissions.

19.1 Required Initial Submission Package

#	Required Section	Expected Content
1	Executive Summary	Concise summary of proposed solution, differentiators, implementation approach, and ability to meet the requirements.
2	Company Profile	Legal name, headquarters, ownership summary, years in operation, relevant experience, project team, and subcontractors.

#	Required Section	Expected Content
3	Relevant Experience	Comparable projects, document volumes, AI/OCR experience, local deployments, SFTP intake, bot retrieval, and title or land records experience if applicable.
4	Technical Solution	Detailed architecture, modules, AI Keyer design, local server design, data model, workflows, integrations, security, reporting, and scalability approach.
5	Implementation Plan	Workstreams, phases, timeline, staffing model, dependencies, client responsibilities, training, testing, go-live, and post-launch support.
6	AI Keyer Plan	Local AI deployment, OCR/HTR approach, image enhancement, model training, throughput plan, quality assurance, confidence scoring, and governance.
7	SFTP and Bot Plan	SFTP transaction model, manifest handling, source retrieval bots, monitoring, reconciliation, exception handling, and audit records.
8	Security and Compliance Response	Access controls, encryption, logging, monitoring, local AI controls, backups, incident response, and data governance.
9	Commercial Response	Commercial structure aligned with the stated budget range, assumptions, payment milestones, included services, excluded services, and ongoing support model.
10	Exceptions and Assumptions	All exceptions to the RFP, assumptions, requested deviations, third-party dependencies, and risks.
11	References	References for comparable enterprise implementations, preferably involving high-volume document processing and local infrastructure.
12	Signed Vendor Certifications	Compliance with communication rules, confidentiality, non-collusion, conflict disclosure, and accuracy of response.

19.2 File and Format Rules

- Submit one complete PDF copy of the response unless another format is requested in writing.
- Submit editable versions of required attachments if templates are provided by the issuing entity.
- Use the file naming convention: [INSERT FILE NAMING CONVENTION].
- Do not include executable files, password-protected files, links requiring registration, or links that expire before evaluation is complete.
- Do not rely on marketing websites or generic brochures as substitutes for direct answers to the RFP requirements.
- Label any trade-secret or confidential sections clearly. The issuing entity is not required to accept overbroad confidentiality markings.
- All claims regarding capabilities, throughput, AI performance, security, local infrastructure, or implementation timing must be supportable and may be tested during evaluation.

19.3 Required Compliance Matrix

Vendors must include a compliance matrix responding to each major requirement. Acceptable response statuses are: Available Now, Configurable, Custom Development Required, Third-Party Dependency, Not Available, or Exception Taken. Vendors must not mark a requirement as available unless it can be demonstrated in a working environment.

Requirement ID	Requirement Summary	Vendor Status	Explanation / Evidence / Exception
AI-001	AI Keyer runs on local servers or locally controlled infrastructure.	[INSERT VENDOR RESPONSE]	[INSERT DETAILS]
AI-002	System supports trained extraction models	[INSERT VENDOR	[INSERT DETAILS]

Requirement ID	Requirement Summary	Vendor Status	Explanation / Evidence / Exception
	with field-level confidence scoring.	RESPONSE]	
AI-003	System supports handwriting recognition and poor-scan enhancement.	[INSERT VENDOR RESPONSE]	[INSERT DETAILS]
PERF-001	System supports required monthly records and page volume.	[INSERT VENDOR RESPONSE]	[INSERT DETAILS]
SFTP-001	System supports full SFTP transaction processing with manifests, validation, acknowledgments, and reconciliation.	[INSERT VENDOR RESPONSE]	[INSERT DETAILS]
BOT-001	System supports authorized bot retrieval with monitoring, credentials, retries, logs, and reconciliation.	[INSERT VENDOR RESPONSE]	[INSERT DETAILS]
PLANT-001	System supports high-speed title plant search across party, legal, instrument, date, and document fields.	[INSERT VENDOR RESPONSE]	[INSERT DETAILS]
WF-001	System supports order desk, abstracting, review queues, flags, notes, and report generation.	[INSERT VENDOR RESPONSE]	[INSERT DETAILS]
SEC-001	System supports role-based access, audit logging, encryption, monitoring, and incident response.	[INSERT VENDOR RESPONSE]	[INSERT DETAILS]

20. Shortlisted Vendor Meeting and Presentation Requirements

After initial written responses are reviewed, ten vendors will be selected for follow-up meetings. Shortlisted vendors should be prepared to discuss technical architecture, scope, risks, implementation plan, assumptions, staffing, AI Keyer design, local infrastructure, SFTP intake, bot retrieval, throughput, search, workflows, security, and support.

- Meetings will be scheduled by the issuing entity. Vendors must not attempt to force, bypass, or expand the meeting process through separate communications.
- Questions may be asked during the scheduled meeting. The issuing entity may choose to answer orally during the meeting, issue a written addendum, or decline to answer.
- After the scheduled meeting, each shortlisted vendor will have three weeks to create a formal presentation and updated proposal package.
- The final presentation should include a solution overview, system architecture, local AI Keyer demonstration or design, sample workflows, implementation plan, risk plan, staffing plan, security approach, support model, and commercial structure.
- The issuing entity may request demonstrations, technical deep dives, architecture diagrams, security documentation, references, proof-of-concept tasks, or additional clarifying materials from shortlisted vendors.

21. Evaluation Criteria

The issuing entity will evaluate proposals based on overall responsiveness, capability, feasibility, risk, technical merit, operational fit, implementation confidence, and value. The issuing entity is not obligated to select the lowest-cost proposal or any proposal.

Evaluation Area	Evaluation Considerations
Technical Fit	Ability to meet functional, technical, AI/OCR, SFTP, bot, search, workflow, reporting, data, and security requirements.
AI Keyer Strength	Local deployment, trained models, handwriting recognition, scan enhancement, model governance, accuracy approach, throughput plan, and human review design.
Implementation Confidence	Project plan, staffing, methodology, timeline realism, dependencies, testing, migration, training, go-live, and risk controls.
Scalability and Performance	Ability to support required record/page volume, search scale, processing queues, data growth, and future expansion.
Security and Compliance	Controls for access, data protection, local AI, audit logging, monitoring, incident response, backups, and data ownership.
Relevant Experience	Comparable work in high-volume records, legal records, AI/OCR, local infrastructure, workflow software, bot retrieval, and enterprise integrations.
Operational Support	Support model, training, documentation, runbooks, monitoring, service procedures, and post-launch stabilization.
Commercial Alignment	Alignment with the stated budget range, value, scope coverage, assumptions, and long-term support approach.
Presentation and Demonstration	Clarity, credibility, evidence, ability to answer questions, and ability to demonstrate or explain the proposed solution in depth.

22. General Terms and Rights Reserved

- The issuing entity reserves the right to reject any or all proposals, waive informalities, request clarification, negotiate with one or more vendors, cancel the RFP, revise the RFP, or issue a new RFP.
- This RFP does not create a contract, commitment to purchase, or obligation to reimburse vendor expenses.
- All costs of proposal preparation, participation, demonstrations, meetings, travel, and presentations are the sole responsibility of the vendor.
- The issuing entity may verify any statement made in a proposal and may consider inaccurate, incomplete, or misleading statements as grounds for rejection or disqualification.
- The issuing entity may require proof of insurance, cybersecurity controls, financial capability, personnel qualifications, background checks, or other documentation before award.
- The issuing entity may require the selected vendor to execute a master services agreement, confidentiality agreement, data protection agreement, security addendum, service level agreement, implementation statement of work, and other required contract documents.
- The issuing entity will own or control its data, source records, images, metadata, extracted data, reviewer corrections, audit logs, reports, and business workflows as specified in the final agreement.
- Vendor intellectual property, third-party components, open-source components, model dependencies, and licensing restrictions must be disclosed before award.
- Vendors must identify any part of the solution that depends on external systems, hosted services, third-party AI providers, third-party OCR providers, data processors, subcontractors, or proprietary components that could affect operations or data rights.

23. Appendix A - Vendor Certification Form

The undersigned vendor certifies that it has read the RFP, agrees to comply with the communication rules, has not engaged in prohibited communications, has disclosed known conflicts of interest, and has submitted accurate information to the best of its knowledge.

Field	Vendor Response
Vendor Legal Name	
Primary Contact Name	
Primary Contact Email	
Primary Contact Phone	
Authorized Signatory Name	
Authorized Signatory Title	
Signature	
Date	

24. Appendix B - Conflict and Subcontractor Disclosure

Vendors must disclose conflicts, subcontractors, third-party technology providers, external AI/OCR dependencies, hosting dependencies, and any material relationship that could affect evaluation, performance, data rights, or project independence.

Disclosure Category	Vendor Response
Actual or potential conflict of interest	
Subcontractors	
Third-party AI/OCR providers	
Third-party hosting or infrastructure providers	
Open-source or restricted-license components	
External data processors	
Known implementation dependencies	
Known risks or exceptions	

25. Appendix C - Initial Vendor Questionnaire

Vendors should answer the following questions directly. Answers may be summarized in the main response and expanded in attachments.

1. Describe the most comparable enterprise records, legal records, or high-volume document processing platform your company has delivered.

   [INSERT VENDOR ANSWER]

2. Describe your approach to local-server AI deployment and the hardware architecture you recommend for the required processing volume.

   [INSERT VENDOR ANSWER]

3. Describe how your AI Keyer reads handwriting, recognizes difficult scans, improves image quality, and routes uncertain results to human reviewers.

[INSERT VENDOR ANSWER]

4. Describe how your system trains or fine-tunes extraction models using corrected records while preserving auditability and preventing unapproved production changes.

   [INSERT VENDOR ANSWER]

5. Describe how you would process forty million records per month with an average of five pages per document.

   [INSERT VENDOR ANSWER]

6. Describe your SFTP transaction framework, including manifests, acknowledgments, checksum validation, batch reconciliation, duplicate prevention, and error handling.

   [INSERT VENDOR ANSWER]

7. Describe your bot retrieval framework, including authorization controls, credentials, scheduling, retries, monitoring, rate controls, logs, and reconciliation.

   [INSERT VENDOR ANSWER]

8. Describe how your title plant search handles names, aliases, legal descriptions, document types, instrument references, book/page values, and document images.

   [INSERT VENDOR ANSWER]

9. Describe how your abstracting workflow connects orders, searches, records, chains, notes, flags, checklists, examiner comments, templates, and exports.

   [INSERT VENDOR ANSWER]

10. Describe the data ownership, audit logging, security, backup, disaster recovery, and incident response controls included in your solution.

    [INSERT VENDOR ANSWER]

11. Describe your implementation team, roles, expected timeline, client responsibilities, training plan, launch plan, and post-launch support plan.

    [INSERT VENDOR ANSWER]

12. Identify the largest risks in this project and explain how your company would reduce those risks.

    [INSERT VENDOR ANSWER]

26. Appendix D - Draft Requirement Categories for Vendor Response

The following requirement categories should be used by vendors to organize a detailed compliance response. The issuing entity may expand or refine these categories before publication.

Category Code	Requirement Category
ADMIN	Administration, user management, role-based access, organization management, settings, notifications, and audit views.
ORDER	Order desk, intake, queues, statuses, assignments, notes, attachments, client references, and workflow routing.
INTAKE	SFTP, direct upload, batch import, manifests, validation, normalization, duplicate detection, and reconciliation.
BOT	Authorized bot retrieval, credentials, scheduling, source-specific logic, monitoring, logs, retries, and source reconciliation.
AI	Local AI Keyer, OCR, handwriting recognition, image enhancement, field extraction, classification, confidence scoring, and training.
DATA	Data model, source records, images, extracted text, structured metadata, audit history, corrections, and

Category Code	Requirement Category
	lifecycle states.
SEARCH	Title plant search, party search, legal search, instrument search, document viewer, filters, saved searches, and performance.
ABSTRACT	Chain-building, selected records, excluded records, notes, flags, checklists, examiner notes, report generation, and exports.
REPORT	Dashboards, operational reporting, QA reporting, exception reporting, source reporting, audit reporting, and compliance reporting.
SECURITY	Access, encryption, logging, monitoring, local AI controls, backups, incident response, vulnerability management, and data governance.
IMPLEMENT	Project governance, migration, configuration, testing, training, go-live, hypercare, documentation, and support.

27. Appendix E - Publication Checklist for Issuing Entity

Before distributing this RFP, the issuing entity should complete the following fields and confirm that all placeholders are accurate.

- Insert issuing entity legal name and address.
- Insert RFP number.
- Insert release date.
- Insert initial submission due date, time, and time zone.
- Insert shortlist notification target date.
- Insert shortlisted vendor meeting window.
- Insert final presentation due date convention or date.
- Insert anticipated award date.
- Insert implementation start target.
- Insert required subject line and file naming convention.
- Insert proposal validity period.
- Review whether an NDA is required before releasing additional technical materials.
- Review whether a separate technical appendix, data sample, diagram package, or architecture questionnaire will be issued to shortlisted vendors.
- Review final legal terms with counsel before publication.

End of Request for Proposal Draft