

TECHNICAL SPECIFICATIONS AND SCOPE OF WORK

Tenders are invited on-line on the website <https://gem.gov.in> from the identified Bidders. The registration should be in the name of bidder for Individual, Proprietorship firm, Partnership firm, Company registered under Companies Act or any other legal entity registered in India.

Technical Specifications and Scope of Work: Design, Development, Implementation and Maintenance of an AI-assisted Tender Evaluation Solution for Coal India Limited, including maintenance and support for five (5) years.

1. INTRODUCTION

Description of work	EMD Amount	Period of Contract
Design, Development, Implementation and Maintenance of AI-assisted Tender Evaluation Solution for Coal India Limited	₹ 18,55,000	Implementation: T + 240 days Maintenance & Support: 5 years from date of Go-Live (Payment and Deliverables shall be governed as per Clause No. 5)

Note: The estimated cost indicated above is inclusive of solution design and implementation, cloud infrastructure and licences for the entire contract period, change management man-days, onsite support and bid processing charges as detailed in the Bill of Quantities (BoQ). The number of bids indicated in the BOQ is tentative and has been estimated for a period of five years. There shall be no minimum commitment with regard to the number of bids. In the event of an increase in the number of bids beyond the tentative quantity indicated in the BOQ, the SI shall process such additional bids at the same rates as quoted in the BOQ.

2. BACKGROUND

A. Coal India Limited (CIL), a Maharatna Public Sector Undertaking under the Ministry of Coal, Government of India, is the single largest coal producing company in the world. CIL, which came into being in November 1975, operates through seven producing subsidiaries:

- a) Eastern Coalfields Limited (ECL)
- b) Bharat Coking Coal Limited (BCCL)
- c) Central Coalfields Limited (CCL)
- d) Western Coalfields Limited (WCL)
- e) South Eastern Coalfields Limited (SECL)
- f) Northern Coalfields Limited (NCL)
- g) Mahanadi Coalfields Limited (MCL)

CIL also has Central Mine Planning & Design Institute (CMPDI), a specialized mine planning and consultancy subsidiary.

Coal India Limited (CIL), together with its subsidiaries, undertakes procurement of goods, works and services through e-procurement portals in accordance with the CIL Procurement Manuals, the General Financial Rules and the guidelines issued by the Government of India from time to time.

B. CIL and its subsidiaries publish approximately 3000 tenders per annum, against which an average of approximately 7-8 offers are received per tender, aggregating to approximately 25,000 bids processed per annum. Each bidder submits multiple documents in support of eligibility, technical and commercial requirements of the Notice Inviting Tender (NIT).

C. On receipt of offers, the Dealing Officer of the Tender Inviting Authority / Contract Management Cell is required to download the offer documents, read each document against the eligibility and technical criteria stipulated in the NIT, and compile the extracted particulars into a tabular format known as the Comparative Statement, which forms the basis of the Tender Committee Report (TCR). This activity is repetitive, document-intensive and is the most time-consuming step in the tender finalisation cycle.

D. CIL intends to deploy an AI-assisted solution to automate the repetitive and mechanical portion of this activity, namely the reading of offer documents, extraction of the particulars required by the NIT, and preparation of a draft Comparative Statement, so as to reduce the time taken by the Dealing Officer in preparing the comparative statement and consequently to expedite the procurement cycle.

E. The objective of the project is limited to assisting the Dealing Officer in the preparation of the draft Comparative Statement and connected draft outputs. The solution shall not determine, decide or recommend the acceptance or rejection of any offer. All evaluation decisions shall continue to be taken by the Tender Committee and the competent authority in accordance with the extant Manuals of CIL. The measurable deliverable of the project is the reduction in time taken to prepare the Comparative Statement.

F. CIL therefore invites bids from experienced bidders (hereinafter referred to as the "System Integrator" or "SI") having in-house capability to design, develop, deploy and maintain such solutions, on a MeitY-empanelled Cloud Service Provider (CSP) infrastructure located within India. The SI shall have overall responsibility to build, run and maintain the solution and to engage with the CSP for billing and service levels for the entire contract duration.

3. DETAILED SCOPE OF WORK

The scope of work for the SI shall include (but not be limited to) the following:

A. Solution Design, Development and Implementation

A.1 High-level process flow (To-Be state)

The solution shall implement the following workflow for each tender:

- i. Acquisition of the NIT/tender document and the offer documents of all participating bidders, in the manner set out in Clause 3.A.2;
- ii. Classification, splitting and tagging of the acquired documents (e.g. eligibility documents, financial statements, CA certificates, work orders/experience certificates, statutory

- registrations, declarations, technical literature, price schedules), with all unclassified pages placed in a common "Others" bucket;
- iii. Conversion of scanned and image-based documents to machine-readable text through OCR/ICR, including handwritten entries, seals and stamps to the extent legible;
 - iv. Extraction of the particulars required by the evaluation criteria of that tender, against a Criteria Schema/Parameter Template defined for the tender, with a verifiable citation for every extracted value;
 - v. Deterministic computation of all arithmetic, aggregation, currency/unit conversion and threshold comparison operations;
 - vi. Presentation of the extracted values to the Dealing Officer for review, correction, acceptance or rejection through the web application (mandatory human verification gate);
 - vii. Generation of the output deliverables set out in Clause 3.A.6 only after the human verification gate is completed.

A.2 Acquisition of tender and offer documents

- i. **Automated mode:** Where the tendering portal (GeM, NIC/CP Portal or the CIL e-procurement portal, as applicable) provides an Application Programming Interface (API) or an equivalent authorised integration mechanism, the solution shall download the NIT and the offer documents automatically, on both a scheduled basis (batch job at a configured time) and an ad-hoc basis (on-demand request by an authorised user). The SI shall implement the integration using credentials furnished by the authorised user and shall not store portal credentials in plain text.
- ii. **Manual mode:** Irrespective of the availability of the API, the solution shall mandatorily provide a manual upload facility through which an authorised user may upload the NIT and the offer documents (individually, as a folder, or as an archive) for processing. The manual mode shall be fully functional and shall not be a degraded fallback.
- iii. The solution shall detect and flag duplicate or repeated submissions on the basis of tender ID and bidder identity.
- iv. The SI shall be responsible for ascertaining, during the Requirement Study phase, the API provisioning position of the concerned portal(s), and shall record the same in the System Requirement Specification (SRS). Non-availability of a portal API shall not relieve the SI of any other obligation under this Scope of Work, and the solution shall in such event operate in manual mode without any reduction in functionality other than the download step.

A.3 Criteria Schema / Parameter Template

- i. Evaluation criteria vary from tender to tender. The solution shall therefore accept the evaluation criteria of each tender as a runtime input (Criteria Schema) and shall not rely on criteria embedded in, or learnt by, any model.
- ii. The solution shall provide (i) a facility for an authorised user to select a saved master Parameter Template applicable to the tender type, and (ii) a facility to add, delete or modify parameters for the specific tender before processing.
- iii. Master Parameter Templates for the various tender types shall be created and maintained by Administrator users only.

- iv. The solution shall support, at a minimum, the following parameter types: identifier parameters (e.g. GSTIN, PAN, bidder name, registration number); document-presence parameters (e.g. whether a particular certificate or declaration has been furnished); numeric parameters (e.g. turnover, net worth, quantity, rate); experience parameters (e.g. value, quantity, scope and period of executed work orders); and structural parameters (e.g. Bill of Quantities line items, price schedules, deviation statements).
- v. The solution shall additionally provide a facility for assisted extraction of the eligibility and technical criteria from the uploaded NIT into a draft Criteria Schema, which shall be presented to the user for confirmation or correction before use. Confirmation by the user shall be mandatory.

A.4 Extraction, citation and computation

- i. Every value extracted by the solution shall carry a citation identifying the source document, page number and the location on the page from which the value has been extracted, and the corresponding source text shall be viewable by the user alongside the extracted value.
- ii. The solution shall implement a verification mechanism whereby an extracted value that cannot be traced to text present in the source document is rejected by the system and flagged to the user as "not found" rather than being reported as an extracted value. Generation of any particular that is not supported by the source documents shall be treated as a defect.
- iii. All arithmetic operations, aggregations, unit and currency conversions, escalations, and comparisons of extracted values against thresholds stipulated in the NIT shall be performed by deterministic program logic and not by a language model. The computation logic shall be auditable and reproducible.
- iv. Where a value cannot be extracted with confidence, or where conflicting values are found in different documents of the same bidder, the solution shall flag the item for user attention along with all candidate values and their citations. The solution shall not silently select one value.
- v. The solution shall support extraction and interpretation of documents in the languages listed in the Eighth Schedule to the Constitution of India, to the extent such documents are submitted by bidders.

A.5 Human verification gate

- i. Human verification shall be a mandatory, non-bypassable stage of the workflow. No output document shall be generated, exported or marked final until the Dealing Officer has reviewed and accepted or corrected each extracted particular.
- ii. The solution shall record, for every particular, whether the value was accepted as extracted or modified by the user, along with the user identity, date and time, and shall retain both the original extracted value and the corrected value.
- iii. Where the user modifies an extracted value, the modified value shall flow to all downstream outputs and computations.

A.6 Proposed Outputs

On completion of the human verification gate, the solution shall generate the following outputs for the tender:

- i. A draft **Comparative Statement** in Microsoft Excel (.xlsx) /Microsoft Word format, in the tabular layout prescribed by CIL, with bidders as columns and evaluation parameters as rows (or as otherwise configured), including a citation reference against each entry;
- ii. A draft **Tender Committee Report (TCR)** in Microsoft Word (.docx) format, in the format prescribed by CIL, populated from the verified data;
- iii. A draft set of **technical/commercial queries** to bidders, in editable format, listing shortfall documents and discrepancies identified during extraction and verification;
- iv. An **exception report** listing all parameters flagged as not found, low-confidence or conflicting;

Note: The formats of the Comparative Statement, TCR and query letters shall be furnished by CIL during the Requirement Study phase and shall be configurable in the solution.

A.7 Exclusions from scope

- i. The solution shall not adjudicate, decide, score, rank or recommend the acceptance or rejection of any offer, and shall not compute any qualification or disqualification conclusion of its own.
- ii. The solution shall not be trained on, and shall not draw inferences from, past Tender Committee decisions for the purpose of arriving at an evaluation outcome.
- iii. Price bid opening, price bid decryption and rank determination on the tendering portal remain outside the scope of this solution.

A.8 Extraction accuracy, acceptance gate and measurement

Extraction accuracy is the measurable quality standard of this contract and shall be determined, certified and applied as under.

- i. **Data point — unit of measurement:** A “data point” means one parameter of the Criteria Schema applicable to a tender, required to be extracted in respect of one bid. Where a single pre-qualification or technical qualification criterion requires the extraction of more than one particular, each such particular shall constitute a separate data point.

***Illustration.** Where the criterion of similar work requires the extraction of the relevance of the work executed, the value of the order, the year in which the order was executed and the percentage of completion, that criterion shall yield four data points in respect of each bid.*

- ii. **Total data points:** The total data points of a tender shall be the number of data points per bid, as determined by the Criteria Schema applicable to that tender, multiplied by the number of bids received and processed.

***Illustration.** Where the Criteria Schema of a tender comprises ten data points and ten bids are processed, the total data points of that tender shall be one hundred.*

- iii. **Extraction accuracy:** “Extraction accuracy” in respect of a tender, a bid or a period means the percentage which the data points determined as correct bears to the total data points reckoned for that tender, bid or period.
- iv. **Correctness of a data point:** A data point shall be reckoned as correct only where —
 - (a) the value presented by the solution corresponds to the value borne by the document submitted by the bidder, and the citation furnished under Clause 3.A.4 points to the location in the source document at which that value appears; or

(b) the solution reports the particular as not furnished, and the particular was in fact not furnished by the bidder.

A data point shall be reckoned as incorrect where the solution presents a value which does not correspond to the document submitted by the bidder, where the value presented is correct but the citation does not point to the location at which it appears, where the value presented is drawn from a document other than that required by the criterion, or where the solution reports a particular as not furnished although the same was in fact contained in a document submitted by the bidder.

- v. **Determination through user feedback:** Correctness shall be determined from the feedback recorded by the Dealing Officer against each data point in the Comparative Statement, by means of the positive and negative feedback controls provided by the solution, classified in the manner set out below. Each data point shall be presented with positive feedback recorded by default. Negative feedback shall not be capable of being recorded without the entry of the corrected value or particular, and shall set the accuracy of that data point to nil for all purposes of this Clause. Every instance of negative feedback shall be written to the record maintained under Clause 3.A.5 together with the original extracted value, the corrected value, the identity of the user and the date and time.

Feedback type	Abbreviation	Description
True Positive	TP	The solution correctly identifies a document or particular which is in fact contained in the bid, and the Dealing Officer verifies the same to be present and correctly extracted. Illustration: the solution presents a GST registration certificate as furnished, and the Dealing Officer verifies that it is furnished in the bid.
True Negative	TN	The solution correctly reports that a document or particular has not been furnished, and the Dealing Officer confirms that the same is in fact absent from the bid. Illustration: the solution reports the non-blacklisting affidavit as not furnished, and the Dealing Officer confirms that it is absent from the bid.
False Positive	FP	The solution reports a document or particular as furnished when the same is in fact absent, or presents a value drawn from a document other than that required by the criterion. Illustration: the solution presents a work order as furnished, whereas the document relied upon is a purchase order or a document unrelated to the criterion.
False Negative	FN	The solution fails to identify a document or particular which is in fact contained in the bid. Illustration: the solution reports the financial statement as not furnished, whereas the same is contained in the documents uploaded by the bidder.

For the purposes of computation under this Clause, data points classified as True Positive and True Negative shall be reckoned as correct, and data points classified as False Positive and False Negative shall be reckoned as incorrect.

- vi. **Measurement and reporting:** The solution shall compute and record extraction accuracy automatically from the record maintained under Clause 3.A.5 and shall report the same through the MIS under Clause 3.I, bid-wise, tender-wise and monthly, stating in each case (a) the total data points reckoned; (b) the data points determined as correct; (c) the numbers falling under each of True Positive, True Negative, False Positive and False Negative; and (d) the resulting extraction accuracy. The computation and the underlying feedback record shall be auditable and shall not be capable of alteration by the SI.
- vii. **Acceptance gate:** An extraction accuracy of not less than eighty-five per cent (85%), computed on the aggregate of the total data points of the tenders nominated for acceptance testing under Clause 3.E with at least 80% accuracy in each tender, shall be demonstrated and certified before go-live of each phase. CIL shall nominate not less than fifty (50) already finalised/processed tenders comprising all categories of tenders under the relevant phase; the number of tenders is tentative and the actual number of tenders and of bids to be nominated shall be at the sole discretion of CIL depending on the phase. Go-live shall not be permitted until the said level is certified for the nominated test tenders.
- viii. **Standard after hyper-care:** With effect from the expiry of the hyper-care period of three (3) months from go-live, the solution shall attain an extraction accuracy of not less than ninety per cent (90%), computed on the total data points of each tender.
- ix. **Consequence in payment:** Where the extraction accuracy of a tender processed after go-live but after the expiry of the hyper-care period is below ninety per cent (90%), the bids comprised in that tender shall not be reckoned in the number of bids processed for the purpose of quarterly payment under Clause 5, and no payment shall be due to the SI in respect of those bids. Where the total data points of a tender are fewer than twenty (20), the said standard shall be applied to the aggregate of all tenders of that category processed during the month, and not to that tender individually. The quarterly system report furnished under Clause 3.I shall separately state the number of bids processed, the number meeting the said standard, and the number excluded from payment on this account.
- x. **Corrective obligation:** Where the monthly extraction accuracy falls below ninety per cent (90%) after expiry of the hyper-care period, the SI shall carry out periodic re-training, tuning, re-configuration and optimisation of the components of the solution as necessary to restore the said level, at no additional cost to CIL. Such work shall not be treated as Change Management and shall not entitle the SI to any extension of the service levels. Where the monthly extraction accuracy remains below the said level for three (3) consecutive months, the same shall constitute a failure to meet the agreed service levels for the purposes of Clause 3.H and the Service Level Agreement.

A.9 Sample Tender for Live Demonstration:

- i. For the purpose of the technical presentation / demonstration forming part of the evaluation, CIL shall share with the shortlisted bidders a set of sample tender documents and sample offer documents, being documents of concluded tenders from which bidder identity and commercially sensitive particulars have been redacted.
- ii. The said documents shall be shared only after the bidder has executed and furnished to the Tender Inviting Authority a Non-Disclosure Agreement via mail before the due date of submission of bids.

- iii. On receipt of the executed Non-Disclosure Agreement, the documents shall be made available to the shortlisted bidder as per QCBS given in ITB through a secure access mechanism designated by CIL. The documents shall be used solely for the purpose of responding to and participating in this tender, shall not be transferred, reproduced or retained beyond the tender process, and shall be certified as destroyed by the bidder on conclusion of the tender.

B. Web Application

- a) The solution shall provide a web-based application accessible over the CIL intranet and, where authorised, over the internet, developed following secure design principles.
- b) Authentication shall be through CIL credentials integrated with CIL Active Directory / LDAP / SSO. Role-based access control shall be provided with, at a minimum, the following roles: Dealing Officer / Tender Officer, Reviewer, System/Bot user, Notification user, and Solution Administrator.
- c) The application shall provide interfaces for: entry of tender-level details; selection and editing of the Parameter Template; submission of download or upload requests; monitoring of processing status; validation of document classification; validation of extracted particulars; and download of the generated outputs.
- d) For classification validation and for field-level validation, the application shall provide a side-by-side (picture-in-picture) view showing the source document page alongside the extracted value, with the source location highlighted.
- e) The user interface shall support filtering by tender ID and by bidder, editable fields, and explicit Accept / Modify / Reject / Save actions with an indication of review status for each item.
- f) The application shall be designed with stateless components; session state, where required, shall be maintained in a database or cache with automatic refresh. The application shall scale horizontally with load.
- g) The application shall not cause any disruption or downtime to existing CIL applications.
- h) Solution Architecture: The application shall be designed using a modular, layered and, wherever technically appropriate, microservices architecture, with minimum dependency between subsystems and flexibility to replace or upgrade individual components without material disruption to the overall solution.
- i) The solution shall use technology-agnostic interfaces for communication between components. IP addresses shall not be hard-coded. Wherever appropriate, asynchronous integration mechanisms shall be used for long-running or resource-intensive processes.
- j) The solution shall expose API-based interfaces for integration with CIL systems and future applications. APIs shall use secure authentication and authorization mechanisms and shall be documented for CIL.
- k) Component failures shall be handled gracefully. Critical components shall be designed with appropriate redundancy and no critical component shall constitute a single point of failure.
- l) The solution shall support automatic horizontal scaling of application and processing components based on configurable workload thresholds, without adversely affecting the response time and throughput requirements specified in this Scope of Work.

- m) Serverless or fully managed cloud services may be used, wherever technically suitable, so that routine infrastructure activities such as capacity provisioning, availability management and patching are handled natively by the CSP. The proposed architecture shall not mandate serverless services where they are unsuitable for the AI/ML workload.
- n) Container images, where used, shall be sourced from a CSP/OEM-vetted or otherwise trusted repository, shall be maintained on supported versions and shall be subject to vulnerability scanning before deployment.
- o) Infrastructure and application configuration shall, to the extent practicable, be maintained through Infrastructure-as-Code (IaC) or equivalent controlled configuration management so that environments can be reproduced and changes can be audited.

C. AI/ML Models and Model Hosting

- i. All models used in the solution shall be deployed within the CIL-designated cloud environment and shall be accessible only through private endpoints. **Externally or publicly hosted models (such as GPT, Gemini, Claude or similar services) shall not be used in any part of the solution,** so that CIL data and bidder data do not leave the CIL-controlled environment at any stage.
- ii. Bidder documents, extracted data, prompts and queries shall not be transmitted to any third-party service and shall not be used for training, tuning or improvement of any model outside the CIL environment.
- iii. The solution shall employ a retrieval-based architecture in which the answers are grounded in the documents of the tender under evaluation. Where retrieval over a corpus of CIL documents is employed for drafting assistance, the retrieved passages shall be shown to the user with their source reference.
- iv. Training and fine-tuning capability shall be required only for the supporting models used for document classification, OCR/ICR, document splitting, form parsing and field extraction. CIL does not require the SI to build a foundation language model under this contract.
- v. Only CIL data shall be used for any tuning of models under this contract, and the resultant model weights and artefacts shall be the property of CIL.
- vi. The solution shall maintain a model repository with versioning, and shall permit export of deployed models in a portable form (e.g. container image) to enable migration.
- vii. The SI shall provision all software, model and platform licences required for the solution for the entire contract period. No unlicensed software shall be deployed.
- viii. The SI shall furnish documentation for each model deployed, describing its purpose, inputs, outputs, known limitations and the version in production.

C.1 MLOps Platform and Model Lifecycle Management

- i. The SI shall provide an enterprise-ready MLOps capability appropriate to the tender-evaluation use case for development, training/tuning, validation, deployment, monitoring and lifecycle management of the AI/ML models used in the solution.
- ii. The MLOps capability shall support reproducible model-development and deployment workflows and shall maintain a centralized repository for models, model versions, associated artefacts and configuration.

- iii. The solution shall support online and batch model serving, as applicable, and shall permit deployment of approved model versions through private endpoints. Multiple model versions shall be capable of being managed and promoted through controlled release processes.
- iv. Models and associated artefacts shall be exportable in a portable form, including containerized form where technically appropriate, to support migration and avoid proprietary lock-in.
- v. Training and tuning capability shall be provided for supporting models relevant to document classification, OCR/ICR, document splitting, form parsing and field extraction. CIL does not require the SI to build a foundation language model under this contract.
- vi. Only CIL-authorized data shall be used for tuning models under this contract. No bidder data, CIL data, prompts or extracted information shall be used to train or improve any external or publicly hosted model.
- vii. The MLOps platform shall support experiment tracking, model evaluation, version comparison, model approval, promotion to production, rollback to an earlier approved version and recording of the model version deployed for each production release.
- viii. The SI shall continuously monitor model performance and shall identify material degradation or model drift. Where extraction accuracy falls below the contractual threshold, the SI shall perform the required retraining, tuning, re-configuration and optimisation without additional cost to CIL, in accordance with Clause 3.A.8.
- ix. The MLOps capability shall integrate with CIL authentication/SSO and role-based access controls, with access to model development, deployment and administration restricted to authorized personnel.
- x. Model endpoints shall be invocable from the workflow orchestration layer through secure APIs, and model execution shall be logged for audit and troubleshooting.
- xi. The platform shall maintain model documentation including purpose, version, training/tuning data source, evaluation results, known limitations, deployment date and approval status.
- xii. The AI/ML layer shall incorporate controls against prompt injection, unauthorized instructions embedded in bidder documents, data exfiltration and unsupported model outputs. Model outputs used for tender evaluation shall be grounded in the source tender/bid documents and shall remain subject to the mandatory human verification gate.
- xiii. The solution shall maintain auditable records of material model interactions, including model/version used, input reference, output, user/process initiating the request and relevant timestamps, subject to CIL's applicable data-retention requirements.
- xiv. The SI shall conduct adversarial and negative testing of the AI/ML components, including testing for unsupported extraction, hallucinated values, prompt injection and attempts to cause disclosure of information outside the authorized tender/document context.

C.2 Workflow, Job Orchestration and Process Automation

- i. The solution shall provide a workflow and job-orchestration capability for scheduled and ad-hoc execution of tender acquisition, document processing, classification, OCR/ICR, extraction, computation, validation and output-generation activities.

- ii. The orchestration layer shall support creation, deployment, scheduling, monitoring and management of automated workflows and shall provide a job queue/tracking dashboard showing status such as queued, running, completed, failed and retried.
- iii. Workflows shall be capable of invoking secure APIs, file-processing services, model endpoints and deterministic computation services at the appropriate stages of the tender-processing pipeline.
- iv. The workflow engine shall support configurable retries, timeout handling, failure handling and restart/resume of interrupted jobs, without causing duplicate processing of the same tender or bid.
- v. Workflow execution may be triggered by the CIL web application, scheduled jobs or authorised external systems through secure REST APIs, as applicable.
- vi. The system shall generate job-level notifications for completion, failure and other configured events and shall maintain execution logs sufficient for audit, debugging and root-cause analysis.
- vii. The workflow/orchestration components shall be deployable within the CIL-designated cloud environment and shall use open standards and documented interfaces to facilitate future migration to an on-premise CIL environment, where required.

C.3 Data Storage, Database and Vector Store

- i. The SI shall provision SQL, NoSQL, vector-store and/or other database technologies as applicable to the approved solution architecture. Only supported and properly licensed enterprise versions of required databases, object/file stores and associated tools shall be used.
- ii. Bid documents, extracted data, metadata, audit records, model artefacts and configuration data shall be stored in appropriate logical repositories with access controls and retention policies defined in consultation with CIL.
- iii. Where Retrieval-Augmented Generation (RAG) or semantic retrieval is used, the solution shall maintain the corresponding embeddings/vector store with appropriate security controls and shall retain a link between retrieved content and its source document/reference.
- iv. The underlying data layer shall be designed so that authorised CIL personnel can access and export the data required for audit, reporting, future analytics and migration, without proprietary lock-in.
- v. Database access shall follow least-privilege principles. Database health, capacity, storage utilisation, failed operations and security events shall be monitored and appropriate alerts shall be generated.

D. Hosting, Cloud Infrastructure and Data Security

- i. The solution shall be hosted on a MeitY-empanelled Cloud Service Provider having its Data Centre and Disaster Recovery site within the territory of India and shall be governed by the data residency, security and exit provisions of the Contract (this Scope of Work and the Service Level Agreement). All CIL data shall reside only in India and shall not be accessed by any entity outside the control of CIL or its authorised representatives.
- ii. The SI shall provision and manage the entire cloud infrastructure, including compute, GPU where required, storage, database (relational, and vector store where applicable), object

storage, networking, load balancing, and backup, sized to meet the service levels of this contract. Root/owner access of the cloud account shall vest with CIL.

- iii. The SI shall provision not less than forty (40) terabytes of usable storage, and shall in addition provide headroom of not less than twenty-five per cent (25%) over and above the said capacity, which shall be made available on demand during the contract period at no additional cost to CIL. Storage required for backups, snapshots and archival under Clause 3.D shall be provisioned separately and in addition to the aforesaid capacity and headroom.
- iv. The cloud account shall be configured with region deny controls, or an equivalent preventive control of the CSP, so as to disallow the creation, storage or processing of CIL data and resources in any region outside India. Evidence of the said control being in force shall be furnished to CIL at go-live and thereafter on demand.
- v. The CSP and OEM services proposed shall have a clear published roadmap and shall not be declared End of Life, End of Sale or End of Support during the five (5) year contract period. The SI shall submit, along with its offer and again at go-live, a certification from the concerned CSP/OEM that support for the offered services shall be available for not less than five (5) years from the date of award. Where any component is nevertheless declared End of Life, End of Sale or End of Support during the contract period, the SI shall migrate the solution to an equivalent or superior supported component at no additional cost to CIL and without degradation of the service levels.
- vi. Any financial, cyber or legal obligation arising on account of any non-compliance or breach not attributable to CIL shall be borne by the SI.
- vii. The solution shall be deployed in a Virtual Private Cloud with logical isolation, segregated public and private subnets, and secure connectivity over an encrypted channel (SSL VPN or equivalent).
- viii. Separate Development, Test/UAT, Production and Disaster Recovery environments shall be provided.
- ix. Data shall be encrypted at rest using AES-256 and in transit using TLS. Key and secret management shall be through a managed key management service; credentials and secrets shall not be hard-coded.
- x. The design shall comply with the prevailing MeitY guidelines for cloud adoption, CERT-In guidelines and the applicable data protection law of India.
- xi. Web Application Firewall protection against the OWASP Top 10 and OWASP API Top 10, DDoS protection, network firewall, intrusion detection and prevention, and endpoint protection shall be provided.
- xii. Vulnerability Assessment and Penetration Testing (VAPT) shall be carried out by a CERT-In empanelled agency before go-live and after every major change, and thereafter at least once every six months. Reports and closure of findings shall be submitted to CIL.
- xiii. The system shall maintain audit trails and transaction logs recording what was changed, when and by whom, including document access, extraction results, user corrections and output generation. Logs shall be retained online for six (6) months and thereafter archived in retrievable form for the contract period, and transaction logs shall in any event be retained and remain retrievable for not less than twelve (12) months. The SI shall further make provision to forward the logs of all security devices and services of the solution to the CIL Security Operations

Centre / SIEM at CIL premises, in a format acceptable to CIL, and shall bear the cost of such integration.

- xiv. The solution shall be portable. The SI shall use applications and services based on open standards and shall not employ any proprietary format, API or service that prevents migration of the solution and its data to another CSP or to a CIL on-premise data centre.
- xv. Backup of databases, application configuration, source repositories and logs shall be taken daily, weekly, monthly, quarterly and yearly, with retention of 7 days, 15 days, 3 months, 1 year and 3 years respectively. Restoration shall be tested at scheduled intervals. Backup storage shall be provisioned in addition to the primary storage indicated in the BoQ.
- xvi. Policies and technical measures shall be implemented for secure disposal and complete removal of CIL data from all storage media on termination or expiry of the contract.

D.1 Environment Management

- i. Separate Development, Test/UAT, Production and Disaster Recovery environments shall be maintained with appropriate logical or physical segregation. Data and credentials shall not be copied from Production to non-production environments except where specifically authorised by CIL and appropriately masked or protected.
- ii. The SI shall ensure that application, infrastructure and security changes are promoted through controlled release processes and that Production deployment occurs only after applicable testing and CIL approval.

D.2 Network and Transport Security

- i. The solution shall maintain logical segregation between public-facing and private workloads/subnets. All communication between users, application components, APIs, databases and external systems shall use encrypted protocols appropriate to the sensitivity of the data.
- ii. All APIs and hosted application, portal, dashboard and reporting interfaces shall use HTTPS/TLS with current strong cryptographic standards. TLS certificates shall be centrally managed, securely stored and renewed before expiry.
- iii. Secure connectivity between CIL's designated network/data centre and the cloud environment shall be provided through SSL VPN, site-to-site VPN, private connectivity or an equivalent CIL-approved encrypted mechanism.
- iv. Network access shall be controlled through security groups/network ACLs/firewall policies following least-privilege principles. Resources in private subnets shall not be directly accessible from the public internet.
- v. DNS security controls, including DNSSEC where applicable to the selected architecture, shall be implemented to mitigate DNS spoofing and hijacking risks.

D.3 Load Balancing and API Gateway

- i. The solution shall provide an application load-balancing mechanism for the web application and API components to support high availability, health checks, traffic distribution and horizontal scaling.
- ii. The load-balancing layer shall support HTTPS/TLS termination or pass-through as appropriate and shall support Layer-7 routing for microservices and API-based application components.

- iii. Where an API Gateway is used, it shall provide secure API publication, authentication/authorization, rate limiting/throttling, monitoring and controlled routing of API requests.

D.4 Cloud Monitoring and Management

- i. The SI shall provide a monitoring capability covering availability, performance, capacity, configuration and security of the cloud resources used by the solution.
- ii. Monitoring shall provide real-time and historical visibility of, at a minimum, compute/VM resources where applicable, CPU, memory, storage, GPU utilisation, network utilisation, database utilisation, application availability and processing workload.
- iii. Threshold-based alerts shall be configured for resource exhaustion, service degradation, processing backlog, failed jobs and other events that may affect the agreed service levels.
- iv. The solution shall provide dashboards and reports for resource availability, utilisation and capacity trends and shall retain the relevant monitoring data for analysis of service-level performance.

D.5 Application Performance Monitoring

- i. The solution shall provide Application Performance Monitoring (APM) covering response time, API latency, application errors, exceptions, database calls, external service calls and other material application performance indicators.
- ii. The monitoring capability shall support end-to-end tracing or equivalent correlation of application requests across relevant components and shall enable root-cause analysis of slow or failed transactions.
- iii. The APM capability shall provide configurable dashboards and reports and shall support correlation of application performance with infrastructure and database metrics.

D.6 Database Monitoring

- i. The SI shall provide regular health checks, monitoring and alerting for database availability, storage utilisation, capacity, performance and failures.
- ii. The solution shall monitor relevant inbound data flows for completeness and consistency and shall generate alerts for database security events, including suspected SQL injection or unauthorised access attempts.

D.7 Centralised Log Management and Audit

- i. The solution shall provide a central facility for collection, storage, indexing and retrieval of application, workflow, infrastructure, database and security logs.
- ii. All material actions and operations shall be logged for audit, event tracing and debugging, including workflow execution, model invocation, user access, user corrections, configuration changes and administrative actions.
- iii. Logs shall support correlation and anomaly detection and shall generate alerts for configured abnormal or security-related events.
- iv. Security-device and relevant cloud security logs shall be capable of being forwarded to the CIL Security Operations Centre / SIEM in a format and manner acceptable to CIL.

- v. Transaction and security logs shall be retained for the periods specified in this Scope of Work and shall remain retrievable throughout the contract period, subject to CIL's applicable retention requirements.

D.8 Identity, Access Management and Zero-Trust Principles

- i. CIL's identity and access-management mechanism shall be the primary trust source for authentication and authorisation of CIL users. Access shall follow least-privilege and role-based access principles.
- ii. Privileged and administrative access shall be protected by multi-factor authentication (MFA) or the equivalent CIL-approved control. Shared administrative accounts shall not be permitted except where technically unavoidable and specifically approved by CIL.
- iii. Development, Test/UAT, Production and Disaster Recovery environments and applicable network zones shall be segregated. Access between zones shall be explicitly authorised and controlled.
- iv. The solution shall follow Zero Trust principles, whereby access to resources is explicitly authenticated, authorised and monitored rather than being trusted solely on the basis of network location.

D.9 Managed Threat Detection and Security Posture

- i. The solution shall continuously monitor for malicious or unauthorised behaviour affecting the cloud account, workloads, applications and data and shall generate actionable alerts.
- ii. The SI shall maintain visibility of security configuration, exposed resources, vulnerabilities and material policy deviations and shall provide mechanisms for remediation and closure tracking.
- iii. Security controls shall be capable of scaling with application workload so that security components do not become a bottleneck for the solution.

D.10 Web Application Firewall

- i. A Web Application Firewall (WAF) shall protect the web application and APIs against common web exploits and vulnerabilities, including OWASP Top 10 and OWASP API Top 10 risks.
- ii. The WAF shall support monitoring and blocking of malicious HTTP/S traffic and configurable security rules and shall be integrated with the application/load-balancing architecture as appropriate.
- iii. The SI shall maintain WAF rules and configurations and shall promptly implement security updates required to address material vulnerabilities.

D.11 DDoS Protection

- i. DDoS protection shall be provided at appropriate network, transport and application layers for internet-facing components, where applicable.
- ii. The protection mechanism shall support continuous detection and automated mitigation of volumetric and behaviour/anomaly-based attacks and shall minimise service disruption.
- iii. DDoS events and mitigation actions shall be logged and made available through dashboards/reports for security review.

D.12 Firewall and Network Security

- i. Inbound and outbound traffic between the internet and the solution's virtual network, and between relevant network zones, shall be controlled through a managed firewall/security-control layer.
- ii. Firewall controls shall support stateful inspection and fine-grained rules based on source/destination, port, protocol and other applicable attributes.
- iii. Firewall and network-security controls shall support intrusion detection/prevention or equivalent controls and shall generate security alerts for detected threats.
- iv. Outbound traffic shall be restricted to the minimum destinations and services required for operation of the solution to reduce the risk of data leakage and communication with known malicious endpoints.

D.13 Key, Secret and Certificate Management

- i. Encryption keys and application secrets shall be managed through a managed key-management and secret-management service or an equivalent CIL-approved mechanism. Keys and secrets shall not be hard-coded in source code, configuration files or container images.
- ii. Key usage shall be auditable and keys shall be rotated in accordance with applicable security policy and the CSP's supported capabilities.
- iii. Public and private TLS certificates, where applicable, shall be securely provisioned, managed, renewed and revoked through controlled processes.

D.14 High Availability, Business Continuity and Disaster Recovery

- i. The production architecture shall be designed across appropriate physically separated facilities/availability zones, wherever supported by the selected CSP and required by the approved architecture, so that failure of a single facility or component does not cause avoidable prolonged service interruption.
- ii. Critical application components shall have appropriate redundancy and automatic failover. Where active-active architecture is technically feasible and appropriate, it shall be used; otherwise, the SI shall provide an approved high-availability/failover architecture.
- iii. The SI shall define the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for the solution in the solution design document and shall demonstrate the same during DR testing. The proposed RPO/RTO shall be subject to CIL approval.
- iv. Backup and replication mechanisms shall be designed to minimise data loss in the event of infrastructure or site failure. Restoration and failover procedures shall be documented and periodically tested.

D.15 Security Assurance and Release Security

- i. Security shall be integrated into the software development and release process through DevSecOps practices, including code review, dependency/security scanning, container image scanning where applicable, configuration security checks and automated testing.
- ii. Internal security testing shall be carried out before major releases and external VAPT/application security assessment shall be carried out at least once every six months and after major changes, through a CERT-In empanelled agency where such empanelment is applicable.

- iii. All material findings identified through security testing shall be remediated by the SI within the timelines agreed with CIL and shall be tracked to closure. No critical security finding shall remain unresolved at Production go-live.

E. Testing, Acceptance, Documentation and Training

- i. The SI shall prepare and obtain sign-off on the System Requirement Specification (SRS), solution design document and test plan before commencement of development.
- ii. Functional, performance, load and security testing shall be carried out by the SI, and test reports shall be submitted to CIL before each release.
- iii. Acceptance testing shall be conducted by CIL on a set of live or representative tenders nominated by CIL. Acceptance shall be based on (i) correct extraction of the particulars against the Criteria Schema for the nominated tenders, and (ii) demonstrated reduction in the time taken to prepare the Comparative Statement as compared with the baseline recorded during the Requirement Study phase.
- iv. Automated testing tools shall be used, and appropriate automated test cases shall be executed as part of the software build/release process. Test evidence and reports shall be submitted to CIL before the corresponding release.
- v. Functional testing shall include API/interface testing, workflow testing, database/data-persistence testing, document classification, OCR/ICR, extraction, citation validation, deterministic computation, user verification and output generation.
- vi. Regression testing shall be carried out for every major release or material change to ensure that previously accepted functionality and extraction behaviour are not adversely affected.
- vii. Performance and scalability testing shall be carried out at representative and peak loads, including verification of processing throughput, application response time, queue behaviour, database performance, report-generation time and resource utilisation.
- viii. Security testing shall include vulnerability scanning, application security testing, API security testing, VAPT and testing of authentication, authorisation, data protection, logging and network controls. Findings shall be remediated before Production go-live in accordance with the severity agreed with CIL.
- ix. AI/ML testing shall include model accuracy, citation/source-grounding, unsupported-output/hallucination, conflicting-value detection, prompt-injection and negative/adversarial test cases. The results shall be documented for each material model release.
- x. Disaster recovery/failover testing shall be carried out before Production acceptance and periodically thereafter as agreed with CIL, with restoration/failover results and observed RPO/RTO submitted to CIL.
- xi. The SI shall record, during the Requirement Study phase and jointly with CIL, the baseline time presently taken to prepare a Comparative Statement for each tender category. This baseline shall be the reference for measurement of the deliverable throughout the contract.
- xii. The solution shall be deployed to production only after successful UAT acceptance by CIL.
- xiii. Production deployment shall additionally be contingent upon a presentation before the CIL Board demonstrating the working of the portal and the outcome of the tender evaluation.

- xiv. The SI shall furnish complete documentation, including SRS, design documents, data dictionary, deployment and configuration documents, administrator manual, user manual and standard operating procedure, in editable form, and shall keep them updated throughout the contract.
- xv. The SI shall impart classroom and hands-on training to CIL officers in at least 5 batches at locations to be intimated by CIL, and shall provide refresher training after every significant functional change.

F. Change Management

- i. The SI shall provide change management services for a period of five (5) years from the date of final acceptance, for 100 man-days as indicated in the BoQ.
- ii. Change management shall cover enhancements and modifications required on account of changes in CIL procurement procedures, output formats, statutory or policy requirements, new tender categories, and additional use cases within the tender evaluation domain.
- iii. All change requests shall be documented in a Change Request (CR) form specifying the nature, scope and impact. The SI shall acknowledge a CR within five (5) working days and furnish an impact analysis with estimated man-days within ten (10) working days.
- iv. CIL shall approve CRs based on priority and budget. The SI shall not commence work on any CR without written approval of the Designated Officer.
- v. All changes shall be tested in the UAT environment before deployment to production.
- vi. The following shall **not** be treated as Change Management and shall be carried out by the SI at no additional cost to CIL: correction of defects; retraining, tuning or re-configuration of components required to maintain the accuracy of extraction; patches, security fixes and version upgrades of solution components; and any work required to meet the service levels of this contract.
- vii. The SI shall furnish monthly reports on all CRs and shall hold monthly review meetings with CIL.

G. DevSecOps and Tool / Solution Management

- i. The SI shall provide a controlled CI/CD capability covering Development, Test/UAT and Production environments.
- ii. The CI/CD pipeline shall support source-code version control, automated build, automated testing, security scanning, packaging and controlled deployment. The pipeline shall support rollback to a previously approved version.
- iii. The solution shall maintain a Git-compliant source repository. CIL shall have appropriate read access to the repository and release artefacts throughout the contract period.
- iv. The DevSecOps toolchain shall, as applicable to the architecture, provide code dependency management, container image repository and vulnerability scanning, configuration management, infrastructure provisioning and environment-drift detection.
- v. Deployment of application and infrastructure changes shall be traceable to an approved release/change request. Production deployment shall require the applicable CIL approval and successful UAT/security gates.

- vi. The CI/CD and configuration-management tools shall be supported enterprise/CSP/OEM tools or actively maintained tools for which the SI has demonstrated capability to configure, operate and support the same throughout the contract period.
- vii. The SI shall maintain release records identifying the version of application code, infrastructure configuration, models and significant configuration items deployed in Production.

H. Support Services

H.1 L1 support (five years)

- i. The SI shall provide L1 support for five (5) years from go-live, during CIL working hours (9:00 AM to 6:00 PM IST on working days), through email, telephone and an online ticketing system.
- ii. The SI shall have to deploy **one personnel at each subsidiary HQ of CIL** and two personnels at CIL HQ.
- iii. L1 support shall cover user queries, issue identification, basic troubleshooting, resolution of common issues, monitoring of system health, and verification of completion of backups.
- iv. The SI shall maintain a ticketing system accessible to CIL, shall issue an automated acknowledgement with a reference number on receipt of each request, and shall furnish monthly support reports covering volume, response time, resolution time and recurring issues.
- v. A knowledge base with self-help resources shall be maintained and kept updated.
- vi. Deployment of support personnel onsite at CIL shall be at the option of CIL and, if required, shall be intimated to the SI; in the absence of such intimation, support may be rendered remotely.

H.2 L2 support and hyper-care (three months)

- i. For a period of three (3) months from go-live of phase-2, the SI shall provide L2/hyper-care support covering escalations from L1, in-depth technical troubleshooting, advanced issue resolution and liaison with the development team. L2 support team should be deployed at CIL HQ only.
- ii. L2 support shall not cover new feature development or major version upgrades. Such matters, and any issue not capable of resolution at L2, shall be escalated to L3 support, meaning the development team of the SI and, where the issue pertains to a third-party or OEM component, the support organisation of the concerned OEM. L3 support shall be arranged and borne by the SI for the entire contract period at no additional cost to CIL.
- iii. On-call support for critical issues shall be available outside normal business hours, including weekends and holidays.
- iv. Detailed incident reports with root cause analysis and preventive measures shall be furnished for all critical incidents.

G.3 General

- i. Clear escalation paths for L2 and L3 support, with contact details, shall be established and kept current.
- ii. All support personnel shall adhere to CIL confidentiality and data security policies, and a Non-Disclosure Agreement shall be executed in respect of each resource deployed.

- iii. Performance against the service levels shall be monitored and reported monthly; quarterly service review meetings shall be held with CIL.
- iv. CIL reserves the right to terminate support services on thirty (30) days notice if the SI fails to meet agreed service levels, and the SI shall in such event ensure smooth transition of support responsibilities to CIL or its nominee.
- v. L1 and L2 support personnel shall be suitably qualified for the functions assigned to them. The SI shall provide replacement resources during planned or unplanned absence so that agreed support levels are maintained.
- vi. The SI shall maintain an up-to-date escalation matrix covering L1, L2, L3, application development and relevant CSP/OEM support, with named roles and contact details.
- vii. The SI shall provide quarterly service review reports covering incidents, SLA performance, recurring issues, root-cause analysis, model accuracy, capacity utilisation, security findings, changes implemented and preventive actions.

I. Reporting and MIS

- i. The solution shall provide dashboards and reports covering, at a minimum: tender-wise summary (key dates, number of offers received, processing status); number of bids processed and time taken per bid and per tender; bids pending processing; user-wise activity; and exception statistics.
- ii. The solution shall provide a report of time taken to prepare the Comparative Statement for each tender, measured from acquisition of documents to generation of the verified output, to enable comparison against the baseline recorded under Clause 3.E.
- iii. A transparent and independently verifiable mechanism to cross-check the number of bids processed by the solution shall be provided, as the same forms the basis of quarterly payment under Clause 5.
- iv. A monthly report of bids processed shall be submitted to the Designated Officer and, in respect of the tenders of each subsidiary, to the Subsidiary Project Leader concerned.
- v. In addition to the above, the solution shall provide dashboards/reports covering, at a minimum: (i) tender-wise processing status; (ii) bid-wise processing status; (iii) processing time by tender and bid; (iv) pending/failed/retried jobs; (v) user-wise activity; (vi) document classification exceptions; (vii) extraction accuracy; (viii) low-confidence and conflicting-value exceptions; (ix) model performance/version; (x) application and infrastructure performance; (xi) SLA compliance; and (xii) security/audit events, as applicable.
- vi. All MIS figures forming the basis of payment or SLA measurement shall be generated from system records and shall be independently verifiable by CIL. The SI shall not be able to alter historical transaction or payment records without an auditable administrative trail. The MIS and the SLA monitoring dashboard of the Solution shall be under the direct and exclusive administrative control of CIL, and the reports forming the basis of payment or SLA measurement shall be generated from the Solution without manual intervention.

J. Intellectual Property, Source Code and Exit Management

- i. All data, documents, extracted content, models tuned on CIL data, configurations and outputs generated under this contract shall be the exclusive property of CIL.

- ii. The complete source code of the bespoke solution developed under this contract, together with build scripts, configuration, deployment artefacts, database schema and documentation, shall be handed over to CIL at the end of the contract, and also at every major release milestone, at no additional cost to CIL. CIL shall have a perpetual, irrevocable, royalty-free right to use, modify and maintain the same for its own purposes and those of its subsidiaries.
- iii. Source code shall be maintained in a Git-compliant version control repository to which CIL shall have read access throughout the contract period.
- iv. On expiry or termination of the contract, the SI shall migrate all data and the working solution to a CIL-nominated environment (cloud or on-premise) and shall provide transition support for a period of thirty (30) days after contract period, at no additional cost.
- v. Any third-party or proprietary component embedded in the solution shall be declared in the solution document at the design stage, and the SI shall ensure that CIL obtains a licence for its continued use, or shall provide an open-standard equivalent.

K. Service Levels

The solution shall meet the following service levels. Detailed measurement methodology and price discounts for non-compliance shall be as set out in the Service Level Agreement forming part of the tender document.

4. PROJECT COMPLETION TIME

The phase-wise roll-out plan shall be as under, where "T" denotes the date of execution of the Agreement, or the forty-fifth (45th) day from the date of issue of the Letter of Acceptance (LOA), whichever is earlier, save where the delay in execution of the Agreement is attributable to CIL (Clause 26.10 of ATC (ITB)):

No.	Milestone	Timeline	Nomenclature
1	Information gathering, requirement study, As-Is process study and baseline time recording, SRS and design/solution documents, resource mobilisation	T + 30 days	T ₁
2	Design sign-off	T ₁ + 15 days	T ₂
3	Solution development, cloud provisioning and deployment	T ₂ + 75 days	T ₃
4	Training, functional testing, load testing and security testing (VAPT)	T ₃ + 30 days	T ₄
5	User Acceptance Testing and acceptance sign-off-Go Live	T ₄ + 30 days	T ₅
6.1	Production implementation — Phase 1: Goods , Works & Services Tender including QCBS	T ₅ + 15 days	T ₆
6.2	Production implementation — Phase 2: Turnkey, Handling Transport And Other Mining Services, Hiring Of Earth Moving Equipment	T ₆ + 45 days	T ₇

No.	Milestone	Timeline	Nomenclature
7	Hyper-care (three months from go-live of Phase 2)	T ₇ + 90 days	T ₈
8	L1 support and bid processing	5 years from T ₅	

For the purpose of liquidated damages, the date of completion of implementation shall be T₇ (production implementation of Phase 2), and the date of Go-Live shall be as defined in the Service Level Agreement.

CIL shall communicate its approval of, or its observations with reasons on, the SRS and the design/solution documents within fourteen (14) days of their submission, and shall notify in writing the defects and/or deficiencies observed in User Acceptance Testing within twenty-one (21) days of receipt of the SI's written notice of readiness for acceptance.

In the event of non-resolution of all issues, or non-attainment of the extraction accuracy standard specified in this Scope of Work, during the Hyper-care period, the Hyper-care period shall stand extended till resolution of all such issues, and no additional payment shall be made by CIL or its subsidiaries for such extended period.

5. PAYMENT SCHEDULE AND DELIVERABLES

Payment shall be released against the following line items of the Bill of Quantities on fulfilment of the corresponding milestones:

Sl. No.	Item description (line item of BoQ)	Required documents	Payment schedule
1	AI-assisted Tender Evaluation Solution — design and implementation as per scope	After go-live and sign-off; certificate by the SI duly accepted by the Designated Officer	Phase 1 — 50% of Portal Development Cost Phase 2 — 25% of Portal Development Cost On completion of hyper-care — 25% of Portal Development Cost
2	Change management (man-days)	Man-days consumed in the corresponding quarter, with sign-off by the Designated Officer	Quarterly based on the consumption of Mandays
3	L1 and L2 support after go-live	Certificate of services rendered, signed by the Designated Officer (CIL HQ) and by the Subsidiary Project Leader of the respective subsidiary (services at that subsidiary)	Quarterly after Go-Live. L2 support cost during Hyper care period will be given for only 3 months from Go-Live Date.
4	Number of bids in evaluation for 5 years	Total number of bids processed in that quarter as per system report, cross-checked as per Clause 3.H; certificate accepted by the Designated Officer (tenders of CIL	Quarterly after Go-Live for the contract period.

Sl. No.	Item description (line item of BoQ)	Required documents	Payment schedule
		HQ) and by the Subsidiary Project Leader of the respective subsidiary (tenders of that subsidiary)	

Notes:

- No advance payment shall be made.
- Payment shall be made only against receipt of invoice(s) duly certified by the Designated Officer or the Subsidiary Project Leader, as applicable, and shall be released by the Paying Authority as defined in the Service Level Agreement. The invoice shall clearly indicate all tax components. CIL shall deduct TDS as applicable under the prevailing taxation laws.
- Each tax invoice shall bear the GSTIN of CIL.
- Payment shall be released through electronic fund transfer, and the bidder shall furnish consent for the same.
- No payment other than the rate/amount quoted in the tender shall be paid by CIL.
- LD of 0.5% of the corresponding line-item cost shall be charged on a weekly basis in case of delay in implementation, subject to a limitation set in 5.15 of SLA/Conditions of Contract.
- Payment shall be made after adjustment of LD, if any, levied against the Service Level Agreement.
- Payment for bids processed shall be made quarterly, on the basis of the number of bids processed by the solution in that quarter, subject to compliance with the performance service levels set out in the Service Level Agreement.
- No payment shall be due in respect of any bid processed at an extraction accuracy below ninety per cent (90%) after expiry of the hyper-care period, and such bids shall be excluded from the quarterly count as provided in Clause 3.A.8.
- Payment for change management shall be released as and when the implementation of the approved change request is completed and sign-off is accorded by the Designated Officer against the proposed change, and the man-days claimed shall not exceed the man-days assessed in the approved impact analysis.
- The successful bidder shall be responsible for extending the validity date and the claim period of all guarantees, warranties and bonds furnished under the contract on account of any delay attributable to the successful bidder, at its own cost.
- All source code, models, data, reports and documentation generated under this contract shall be the property of CIL and shall be submitted to CIL in soft copy, as provided in Clause 3.J.
- The requirement of reports and documents may vary depending upon the availability of data or documents.

6. OTHER CONDITIONS

The above specified scope of work is indicative and not exhaustive and the bidder is deemed and obliged to provide all necessary equipment / infrastructure / accessories / licences and/or services within the quoted cost for successful implementation / completion of the entire work scope / project, as the case may be.

In case of any overlap or inconsistency between the clauses of this Scope of Work and the Annexures, the clauses of this Scope of Work shall prevail.

Sample Documents and data to be shared with bidders for Live Demonstration:

- i. For the purpose of the technical presentation / demonstration forming part of the evaluation, CIL shall share with the shortlisted bidders a set of sample tender documents and sample offer documents, being documents of concluded tenders from which bidder identity and commercially sensitive particulars have been redacted.
- ii. The said documents shall be shared only after the bidder has furnished to the Tender Inviting Authority a Non-Disclosure Agreement via mail, before the due date of submission of bids.
- iii. The documents shall be made available to the shortlisted bidder through QCBS method in ITB through a secure access mechanism designated by CIL. The documents shall be used solely for the purpose of responding to and participating in this tender, shall not be transferred, reproduced or retained beyond the tender process, and shall be certified as destroyed by the bidder on conclusion of the tender.
- iv. This bid document and the tender process flow details described herein are proprietary to CIL, are issued to the bidder for the exclusive purpose of participating in this tender, and shall not be transferred, reproduced, published or used for any other purpose without the prior written permission of CIL. All costs of preparing and submitting the offer shall be borne by the bidder.

7. TIME SCHEDULE OF TENDER

- i. Bid Start Date/Time: Will be defaulted to the date/time when bid is published.
- ii. Bid Duration: 30 days.
- iii. Pre-Bid Meeting: As mentioned in GeM Portal
- iv. Bid End Date/Time: 30 × 24 hrs from the Bid Start Date/Time.
- v. Bid Opening Date/Time: 24 hrs after Bid End Date & Time / Date & time mentioned in the GeM Bid Document.
- vi. Seek Clarification / Representation: As per GeM Portal.

Note:

- The work is not splittable.
- If the number of bids received online is found to be less than three on the end date of bid submission, the last date of submission of bid and the date of opening of tender will be auto-extended at the time of bid opening as per GeM functionality for a period of four days. If any of the extended dates falls on a Sunday/holiday, i.e. a non-working day, the same shall be rescheduled to the next working day. This extension shall also apply in case of receipt of zero bids.

- Bidders will have the right to modify / withdraw their bids during the extended period of submission of bids as per GeM functionality.
- The validity period of the tender shall be decided based on the final end date of submission of bids.
- The Employer reserves the right to issue corrigendum/addendum and it shall be binding on the part of the Bidders.
- It is the bidder's responsibility to comply with the system requirements, i.e. hardware, software and internet connectivity at the bidder's premises to access the GeM portal. Under no circumstances shall CIL be liable to the bidders for any direct/indirect loss or damages incurred by them arising out of incorrect use of the e-tender system or internet connectivity failures.
- The Company is not under any obligation to accept the lowest bid/bids and reserves the right to reject any or all the bids without assigning any reason whatsoever, and also to accept the tender in part and not in its entirety, at its sole discretion.
- The Company reserves the right to extend the date of submission and opening of bid or to cancel the bid without assigning any reason whatsoever. Any addendum/corrigendum/date extension in respect of the above tender will be published on the GeM portal only. Bidders are therefore requested to visit the portal regularly to keep themselves updated.
- Canvassing in connection with the tenders in any shape or form is strictly prohibited and tenders submitted by such tenderers who resort to canvassing shall be liable for rejection.
- The Bidders should submit bid for the whole work mentioned in the Bid Document.
- The successful Bidder will be expected to complete the work by the Intended Completion Date specified in the tender document.
- The price bids of the tenderers shall have no condition.

8. PRE-CONTRACT INTEGRITY PACT

Bidders are required to accept the pre-contract integrity pact as available in the Bid Document through the Bid Submission Confirmation Sheet provided in the GeM Bid Document. This will be signed by the authorised signatory of the Bidder(s) with name, designation and seal of the Company at the time of execution of the formal agreement.

Name, address and contact number of the Independent External Monitor (IEM) are as follows:

Name	Address	e-mail ID	Contact Number
Mr. K.D. Tripathi IAS (Retd.)	A-5, Sector-19, Noida UP- 201301	tripathikd.1958@gmail.com	9868506966
Mr. O.P. Singh IPS (Retd.)	M-6, First Floor, Green Park Extension, New Delhi- 110016	ops2020@gmail.com	9818564455

Name	Address	e-mail ID	Contact Number
Shri Rakesh Mohan, IA&AS (Retd.)	Flat No. 7020, Sector B-10, Vasant Kunj, New Delhi-110070	rmohan1987@gmail.com	9205175050

9. PROCUREMENT OF SERVICES THROUGH GeM PORTAL

- a) The guidelines issued by GeM / Gol from time to time through Notification / Circular / Office Memorandum will be followed for procurement through GeM (only if mandated by GeM Portal), even if the same are either not specifically indicated in the NIT or not in line with the provisions of CIL Manuals.
- b) The other provisions which are not mandated by the GeM portal shall be guided as per the respective Manuals / Guidelines of CIL.

**Tender Inviting Authority
Coal India Limited**