RFP for License Renewal and Annual Technical Support of Data Encryption Solution for i3MS Project, DoMG, Govt. of Odisha

RFP No. STPI/BBSR/PMC/2025-26/01

ENVISAGED BY

Directorate of Mines & Geology

Department of Steel & Mines

Govt. of Odisha

Software Technology Parks of India

(Ministry of Electronics & Information Technology (MeitY), Govt. of India)

Bhubaneswar, Odisha

Table of Contents

1 Invitation for System Integrator

Software Technology Parks of India (STPI), Bhubaneswar invites **"RFP for Selection of System Integrator for the License Renewal and Annual Technical Support of Data Encryption Solution for i3MS Project"** through the STPI's System Integrator empanelment process**.** This RFP document is being shared to the STPI empanelled system integrators. All empanelled system integrators are requested to go through the document and the interested SI shall participate in this bid, through submitting the techno-commercial proposal only in a sealed envelope mentioning the RFP No. in the top of the envelope either in person or by post/courier to Director, Software Technology Parks of India, STPI-ELITE Building, Plot No. 2/A, IDCO Industrial Area, Gothapatna, PO-Malipada, Bhubaneswar, Odisha, Pin Code- 751003 on or before **23/05/2025, 5:00 PM**. System Integrator are expected to examine the RFP document carefully. Failure to furnish all information required as per the RFP Document may result in the rejection of the Techno commercials. Techno commercial proposal will not be accepted after the above-mentioned date and time. Any subsequent corrigendum/ clarification will be made available by email.

Yours Sincerely

Director

Software Technology Parks of India

STPI ELITE Building, Plot. No. 2/A, IDCO Industrial Area,

Gothapatna, Malipada, Bhubaneswar, Pin Code: 751003, Odisha

2 Introduction

2.1 About the Directorate of Mines and Geology

The Directorate of Mines and Geology, Odisha functions under the administrative control of Steel & Mines Department of Odisha. The major functions of the Directorate are:

- Administration of mines & minerals
- Processing of mineral concession applications
- Collection of mineral revenue
- Prevention & control of illegal mining & smuggling of minerals
- Enforcement of statutory provisions for exploration of minerals
- Peripheral development of mining areas
- Chemical analysis of ores & minerals etc.

Directorate of Mines & Geology has its head office at Bhubaneswar and carries out the administrative functions through 14 circle mining offices located in different parts of the State.

2.2 Software Technology Parks of India (STPI)

Software Technology Parks of India (STPI) was established during the year 1991 by Ministry of Communications & IT, under Department of Electronics & IT, (The then Department of Electronics) Govt. of India with distinct focus for promotion of IT/ITeS exports from the country by providing single window regulatory services under STP & EHTP schemes, plug & play incubation facilities for the start-up companies and young entrepreneurs as well as High Speed Data communication services for a seamless access for offshore IT/ITeS exports. STPI has been successfully delivering Statutory services to the IT/ITeS industries in most industry friendly environment and has earned the goodwill of the industry for its liberal style of functioning.

STPI has pan-India presence with 67 centres across the country including at Bhubaneswar, Rourkela, Berhampur, Balasore, Jeypore and Jajpur in the State of Odisha.

STPI maintains internal resources to provide consulting, training and implementation services. Services cover Network Design, System Integration, Installation and Maintenance of application networks and facilities in varied areas.

The basic objectives of the Software Technology Parks of India are:

(a) To promote the development and export of software and software services including Information Technology (IT) enabled services/ Bio- IT.

(b) To provide statutory and other promotional services to the exporters by implementing Software Technology Park (STP)/ Electronics Hardware Technology Park (EHTP) schemes and other such schemes this may be formulated and entrusted by the Government from time to time.

(c) To provide Data Communication services including Value Added services to IT/IT enabled services (ITeS) related industries.

(d) To promote micro, small and medium entrepreneurs by creating conducive environment for entrepreneurship in the field of IT/ITES.

MeitY, Govt. of India while framing the policies to boost Software sectors with distinct focus at software exports nationwide identified Bhubaneswar to be one of the spot to set up Software Technology Park of India.

2.3 About i3MS

Integrated Mines & Minerals Management System (i3MS) was designed for effective monitoring of Mineral Administration in the State of Odisha. The seminal features of i3MS are:

(a) End to end tracking of Mineral Ore from Source till (Rail, Port & Industry Head)

(b) First application in the Country to have integrated with Freight Operating Information System (FOIS) of Indian Railways.

(c) First application to integrate with the RTO, Vahan & Sarathi database in real time

(d) Integrated with Commercial Tax Department for real time validation of the TIN and generation of e-Waybill.

(e) 6 major Ports are integrated with i3MS to provide information of export & import of minerals.

(f) Collection of mining revenue online to Odisha Treasury

i3MS enables the department and other regulating bodies to administer, monitor and undertake activities such as issuance/renewal of licenses and leases, collection of royalties, taxes etc., issuance of permits and transit pass. The department now has a repository of 14 years' worth data related to the mining operations within the state.

The information collected and stored in the department's database dates back to 2010-11. Over the years, the system has catered to 200 mining Leases that have dispatched 3571.409 MMT (2010-2025) of minerals through engagement of over 2.18 Lakh vehicles. The system has handled monetary transactions of over INR 42,066.24 Crores through revenue collection for FY 2024-25.

The various milestones in the augmentation of i3MS as a holistic mines and mineral management system are cited below:

Year	Achievement
2010	Development of Application
2010	Deployment of Dedicated Server Environment at Portal Centre
2013	Deployment of Full phase Server Environment at Odisha State Data Centre (OSDC)
2016	Deployment of High Availability (HA) Environment at OSDC
2019	Deployment of Business Continuity Plan (BCP) at STPI Data Centre
2020	Implementation of Data Encryption Solution & Mining lease Grant (EoDB)
2021	Implementation of AR- enabled Sampling and Testing of ore saleable
2022	Implementation of Weighbridge Automation System
2022	Implementation of IoT enabled Sampling Lab

The ERP application, i3MS, is a repository of gargantuan amounts of sensitive and transactional data of various stakeholders of mining administration as well as operations. This data also maps out the revenue path of the state facilitating authorities in decision making regarding financial and administrative concerns. As an end-to-end solution, the system also deals with collections of royalties and other fees in addition to material movement and real time tracking.

Data is a critical asset that holds the key to unlocking empowerment, progress and innovation in economies worldwide. To unleash its potential, organizations need to inspire confidence in their ability to keep data safe and secure. STPI acknowledges the Department's vision of safeguarding this data for which intend to implement the objective with the help of selected System Integrator through this RFP, highlighting the feasibility and approach for renewal and support of Data Encryption Mechanism for i3MS. In addition, considering the stringent time frame available for complying with the upcoming, data protection regime, STPI on behalf of the Directorate intends to engage a system integrator to renewal and support of solution for protection of the sensitive and critical personal data available in i3MS.

3 Instruction to System Integrator

3.1 Introduction

a) STPI will select a System Integrator (SI) in accordance with the method of selection specified in the STPI's SI empanelment process.

b) The date, time and address for submission of the proposals have been mentioned in the "Invitation for System Integrator" section of the RFP.

c) The eligible System Integrators are invited to submit their Proposal, for assignment - **"RFP for Selection of System Integrator for the License Renewal and Annual Technical Support of Data Encryption Solution for i3MS Project"**.

d) SI should familiarize themselves with the existing project conditions and take them into account for preparing their Proposals.

e) STPI will provide assistance to the SI's including inputs and facilities specified in the Data Sheet, for obtaining licenses and permits needed to carry out the Assignment, and make available relevant project data and reports.

f) SI's shall bear all costs associated with the survey, system study, preparation and submission of their proposals and contract negotiations. STPI is not bound to accept any proposal, and reserves the right to annul the selection process at any time prior to contract award, without assigning any reason or reasons and will in no case incurring any liability to the Agencies.

3.2 Definitions

a) "STPI" means the "Software Technology Parks of India" that has invited the system integrator (SI) for selection of System Integrators and with which the selected SI signs the Contract for the Services and to which the selected SI shall supply the necessary license software and provide technical support services as per the terms and conditions of the RFP.

b) "SI" means "System Integrator" - any entity or person or association of persons who is eligible to submit proposals to provide technical support services to the STPI's under this Contract.

c) "Contract" means the Contract signed between the System Integrator and STPI.

d) "Project specific information" means such part of the Instructions to SI's used to reflect specific project and assignment conditions.

e) "Day" means calendar day.

f) "Government" means the Government of Odisha unless otherwise specified.

g) "Instructions to System Integrator" means the document, which provides the system integrator with all information needed to prepare their proposals.

h) "Proposal" means the Technical Proposal and the Financial Proposal.

i) "RFP" means the Request for Proposal prepared by STPI for the selection of SI.

j) "Assignment / job" means the work to be performed by the SI pursuant to the Contract.

k) "Sub-agencies" means any person or entity to which the SI subcontracts any part of the Assignment/job.

3.3 Clarification and Amendment of RFP Documents

a) System Integrators may request a clarification on any clause of the RFP documents up to the number of days indicated in RFP before the proposal submission date. Any request for clarification must be sent by email to STPI's email id indicated in the RFP. The STPI will respond by email only. Should the STPI deem it necessary to amend the RFP as a result of a clarification, it shall do so following the procedure under Para 3.3 (b) below.

b) At any time before the submission of Proposals, the STPI may amend the RFP by issuing an addendum by email. The addendum shall be sent to all system integrators and will be binding on them. System integrators shall acknowledge receipt of all amendments. To give SI's reasonable time in which to take an amendment into account in their Proposals the STPI may, if the amendment is substantial extend the deadline for the submission of Proposals.

3.4 Language of Empanelment Process & Correspondence

The empanelment process will be submitted by the system integrator in English language only. All the documents relating to the empanelment process supplied by the System Integrator should also be in English, and the correspondence between the system integrator & STPI will be in English language only.

3.5 Proposal

The System integrator may submit one proposal only. If a system integrator submits or participates in more than one proposal, all such proposals shall be disqualified.

3.6 Proposal Validity

The period of validity from the date of submission of the proposals by SI's will be 180 days. During this period, the technical and financial proposal shall remain unchanged. The STPI will make its best effort to award the contract within this period. However, STPI may request for extension of the validity period of their proposals. Any SI that does not agree, has the right to refuse to extend validity of their Proposals; under such circumstance, STPI shall not consider such proposal for further evaluation.

3.7 Preparation of Proposals

a) The Proposal and all related correspondence exchanged by the SIs and STPI shall be in English language, unless specified otherwise.

b) In preparing their proposal, SI's is expected to examine in detail the documents comprising the RFP. Material deficiencies in providing the information requested may result in rejection of a Proposal.

c) While preparing the Technical Proposal SI's must give particular attention to the following:

   i. If a short-listed System Integrator considers that it may enhance its expertise for the assignment/job by associating with other SI in sub- SI, it may associate with a non-short-listed SI.

ii. While preparing the proposal, the SI must ensure that it proposes the minimum number and type of materials and experts as sought by STPI, failing which the proposal shall be considered as incomplete.

d) Depending on the nature of the assignment, agencies are required to submit a Technical Proposal (TP).

e) Financial Proposals: The Financial Proposal shall be submitted in the prescribed tables/format as per the RFP. It shall list all costs associated with the assignment/job, including (a) License of Software & COTS cost (b) Remuneration of the Resources deployed etc. The financial proposal shall not include any conditions attached to it and any such conditional financial proposal shall be rejected summarily.

3.8 Taxes

The Bidder shall fully familiarize themselves about the applicable taxes (such as: Good & Service Taxes, income taxes, duties, fees, levies) on amounts payable by STPI under the Contract. All such taxes must be included by the agency in the financial proposal. However, any addition in Taxes notified by Government of India time to time shall be paid separately at the time of billing as per actuals.

3.9 Currency

System Integrator shall express the price of their assignment/job in Indian Rupees (INR) only.

3.10 Performance Security

STPI will require the SI to provide a Performance Bank Guarantee within 15 days from the Notification of award for a value equivalent to 5% of the quoted project cost for each year excluding taxes. The Performance Guarantee shall be renewed annually and the value of performance security shall be revised commensurately to the tune of revised quote annually. The SI shall be responsible for extending the validity date and claim period of the Performance Guarantee as and when it is due on account of non-completion or extension of the project duration.

In case the SI fails to submit performance guarantee within the time stipulated, STPI at its discretion may cancel the order placed on the SI without giving any notice. STPI shall invoke the performance guarantee in case the selected SI fails to discharge their contractual obligations during the period or STPI incurs any loss due to SI's negligence in carrying out the renewal of license and technical support services as per the agreed terms & conditions.

3.11 Forfeiture of Security Deposit/Performance Guarantee

a) If the successful SI refuse/fails to accept Purchase Order issued by STPI or the job assigned to the SI are not done as per the scope of work/schedule of requirement, Security Deposit will be forfeited.

b) If the SI withdraws its application during the empanelment process before/after finalization of the tender, EMD will be forfeited.

c) If the contract is terminated by STPI due to poor supply/violation of any clause of agreement or any bad act of selected SI, security deposit/PG will be forfeited.

d) In case of unreasonable price quoted by the SI that may disrupt any part of the entire part of the tender process EMD, of such bidder(s) will be forfeited.

3.12 Rejection of the System Integrator

a) The SI is expected to examine all instructions, formats, terms & conditions, and scope of work in the bid document. Failure to furnish complete information or false information/documents which is not substantially responsive to the bid document in all respect shall result in rejection of bid.

b) In respect of interpretation/clarification of this bid document and in respect of any matter relating to this bid document, the decision of STPI-Bhubaneswar shall be final.

c) The SI will have to furnish the requisite document as specified in the bid document, failing which the bid will be considered as incomplete and is liable to be rejected.

3.13 General Terms and Conditions

a) Prices quoted by the SI's should include all local taxes, GST, duties, levies etc., till the empanelment process validity period.

b) The SI has to submit the OEM authorization for sale, support and service.

c) Delivery/ installation of the solution should strictly be completed within the stipulated period of delivery. Any incident during installation will be bidder's risks.

d) Rate/Price should be clearly quoted in figures as well as in words separately in the prescribed format attached with make & model. Rate/Price quoted should be inclusive of excise duty if any and taxes (GST), freight, insurance etc.

e) The quoted price shall be firm and fixed and there shall be no change. No additional charges shall be paid other than quoted price in the bid.

f) STPI reserves the right to vary the bill of quantity and the bidder shall supply at the unit price quoted in the bid and the payment shall be done based on total unit price only.

3.14 Cancellation by Default

STPI may without prejudice to any other remedy for breach of terms and conditions, including forfeiture of Performance Security by written notice of default sent to the company, terminate the work / task in whole or in part after sending a notice to the system integrator in this regard. If the system integrator fails to deliver or complete the job assigned in the terms and conditions within the time period (s) specified in the RFP and if the system integrator fails to perform any other obligations under the terms and conditions.

3.15 Blacklisting

Company/Firm blacklisted by Govt. / PSU organization are not eligible to participate in the bidding process. If at any stage of bidding process or during the currency of work order, such information comes to the knowledge of STPI, STPI shall have right to reject the bid or cancel the work order, as the case may be, without any compensation to the bidder. The bidders have to be submitted an undertaking for not being black listed since last 3 years by any Govt./ PSU organization.

3.16 Arbitration and Conciliation Act

The parties shall make every effort to resolve amicably by direct informal negotiations,

any disagreement or disputes, arising between them under or in connection with the tripartite agreement.

If the parties fail to settle such dispute or difference amicably within 15 days of such disputes or differences having first arisen then such dispute(s) or difference(s) shall be referred to Government for a decision in the matter, which will be binding on the parties. If the dispute(s) or difference(s) remain, then such dispute(s) or difference(s) shall be referred to the arbitration and conciliation act 1996 by the sole arbitrator selected by Director General, STPI.

3.17 Confidentiality

Any information pertaining to STPI or any other agency involved in the project, matters concerning STPI or with the agency that comes to the knowledge of the Bidder in connection with this contract will be deemed to be confidential and the Bidder will be fully responsible for the same being kept confidential and held in trust, as also for all consequences of its concerned personnel failing to do so. The Bidder shall ensure due secrecy of information and data not intended for public distribution.

3.18 Force Majeure

If, at any time, during the continuance of the agreement, the performance in whole or in any part by either party of obligation under the agreement shall be prevented or delayed by reasons of any war, hostile acts of the enemy, civil commotion, subrogate, fire, floods, earthquakes, explosions, epidemics, strikes and quarantine restrictions by acts of God,(herein after referred to as eventualities) then provided notice of the happening of any such eventualities is given by either party to the other within two days from the date of occurrence thereon, neither party shall, by reason of such eventualities be entitled to terminate this contract agreement nor shall either party have any claim of damages against the other in respect of such non-performance or delay in performance. Performance of the contract agreement shall, however be resumed as soon as practicable after such eventuality has come to an end.

3.19 Pre-Bid Query

Pre-bid queries if any can be submitted to email id anilkumar.hembram@stpi.in

4 Appointment of System Integrator or Service Provider

4.1 Award of Contract

- SI selection process shall be done by the bid committee by comparing the technical (T1) with the highest technical score and commercial (L1) with the lowest priced bid (L1) received from the STPI's empanelled SI only. STPI shall issue a Purchase/Work Order to the selected SI, prior to the expiry of the period of Bid validity.
- The Successful SI shall give his acceptance within 7 days from the date of issue of PO/WO.
- The SI is expected to commence the assignment/job on the date and at the location specified in the RFP.

- Liability of the successful SI to perform the job will commence from the date of PO. The Completion Period shall be counted from the date of PO.

4.2 Right to Accept Any Proposal & Reject Any / All Proposal(s)

STPI reserves the right to accept or reject any proposal, and to annul the tendering process / Public procurement process and reject all proposals at any time prior to award of contract, without thereby incurring any liability to the affected bidder or bidders or any obligation to inform the affected bidder or bidders of the grounds for such action.

4.3 Notification of Award

The notification of award will constitute the formation of the contract. Upon the successful SI's furnishing of Performance Bank Guarantee.

4.4 Implementation

The solution proposed by the system integrator shall cater to the following requirement:

4.4.1 File and Database Encryption

File and Database Encryption should be implemented to protect on premise data from theft and misuse. The solution should facilitate segregation of duties and access on a role and right basis. It should limit access to sensitive data. The security mechanism should be designed to meet compliance regulations determined by the government as well as globally practice industry standards.

Encryption and decryption operations should be conducted without any consequential loss on system performance. The solution should be highly scalable for heterogeneous environments and shall facilitate the following:

- Transparent encryption and decryption
- Secure, centralized key and policy management
- Granular support for regulatory compliance
- Live data transformation
- Seamless integration across **on-premises**, **public**, and **private cloud** infrastructures.
- Ensure that access to encryption keys and sensitive operations is restricted based on **user roles and permissions**.
- Provide comprehensive logs of encryption/decryption activity to support **forensic analysis**, **compliance audits**, and **anomaly detection**

- Ensure **redundancy**, **failover capabilities**, and **data resilience** to avoid disruptions in case of system failures.
- Encrypt data **stored**, **moving across networks**, and **actively being processed**, enabling **end-to-end security**.

4.4.2 Data Protection for Databases

Use of hardware acceleration (e.g., AES-NI, TPM, HSMs) and efficient algorithms to minimize latency and resource consumption. Data Protection for Databases. Data Protection solution for databases should provide automated sensitive data discovery and classification, real-time data activity monitoring and cognitive analytics to discover unusual activity around sensitive data. It should protect against unauthorized data access by learning regular user access patterns. It should also have provision for generating real-time alerts on suspicious activities. It should dynamically block access or quarantine user IDs to protect against internal and external threats and also help streamline and automate compliance workflows. The product should be built on a scalable architecture that provides full visibility on data activity across all major databases.

Data protection solution shall facilitate:

4.4.2.1 Data Confidentiality

- Encryption of data **at rest**, **in transit**, and optionally **in use**
- Secure key management (e.g., centralized, hardware-backed)
- Access controls to prevent unauthorized data exposure

4.4.2.2 Data Integrity

- Mechanisms to detect **unauthorized changes** (e.g., checksums, digital signatures)
- Version control and integrity checks for stored and transmitted data

4.4.2.3 Data Availability

- **Backup and recovery systems** with versioning and redundancy
- High availability (HA) and **disaster recovery (DR)** support
- Protection against ransomware and other data-denial threats

4.4.2.4 Access Control and Authentication

- Role-Based Access Control (RBAC) and/or Attribute-Based Access Control (ABAC)
- Strong user authentication (e.g., MFA, SSO integration)
- Audit trails for user and admin activity

4.4.2.5 Regulatory Compliance

- Adherence to standards such as **GDPR**, **HIPAA**, **PCI DSS**, etc.

- Support for data classification, retention policies, and audit logs

4.4.2.6 Scalability and Flexibility

- Support for **multi-cloud**, **hybrid**, and **on-premises** deployments
- Easily scalable to accommodate data growth and new applications

4.4.2.7 Granular Policy Enforcement

- Ability to define and apply protection policies at the **file, folder, database**, or **user** level
- Context-aware policies (e.g., location, device, behaviour-based rules)

4.4.2.8 Comprehensive Monitoring and Reporting

- Real-time alerts and dashboards for data access and anomalies
- Detailed reporting for compliance and internal auditing

4.4.2.9 Integration Capabilities

- APIs and connectors for seamless integration with **SIEM**, **DLP**, **IAM**, and other security tools
- Plug-and-play compatibility with existing enterprise systems

4.4.2.10 User Awareness and Training

Built-in support for **user education**, **data handling guidelines**, and **incident response training**

4.4.3 Vulnerability Assessment

Vulnerability Assessment solution should enable the facility of scanning data infrastructures (databases, data warehouses and big data environments) to detect vulnerabilities, and suggest remedial actions. The solution should identify exposures such as missing patches, weak passwords, unauthorized changes and misconfigured privileges. Full reports should be provided along with suggestions to address all vulnerabilities. It should detect behavioural vulnerabilities such as account sharing, excessive administrative logins and unusual after-hours' activity. It should identify threats and security gaps in databases that could be exploited by hackers. This solution shall facilitate:

4.4.3.1 Comprehensive Asset Discovery

- Identify all **hardware**, **software**, **network devices**, and **cloud resources** in the environment.
- Include **shadow IT** and unmanaged devices for full visibility.

4.4.3.2 Automated Vulnerability Scanning

- Use automated tools to **scan systems** regularly for known vulnerabilities (CVEs).

- Support for different environments: **on-premises, cloud, containers, mobile**, and **IoT**.

4.4.3.3 Accurate Vulnerability Detection

- Maintain an up-to-date vulnerability database (e.g., NVD, vendor advisories).
- Detect **misconfigurations**, **outdated software**, **open ports**, and **weak credentials**.

4.4.3.4 Risk Scoring and Prioritization

- Assess vulnerabilities based on severity (e.g., CVSS score), **exploitability**, and **business impact**.
- Prioritize issues that pose the greatest risk to critical assets.

4.4.3.5 Contextual Analysis

- Understand the **context of each vulnerability**, including affected systems, usage, and exposure.
- Consider environmental factors like network segmentation and existing controls.

4.4.3.6 Reporting and Dashboards

- Provide clear, actionable reports for **technical teams** and **executive stakeholders**.
- Include **remediation steps**, timelines, and trends over time.

4.4.3.7 Integration with Patch Management

- Link assessment results with **patching tools** and processes for efficient remediation.
- Automate ticket generation for IT teams (e.g., through ServiceNow, Jira).

4.4.3.8 Compliance Mapping

- Align with regulatory standards such as **PCI DSS**, **HIPAA**, **ISO 27001**, **NIST**, etc.
- Provide audit-ready documentation and evidence of remediation efforts.

4.4.3.9 Continuous Assessment and Monitoring

- Support **scheduled scans**, **on-demand scans**, and **real-time assessments**.
- Adapt to changing environments and emerging threats.

4.4.3.10 Remediation Tracking

- Track the status of fixes and verify successful remediation.
- Re-scan to confirm vulnerabilities are closed.

4.5 Bill of Quantity

#	Item Description	Quantity
1.	Software Assurance (SA) of IBM Security Guardium Tools	
1.1.	Data Protection for Databases Resource Value Unit	1
1.2.	Vulnerability Assessment for Databases	1
1.3.	Collector Software	3
1.4.	Aggregator Software	2
1.5.	File and Database Encryption	3
1.6.	Data Encryption Key Management	3
2.	Servers for Security	
2.1.	Annual Maintenance Service for Servers	5
2.2.	Technical Support (Crypto analyst)	1

4.6 Roles & Responsibility

Activity	SI	STPI/ Directorate
Supply of Licenses	✓	
Installation of Licenses	✓	
Necessary Permissions & Clearances		✓
Coordination with i3MS SI/Vendor	✓	
Coordination for SDC and STPI DC Access		✓

4.7 Project Schedule

Sl.#	Activity/ Milestone	Timeline
1.	System Study/ Requirement Gathering	T0 + 2 days
2.	Procurement of Software Assurance (SA) of IBM Security Guardium Licenses & Tools	T0 + 5 days
3.	Installation, Commissioning & Monitoring	T0 + 7 days
4.	Annual Maintenance Support for Servers	T0 + 33 Months
5.	Software Assurance (SA) for Software	36 months from the date of expiry of the license.
6.	Technical Support (Crypto analysis)	T0 + 33 Months

T0 = Date of Award of Contract

4.8 Self-Declaration: Not Blacklisted (in company letterhead)

To

Director,

Software Technology Parks of India,

Bhubaneswar, Odisha

In response to the RFP No. <<RFP No. >>, for RFP titled "Selection of System Integrator for the License Renewal and Annual Technical Support of Data Encryption Solution for i3MS Project.", I/ We hereby declare that presently our Company/ firm is not under declaration of ineligibility for corrupt & fraudulent practices, blacklisted either indefinitely or for a particular period of time, or had work withdrawn, by any State/ Central government/ PSU.

If this declaration is found to be incorrect then without prejudice to any other action that may be taken, my/ our security may be forfeited in full and the tender, if any to the extent accepted, may be cancelled.

Thanking you,

Name of the SI: .....

Authorized Signatory: .....

Signature:

Seal:

Date:

Place:

4.9 System Integrator's Authorization Certificate

(Company letterhead)

To

Director,

Software Technology Parks of India,

Bhubaneswar, Odisha

Subject: Proposal for the RFP for Selection of System Integrator for the License Renewal and Annual Technical Support of Data Encryption Solution for i3MS Project.

Reference No.: <<RFP No.>>

Sir,

<Name>, , <Designation> is hereby authorized to attend meetings & submit technical & commercial information as may be required by you in the course of processing the above said Bid. S/He is also authorized to attend meetings & submit technical & commercial information as may be required by you in the course of processing above said application for the purpose of validation, his/ her verified signatures are as under.

Thanking you,

Name of the SI: -

Verified Signature:

Authorized Signatory: -

Seal of the Organization: -

Date:

Place:

4.10 Acceptance of Terms & Conditions/Clauses

To

Director,

Software Technology Parks of India,

Bhubaneswar, Odisha

Sir,

I have carefully and thoroughly gone through the Terms & Conditions contained in the RFP Document [<<RFP No.>>] regarding Selection of System Integrator for the License Renewal and Annual Technical Support of Data Encryption Solution for i3MS Project.

I declare that all the provisions/clauses of this RFP/Tender Document are acceptable to my company. I further certify that I am an authorized signatory of my company and am, therefore, competent to make this declaration.

Thanking you,

Name of the SI: .....

Authorized Signatory: .....

Signature:

Seal:

Date:

Place:

4.11 Format for fairness of documents

(Company letterhead)

To

Director,

Software Technology Parks of India,

Bhubaneswar, Odisha

Sir

In response to the RFP No. <<RFP No.>> titled "Selection of System Integrator for the License Renewal and Annual Technical Support of Data Encryption Solution for i3MS Project", I/ We hereby declare that any documents or information submitted under this bid is without any doubt, true and fair, to the best of my/our knowledge.

If this declaration is found to be incorrect then without prejudice to any other action that may be taken, my/ our security may be forfeited in full and the tender if any to the extent accepted may be cancelled.

Thanking you,

Name of the SI: -

Authorized Signatory: -

Seal of the Organization: -

Date:

Place:

4.12 OEM Authorization Certificate

(Company letterhead)

To

Director,

Software Technology Parks of India,

Bhubaneswar, Odisha

Subject: Proposal for the RFP for Selection of System Integrator for the License Renewal and Annual Technical Support of Data Encryption Solution for i3MS Project.

Reference No.: <<RFP No. >>

Sir,

We manufacturers of original equipment's/cartridge at (address of factory) do hereby authorize M/s. (Name and address of Agent) to submit a bid, negotiate and receive the order from you against your tender enquiry/GeM Bid _____in Delhi region.

No company, firm, or individual other than M/s. (Name with complete address and phone number) is authorized to bid, and conclude the contract in regard to this business.

We hereby extend our full guarantee for supplying of Original IBM Licenses and services offered by the above firm.

Thanking you,

Name of the SI: -

Verified Signature:

Authorized Signatory: -

Seal of the Organization: -

Date:

Place:

4.12.1 Summary Cost

SL #	Components	Basic Cost	GST @ 18%	Total
A	Operational Expenses along with Software Assurance (Year-1)			
B	Operational Expenses along with Software Assurance (Year-2)			
C	Operational Expenses along with Software Assurance (Year-3)			
			Total (in Figures)	
Total (in Words)				

4.12.1.1 Operational Expenses along with Software Assurance (Year-1)

SL#	Capital Expenses (Year-1)	Unit	Qty	Basic Cost	GST @ 18%	Total
1	Software Assurance (SA) of Security Licenses (IBM) (From 1st Mar 2025 to 28th Feb 2026) or from current dt.	Lot	1			
2	Annual Maintenance Service for Servers (1st June 2025 to 28th Feb 2026)	Lot	1			
3	Technical Support (Crypt o analyst) (1st June 2025 to 28th Feb 2026)	Man Month	9			
4	Optional (Re-Installation, Re-Configuration)	Lot	1			
					Total (in Figures)	
Total (in Words)						

4.12.1.2 Operational Expenses along with Software Assurance (Year-2)

SL #	Recurring Expenses (Year-2)	Unit	Qty	Basic Cost	GST @ 18%	Total
1	Software Assurance (SA) of Security Licenses (IBM) (From 1st Mar 2026 to 28th Feb 2027)	Lot	1			
2	Annual Maintenance Service for Servers (From 1st Mar 2026 to 28th Feb 2027)	Lot	1			
3	Technical Support (Crypto analyst) (From 1st Mar 2026 to 28th Feb 2027)	Man Month	12			
					Total (in Figures)	
Total (in Words)						

4.12.1.3 Operational Expenses along with Software Assurance (Year-3)

SL #	Recurring Expenses (Year-2)	Unit	Qty	Basic Cost	GST @ 18%	Total
1	Software Assurance (SA) of Security Licenses (IBM) (From 1st Mar 2027 to 29th Feb 2028)	Lot	1			
2	Annual Maintenance Service for Servers (From 1st Mar 2027 to 29th Feb 2028)	Lot	1			
3	Technical Support (Crypto analyst) (From 1st Mar 2027 to 29th Feb 2028)	Man Month	12			
					Total (in Figures)	
Total (in Words)						

Note: Quantity may also increase/decrease depending on the actual requirement/ situation.

5 Scope of Work & Current Infrastructure

5.1 Scope

System Integrator to supply / renew the IBM security license and provide the Crypto Analyst with technical support for the project, which will be renewed on yearly basis post customer's confirmation.

- Onsite support service through a Crypto Analyst at DoMG-HO, Bhubaneswar with 9X6 as per the DoMG office timings & calendar
- Remote support services with 24X7 availability.
- Crypto Analyst shall meet the below minimum technical & experience requirement:

Job Description

a) Resolution for the incidents reported
b) Documentation & Reporting the Root Cause Analysis
c) Performing advanced activities like:
    - Driving Database Activity Monitoring (DAM) product fixes and enhancements
    - New system integrations (if any)
    - Analysing and addressing issues related to performance, stability, scalability and extensibility of the systems
    - Recommending DAM process improvements as and when required
        - Support Disaster Recovery (BCP / DR) Drills.

The proposed technical resource should possess the following qualification and skills:

Experience:

- B.E./ B. Tech / MCA equivalent with 5+ years in IT Security / Database Mgmt.

Skills:

- Expert knowledge and experience in deploying & management of IT Security, Database Activity Monitoring using multiple products.
- Strong experience in Database Activity Monitoring, Vulnerability Assessment and Data Encryption.
- Should have good integration knowledge.
- Good hands-on experience for IBM Guardium IT security & Databases.
- Should handle all the technical issues and meetings related to DoMG Data Encryption project in both SDC & STPI-DC locations.
- Should be capable of translating customer business requirement to Technical/ Functional requirement.

5.2 Stakeholders

Secure and robust IT infrastructure has been installed at SDC, for streamlining the administrative processes to improve the service delivery standards in mines area. The key stakeholders for the projects are: -

- Department of Steel & Mines
- Directorate of Mines
- Mining Circle Offices
- Government Check Gates' Users
- Mining Lease Holders
- Licensees:
    - Traders
    - Storage/ Depot
    - Processing Unit
    - Small consumers
- Transporters
- Truck Owners
- Indian Railway
- Ports
- Indian Bureau of Mines
- Other Government Departments

5.3 IT Infrastructure at OSDC

5.3.1 Server Infrastructure

A dedicated server environment is installed at OSDC in a co-location mode. The Server infrastructure is provided by the DoMG, GoO and other infrastructure like Network, Storage, Power, Security and cooling are provided by OSDC. The necessary security policy is followed for this organization. The server infrastructure is given below:

Application/Web Server: The application servers are configured with Load-balancing mode. The hardware load balancer of OSDC is used for this purpose. Multiple applications are running in the servers. The load balancer is configured to distribute the load between multiple application servers. Necessary configuration on forwarding request is done in the load balancer.

- Web environment: IIS 8.5
- Frame work: .Net 4.0

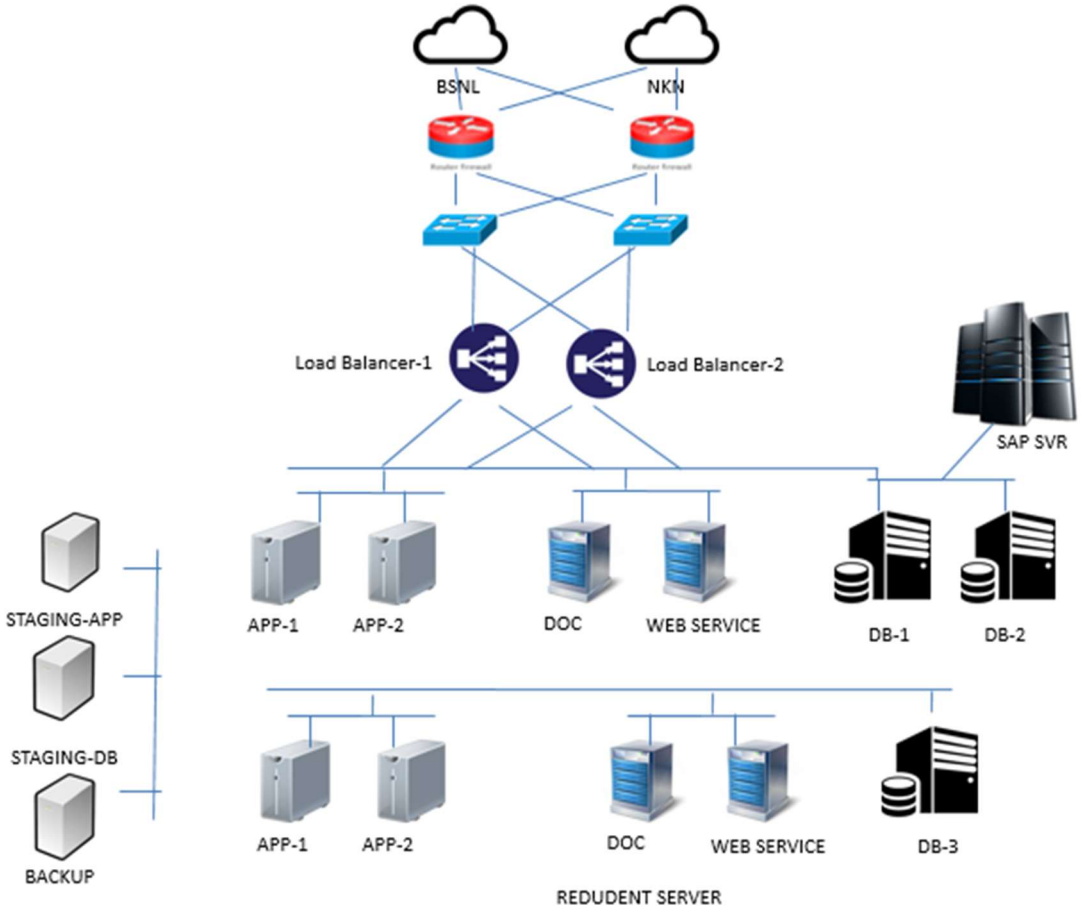
Database Server: The database servers are configured in cluster mode. Two servers are configured dedicatedly for this purpose. Another DB server is configured in standalone mode for backup purpose.

- RDBMS: MS SQL Server 2017 Enterprise

Document Server: As the applications are configured in load-balancing mode, a common document server is maintained for all application servers. The document server is configured in sharing mode.

Staging server: The staging server environment is available for application, web and DB servers. All the testing and modifications are done in this server before going to live server environment.

SAP Server: 2 servers are configured for SAP implementation.



5.3.2 Server Hardware

Servers			CPU	RAM	HDD	Purpose	Status
A	HP BLADE C3000	**HP BLADE CHASIS 1**					
1	HP BL460C G7 Blade	HP BLADE SERVER 1	8 Core **x** 2	64 GB	300 GB	Replication DB	Active
2	HP BL460C G7 Blade	HP BLADE SERVER 2	8 Core **x** 2	64 GB	300 GB	Document Server	Active
3	HP BL460C G7 Blade	HP BLADE SERVER 3	8 Core **x** 2	64 GB	300 GB	Web Server1 (i3ms)	Active
4	HP BL460C G7 Blade	HP BLADE SERVER 4	8 Core **x** 2	64 GB	300 GB	Web Server2 (i3ms)	Active
5	HP BL460C G7 Blade	HP BLADE SERVER 5	8 Core **x** 2	64 GB	300 GB		Not used

Servers			CPU	RAM	HDD	Purpose	Status
6	HP BL460C G7 Blade	HP BLADE SERVER 6	8 Core **x** 2	64 GB	300 GB	Support Server	Active
7	HP BL460C G9 Blade	HP BLADE SERVER 7	16 Core **x** 2	128 GB	300 GB	Staging DB	Active
8	HP BL460C G9 Blade	HP BLADE SERVER 8	16 Core **x** 2	128 GB	300 GB	Website and Services 1	Active
B	HP BLADE C3000	**HP BLADE CHASIS 2**					
9	HP BL460C G9 Blade	HP BLADE SERVER 9	32 Core **x** 2	256 GB	300 GB	DB Server1	Active
10	HP BL460C G9 Blade	HP BLADE SERVER 10	32 Core **x** 2	256 GB	300 GB	DB Server1	Active
11	HP BL460C G9 Blade	HP BLADE SERVER 11	16 Core **x** 2	128 GB	300 GB	Web Server3 (i3ms)	Active
12	HP BL460C G9 Blade	HP BLADE SERVER 12	16 Core **x** 2	128 GB	300 GB	Web Server4 (i3ms)	Active
13	HP BL460C G9 Blade	HP BLADE SERVER 13	16 Core **x** 2	128 GB	300 GB	SAP Server	Active
14	HP BL460C G9 Blade	HP BLADE SERVER 14	16 Core **x** 2	128 GB	300 GB	SAP Server	Active
15	HP BL460C G9 Blade	HP BLADE SERVER 15	16 Core **x** 2	128 GB	300 GB	Website and Services 2	Active
16	HP BL460C G9 Blade	HP BLADE SERVER 16	16 Core **x** 2	128 GB	300 GB	Document Server2	Not used

5.3.3 Other Infrastructure

Storage Environment: The database and document servers are connected to the SAN storage available at OSDC. They are facilitated with 1 TB storage each.

Backup Environment: As both application and database files are stored centrally at the SAN, provided by OSDC, so the backup policy of OSDC is followed for this application. The incremental and full back up is taken periodically as per policy.

Network Environment: As the servers are configured inside OSDC, so the network of OSDC is used for accessing the servers. The necessary configuration of Firewall and Network switch is configured for the servers and storage.

Connectivity: 10 Mbps ISP MPLS is connected between SDC and Directorate of Mines.

Internet: NKN internet is used in SDC to facilitate the WAN connection to all the applications hosted.

DR Provision: The SDC storage is connected with NDC. The replication of data has been done into NDC. The Near DC is configured at STPI DC. The replication of data is also plan to done at this location.

5.3.4 Software

#	Software	Details	Qty
1	Operating System	Windows server 2008 R2 Enterprise	6
2	Operating System	Windows server 2012 R2 Data Centre	10
3	RDBMS	MS SQL Server 2012 Enterprise Edition	2

5.3.5 Application/Websites

#	Software	Details
1	Website	www.odishaminerals.gov.in
2	Application	https://i3ms.odishaminerals.gov.in
3	Application	https://ds.odishaminerals.gov.in
4	Application	https://dmf.odishaminerals.gov.in
5	Application	http://docs.odishaminerals.gov.in
6	Application	SAP Application
7	Services	http://services.odishaminerals.gov.in

5.3.6 Modules running in the servers

Currently i3MS application is being used for managing and monitoring all mining related operations in the state. The application manages end-to-end solution to business critical problems. Most of them run on web platform on a 24X7 service delivery basis. The various modules constituting the system are:

- Mines and Licensee Profile
- Mineral Due Clearance Certificate
- Grant of New/ Renewal of Licensee
- Transit/ Transport Permit Management System
- Weigh Bridge Approval System
- Mineral Carrying Vehicle Registration

- Transporter Registration
- Vehicle Seizure
- OMPTS & Administrative Monthly Returns
- Demand Assessment on Royalty, DMF & NMET
- MCDR Returns
- e-Transit Pass through weighbridge automation system
- e-Transit Pass Software for licensee/ End User
- Small Consumer Registration & Return
- Reporting of Steel Plant MoU

5.3.7 Current Storage Size

DB Size	1000 GB without log
Replication DB	510 GB
Staging DB	110 GB
App	45 GB
Document (pdf)	2 TB
Space Allocated	20 TB

5.4 IT Infrastructure at STPI DC

The Near DC has been planned to execute at STPI DC. The below IT Infra has been deployed for this project.

5.4.1 Server Infrastructure

#	Server	Qty	Details
1	Application Server	2	VM-1 : Web Server1 (i3ms) VM-2 : Web Server2 (i3ms) VM-3 : Website and Services 1
2	Database Server	1	Installed & Configured at both DC
3	File Server	1	VM-1 : Document Server1 VM-2 : Web Server3 (i3ms) VM-3 : Support Server VM-4 : Staging Server

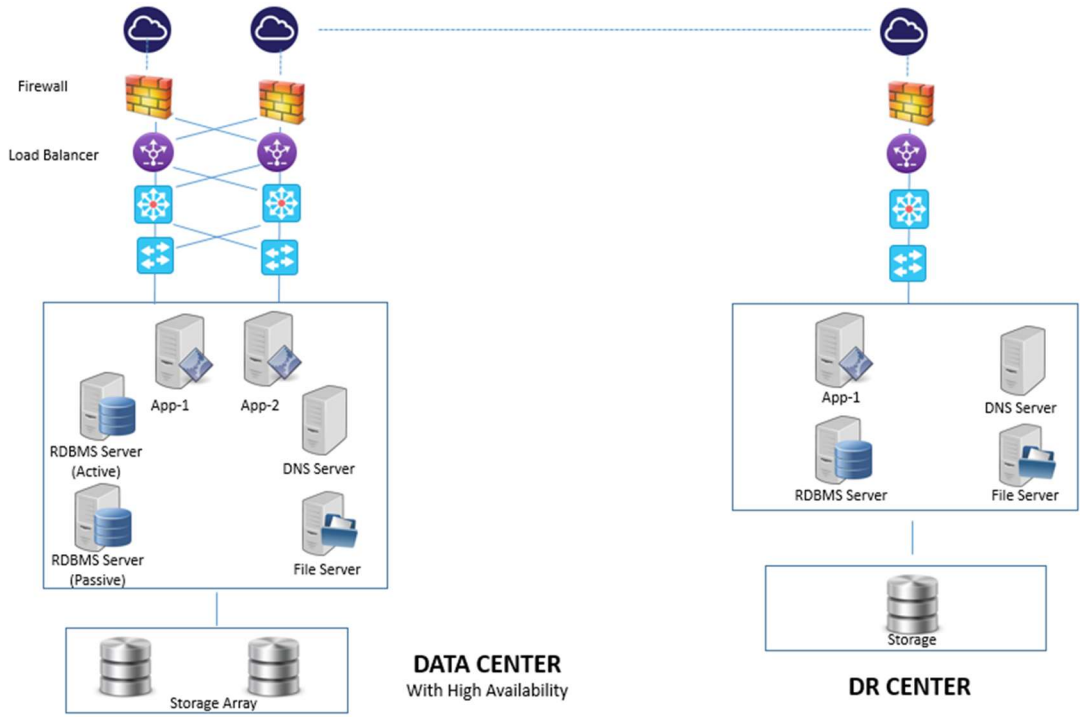
#	Server	Qty	Details
4	Other Server	1	VM-1 : Website and Services 2 VM-2 : Web Farm Server VM-3 : Document Server2

5.4.2 Other Infrastructure

- 20 TB SAN Storage has been provisioned dedicatedly to this environment.
- STPI has provided the Internet Connectivity to the servers.
- The MPLS connectivity is configured from STPI DC to OSDC
- Other Facilities are provided by STPI

5.4.3 Software

#	Software	Details	Qty
1	Operating System	Windows server 2008 R2 Enterprise	5
2	Operating System	Windows server 2012 R2 Data Centre	1



5.5 Security Requirement

The requirements of data security for this solution are.

- Classification of sensitive data related to data protection.
- Real-time data activity monitoring and cognitive analytics to discover unusual activity around sensitive data.
- Protects against unauthorized data access by learning regular user access patterns
- Provide real-time alerts on suspicious activities.
- Dynamically block access or quarantine user IDs to protect against internal and external threats
- Support both SQL and non-SQL database
- Data Protection for Files
- Help the right users have the right access to the right unstructured data.
- Data Protection for Files supports file
- Continuous monitoring and real-time security and protection policies protect unstructured data across the enterprise.
- Encryption capabilities to help protect file and database data on-premises from misuse.
- Separation of duties, so that administrators do not have free access to sensitive data.
- Encrypting file and database data helps organizations meet government and industry compliance regulations.
- This offering performs encryption and decryption operations with minimal performance impact and high scalability for heterogeneous environments.
- Event and Log Monitoring

i3MS applications consists of a number of modules that are of different nature and serve the requirements of different sets of stakeholders using the system.

Sl#	Module Name	SENSITIVITY	BUSINESS CRITICALITY	Priority (0-5)
1	Website	High	High	5
2	Mines and Licensee Profile	High	High	5
3	Permit Management	High	High	5
4	e-Pass Management	High	High	5
5	Grant of Licensee	High	High	4
6	Weigh Bridge Approval	High	High	4
7	Truck Registration	High	High	4
8	Transporter Registration	High	High	4
9	Mines State Returns (MPR)	High	High	3
10	Licensee State Return (OMPTS)	High	High	3
11	Mines IBM Returns	High	High	3
12	Licensee IBM Return	High	High	3
13	Demand Assessment	High	High	3
14	Due Clearance Certificate(MDCC)	High	High	2
15	Port Transaction	High	High	1
16	Seizure of Vehicle	Medium	Medium	1
17	Small Consumer Registration	Medium	Medium	2
18	Physical & Financial Reporting of MoU Signed Steel Plants	Low	Low	0
19	Ad Hoc Reporting	High	High	5
20	Audit Compliance	Medium	Medium	1
21	Litigation Case Management	Medium	Medium	1
22	Mail & SMS Integration	High	High	4
23	Road Transport Integration	High	High	5
24	Online Payment Integration	High	High	5
25	Commercial Tax Integration	High	High	1
26	Railway Integration	High	High	5
27	VTS Integration	High	High	5

The current system has the following security mechanism in place to cater to security threats:

- Regular third party application audit to ensure that the security criteria for the application are being complied as per the CERT-In Guideline.

- Network level security to fend any unauthorized incursions into the system at network level

However, considering the growth of business, some of the below major security provisions need to be implement in the solution.

- The information/data stored in database and file level needs to be encrypted to avoid un-authorized access.
- The data accessibility log needs to be provisioned in the system, so that the historic activities must be tracked.
- There must be some protection methodology within the system which make secure to the folder contents like mail, financial information, and other sensitive information.
- Real-time Monitoring provision of application and database level threats.