RAILTEL CORPORATION OF INDIA LIMITED

(A Govt. of India Undertaking)

Expression of Interest for Selection of Partner from Authorized LSP of Microsoft

For

" Provisioning of Microsoft Azure Cloud Services"

EOI No: RailTel/EOI /CO/EB/2025-26/Microsoft Azure Cloud Services/01 dated 14-October-2025

EOI NOTICE

Plate-A, 6th Floor, Office Tower-2, NBCC Building, East Kidwai Nagar, New Delhi-110023

EOI Notice No: RailTel/EOI /CO/EB/2025-26/Microsoft Azure Cloud Services/01 dated 14-Oct-2025

RailTel Corporation of India Ltd., (here after referred to as "RailTel") invites EOIs from Authorized LSP of Microsoft for the selection of suitable partner as Exclusive pre bid teaming arrangement for **"Provisioning of Microsoft Azure Cloud Services"**

The details are as under:-

1	Last date for submission of Technical Packet against EOIs by bidders	28-Oct-2025 at 11:00 Hours
2	Opening of Technical Bid of EOIs	28-Oct-2025 at 11:15 Hours
3	Number of copies to be submitted for scope of work	One
4	EOI fees inclusive tax (Non-refundable)	Rs. 5,900/- (Five Thousand Nine Hundred only)
5	Token EOI EMD	Rs. 5,00,000/- (Five Lakhs Only) to be submitted along with EOI **(To be submitted via online bank transfer only).** RailTel Bank Details: Union Bank of India, Account No. 340601010050446, IFSC Code - UBIN0534064. Partner needs to share the online payment transfer details like UTR No. date and Bank along with the proposal.

Eligible Authorized LSP are required to direct all communications related to this Invitation for EoI document, through the following Nominated Point of Contact persons:

Contact: Sh. Hemant Yadav
Designation: JGM/GB
Email: hemantyadav@railtelindia.com

Note: -

1. Empaneled partners are required to submit a soft copy of the technical packet through an e-mail at **eoi.ebco@railtelindia.com** duly signed by Authorized Signatories with Company seal and stamp.

2. The EOI response is invited from eligible authorized Microsoft Azure LSP.

3. All the documents must be submitted with **proper indexing** and **page no.**

4. This is an **exclusive pre-bid partnership arrangement with an empaneled business associate of RailTel for participating in the end customer RFP.** The selected partner's authorized signatory has to give an undertaking they will not submit directly or indirectly theirbids and techno-commercial solution/association with any other organization once selected in this EOI for pre-bid teaming arrangement (before and after submission of bid to the end customer organization by RailTel). This undertaking has to be given with this EOI Response.

5. **Transfer and Sub-letting.** The Business Associate has no right to give, bargain, sell, assign, or sublet or otherwise dispose of the Contract or any part thereof, as well as to give or to let a third partytake benefit or advantage of the present Contract or any part thereof.

Chapter-1

About RailTel

RailTel, a "Navratna" Central Public Sector Enterprise is an ICT provider and one of the largest neutral telecom infrastructure providers in the country owning a Pan-India optic fiber network. The OFC network covers important towns & cities of the country and several rural areas

Purpose of the Bid

RailTel intends to migrate existing and introduce new workloads to public cloud with an intent to optimize costs, scalability& reliability, robust security features and compliance certifications, ensuring that data and applications are protected against threats, modernizing applications using cloud-native technologies, which can drastically increase cost efficiency and enable faster innovation, support a wide range of workloads, including Oracle, SAP, SQL Server, and open-source databases, and providing RailTel customers with the flexibility to migrate and modernize various applications. RailTel and Microsoft have entered a five-year strategic partnership aimed at driving AI-driven digital transformation within Indian Railways and the public sector

This collaboration seeks to position RailTel as an AI-first organization and a leading systems integrator partner by leveraging advanced AI solutions. A key component of this partnership is the establishment of an AI Center of Excellence (CoE) by RailTel with Microsoft's support, which will bolster AI adoption, enhance implementation capabilities, and drive innovation in railway operations Additionally, Microsoft's AI National Skills Initiative and Enterprise Skilling Initiative will equip RailTel employees with expertise in next-generation technologies, fostering digital proficiency and workforce readiness
This alliance marks a significant step in modernizing India's railway ecosystem through AI, cloud computing, and advanced digital solutions, aiming to improve decision-making, enhance operational efficiency, and create scalable, intelligent solutions for nationwide deployment

Chapter-2

Bidder Scope of Work

1. Managed Services

The Bidder shall have to perform the Azure Cloud Management activities as per the scope of work given below for 3 Years from the date of empanelment with RailTel. Additionally, the tenure of services shall also be for a period of 3 Years from the date of issuance of the purchase order by the end customer, whichever is later, but not limited to:

1.1 Requirements Analysis

- Collaborate with stakeholders to gather and understand business and technical requirements.
- Identify the specific cloud services needed to meet the requirements.
- Liaison with CSP for the requirement as per RAILTEL request.
- Consider security, compliance, and performance requirements during the analysis.
- All the above services come at no extra cost to RailTel.

1.2 Cloud Service Selection

Choose the appropriate cloud services of the CSP (Microsoft Azure) based on organizational needs and preferences.

1. Prepare cloud deployment architecture based on department's requirements. Get CSP's review done for the proposed architecture and services.

2. Provide Bill of Quantity (BoQ) to the department and get approval on BoQ.

3. Resource Provisioning Setup, provision and configuration of landing zone and cloud resources and services in the cloud environment available on CSP's Portal and marketplace.

4. Installation & configuration of system software viz. Operating System, Database, Design & configuration of Network and Security of cloud systems.

5. Carry out hardening of all infrastructure including VM, Operating System, Database, network, and security appliances as per RAILTEL Security Policy before putting for actual usage.

6. Configure all organizational controls basis the requirement from the department.

7. Any additional Remote resource in case required shall be provided on immediate basis.

8. RAILTEL reserves the right to bring its own licenses for system software like operating system and database. However, if Bidder provides these licenses, it will be responsible for managed services of the respective software.

9. RAILTEL can procure additional licenses which includes SaaS services procured as part of contract , at the agreed rate anytime during the contract period. RAILTEL can reduce the number of licenses on need basis.

10. **Automation and Orchestration** Implement automation tools and scripts for resource provisioning and configuration.

11. The Bidder shall have to perform the Cloud Management activities as per the scope of work given below, but not limited to:

- Utilize orchestration tools to streamline and automate complex workflows.

- Bidder should develop reusable scripts to automate the process of infrastructure (like virtual machine, storage, and network etc.) deployment and subsequent configuration for various use cases at no additional cost to RAILTEL.
- Bidder shall establish an enterprise scale landing zone for connectivity between Railtel DC and Azure and setup necessary network security components (Layer 4-Layer 7) along with their monitoring using native tools after as per RAILTEL's requirement.
- Monitoring and Performance Optimization Set up monitoring tools to track the performance and health of cloud resources.
- Establish alerts for potential issues and implement proactive measures.
- Optimize resource utilization to ensure cost-effectiveness.
- Bidder shall deploy sufficient certified, qualified, and experienced manpower with 24x7 support to meet defined SLA.
- The Bidder must provide cloud native monitoring tools for measuring the service levels, application performance & utilization for servers, storage, and network. The tool shall be capable of providing the exact utilization of servers and shall be able to generate per day, per month and per quarter utilization reports based on which the payments will be made to the Bidder. Bidder should also provide access of this tool to RAILTEL.
- Backup and Disaster Recovery Configuration and execution of Backup as per RAILTEL policy and testing restoration of backups on regular interval and/or as requested by RAILTEL.
- Plan Disaster Recovery of Cloud Environment and Applications as per RAILTEL's requirement, post discussion and agreement with RAILTEL.
- Implement and manage of Disaster Recovery of cloud environment and applications as approved by RAILTEL.
- Develop and test disaster recovery plans to ensure business continuity in case of failures and conduct DR Drills as per agreed between Bidder and RAILTEL.
- Execute Disaster Recovery in case of any events as per RAILTEL BCP and DR Guidelines after necessary approval from RAILTEL.

1.3 Cost Management Monitor and analyze cloud costs regularly.

- Provide proactive recommendations to optimize cost on cloud resources.
- Implement cost allocation and budgeting mechanisms.
- Optimize resource usage to minimize costs without compromising performance.
- The Bidder should provide metering and billing to provide service assurance for maintenance & operations activities. Detailed user level or user group level auditing, monitoring, metering, accounting, quota, and show-back information is essential for the cloud platform to be offered.

1.4 Documentation

- Maintain comprehensive documentation for all provisioned resources and configurations.

- Document procedures for resource scaling, updates, and troubleshooting.
- Collaboration and Communication Collaborate with cross-functional teams, including developers, operations, and security teams.
- Communicate effectively with stakeholders regarding changes, updates, and incidents.
- Upgrades Any required version / software / hardware upgrades, patch management etc. provided by the Bidder / CSP will be managed by the Bidder for the entire contract period at no extra cost to RAILTEL.
- Bidder to consult / inform RAILTEL before doing any upgrade and share detailed report of associated services / functionalities which may get impacted due to the upgrade.

1.5 Compliance and Governance

The CSP/BIDDER shall comply or meet any security requirements applicable to CSP/BIDDER published (or to be published) by MeitY or any standards body setup / recognized by Government of India from time to time and notified to the CSP/Service Providers by MeitY as a mandatory standard within the time frame set by RAILTEL.

- The CSP/BIDDER shall meet all the security requirements, as applicable to RAILTEL, indicated in the IT Act 2000 and its subsequent amendments, and as notified by CERT-In and MEITy from time to time the terms and conditions of the Empanelment of the Cloud Service Providers and shall comply to the audit criteria defined by STQC.
- The CSP/BIDDER will comply with all Government of India regulations like Aadhaar Act/ Digital Personal Data Protection Bill 2022 etc. as applicable from time to time.
- Bidder shall be accountable and responsible for any lapses in the deliverables by CSP and shall be penalized accordingly as per the defined SLA.

1.6 Training and Knowledge Transfer Provide training to the internal team on cloud services and best practices.

- Facilitate knowledge transfer sessions to ensure the team is well-equipped to manage cloud resources effectively.

1.7 Continuous Improvement

- Regularly assess and review the cloud architecture for opportunities to enhance performance, security, and cost efficiency.
- Stay updated on the latest cloud technologies and best practices.

1.8 MIS Reports

- Bidder shall submit the reports on a regular basis in a mutually decided format. The Bidder shall workout the formats for the MIS reports and get these approved by RAILTEL after awarded the contract. The following is only an indicative list of MIS reports that may be submitted to RAILTEL:

Weekly Reports

- Summary of systems rebooted.
- Summary of issues / complaints logged with the OEMs.
- Summary of changes undertaken for the cloud services including major changes like configuration changes, patch upgrades, etc. and minor changes like log truncation, volume expansion, user creation, user password reset, etc.

Monthly Reports

- Component wise server as well as virtual machines availability and resource utilization.
- Consolidated SLA / Non- conformance report.
- Summary of service wise uptime.
- Log of break-fix / preventive / scheduled maintenance undertaken.
- All relevant reports required for calculation of SLAs.
- Any security incidents and associated remediation.

Quarterly Reports

- Consolidated component-wise availability and resource utilization.
- All relevant reports required for calculation of SLAs.
- The MIS reports shall be in-line with the SLAs and the same shall be scrutinized by RAILTEL.

1.9 Security Architecture and Design

- Collaborate with stakeholders to understand business requirements and regulatory constraints.
- Design a comprehensive security architecture that aligns with industry best practices and organizational needs.
- Evolve security strategies based on emerging threats and changing business requirements.
- Define security policies, procedures, and standards as per RAILTEL guidelines/policies.

- Bidder shall also be able to meet any new security requirements as specified by RAILTEL auditor during the period of the contract.
- The CSP/BIDDER undertakes to treat information passed on to them under this Agreement as classified. Such Information will not be communicated/ published/advertised by the CSP/BIDDER to any person/organization without the express permission of RAILTEL.
- The location of the data (text, audio, video, or image files, and software (including machine images), that are provided to the CSP for processing, storage or hosting by RAILTEL or any end user derives from the foregoing through their use of the CSP's services), including High Availability/Geo-replication, shall be as per the terms and conditions prescribed by MeitY.
- The Cloud Service Provider's services offerings shall comply with the audit requirements defined under the terms and conditions of the Provisional Empanelment of the Cloud Service Providers (or STQC/MeitY guidelines as and when published). If the services are not meeting the STQC/MeitY guidelines, RAILTEL shall have the option to discontinue the service and/or entire contract.
- The Audit, Access and Reporting Requirements should be as per the terms and conditions of the MeitY Empanelment of the Cloud Service Provider.
- BIDDER/CSP should provide required logs of SaaS/API services for investigation on demand. Provision should be made to maintain logs for entire contract period.

1.10 Cloud Provider Security Features

- Leverage built-in native security features provided by the cloud service provider (CSP).
- Configure network security groups, access controls, and encryption settings.
- Implement identity and access management (IAM) controls provided by the CSP.
- Bidder should be capable of supporting audit with features such as what request was made, what is the source IP address from which the request was generated, who made the request, timestamp, etc.
- Bidder should implement a security monitoring setup along with CSPM for the tenant.

1.11 Identity and Access Management (IAM)

- Establish robust IAM policies to ensure proper authentication and authorization.
- Implement the principle of least privilege for users and services.
- Integrate with enterprise identity systems if applicable.

1.12 Data Encryption

- Implement encryption for data at rest, in transit, and during processing (if specifically asked by the department).
- Utilize the native encryption capabilities of the cloud provider.
- Manage and rotate encryption keys securely.

1.13. Network Security

- Set up and configure cloud native firewalls, WAF, DDoS and intrusion detection/prevention systems.
- Implement Virtual Private Clouds (VPCs) and subnets with appropriate security controls.
- Monitor network traffic for anomalies and potential security incidents.

1. 14 Endpoint Security

- Implement security measures for cloud-based servers and endpoints.
- Install and configure antivirus software, intrusion detection systems, and endpoint protection.
- Regularly update and patch operating systems and software.
- Maintain up to date antivirus/ virtual patching.

1.15 Security Monitoring and Incident Response

- The scope of BIDDER services shall include the following broad areas using Microsoft's Sentinel (SIEM, SOAR, UEBA) and Microsoft Defender for Cloud, Defender for Servers (Cloud Security Posture Management and Cloud Workload protection tools).

Incident Triage, Analysis, and Response	
Real-Time Alert Monitoring and Triage	Performing triage and short-turn analysis of potential security incidents generated by near-real-time security alert feeds.
Incident Reporting Acceptance	Receiving and processing reports of potential security incidents from constituents and third parties. These reports may come through written (e.g., email) or verbal means.
Incident Analysis and Investigation	Performing in-depth, detailed analysis of suspected incidents. This includes identifying details such as the origin, extent, and implications of an incident, and characterizing the confidence of these conclusions.
Containment, Eradication, and Recovery	Recommendations of activities supporting incident/adversary containment, damage management, adversary eviction, and system recovery to reduce current impact and move to a state that shall prevent future incidents.
Incident Coordination	Performing information gathering, information distribution, and notification in support of an ongoing incident. Directing and/or coordinating response in partnership with constituents, incident response stakeholders and third parties/external agencies.
Forensic Artefact Analysis	Examining media samples and digital artefacts (hard drives, files, memory) to draw detailed observations
Cyber Threat Intelligence, Hunting, and Analytics	
Cyber Threat Intelligence Collection, Processing, and Fusion	Collecting cyber threat intelligence products, including CTI feeds and reports. Processing and integrating CTI into SOC systems and parsing and filtering information for further consumption by the SOC and its constituency
Threat Hunting	Performing proactive operations to identify potentially malicious activity, outside the scope of established SOC alerts, based on hypotheses that the adversary is operating in or against the constituency. This includes developing and refining custom analytic capabilities.

Sensor and Analytics Tuning	Performing curation, tuning and optimization of detections, analytics, signatures, correlation rules, and response rules deployed on SOC detection and analytics systems, such as EDR, SIEM, UEBA and SOAR.
Expanded SOC Operations	
Attack Simulation and Assessments	Performing red teaming, penetration testing, adversary emulation, purple teaming, breach and attack
Insider Threat	Supporting detections, analytics, and investigations focused on finding malicious or anomalous activities carried out by users with legitimate access to constituency systems.
Cybersecurity Exercises	Formulating and facilitating cybersecurity scenario-based simulations and exercises, such as mock critical severity incidents.
Vulnerability Management	
Asset Mapping and Composite Inventory	Collecting and curating knowledge of constituency assets, networks, and services, mapping their interdependencies, and calculating criticality and risk.
Vulnerability Scanning	Interrogation of constituency assets for vulnerability status, including patch level and installed software and security-relevant configuration, for purposes of calculating security risk and compliance status.
Recommendation for Vulnerability Patching and Mitigation	Providing specific advisory/directions to the constituents for addressing vulnerabilities through applying patches or mitigating the risk of vulnerability exploitation through minimizing vulnerability exposure to adversaries such as system or service configuration changes.

1.16 Vulnerability Management

- Use cloud native security solution to Conduct regular vulnerability assessments on cloud resources.
- Remediate identified vulnerabilities promptly as shared by RAILTEL team.
- Stay informed about security patches and updates from the cloud provider.
- Patch all information infrastructure periodically including OS, DB, App, Web, network and security appliances.

1.17 Security Compliance and Auditing

- Use cloud native security solution to Ensure compliance with relevant regulatory requirements and industry standards.
- Generate and retain audit logs for compliance purposes.

- Application and Database Log Management and Analysis.
- Support the third-party auditor / program management team / internal IT team with respect to third party audits and other requirements such as forensic investigations, SLA validation.

1.18 Cloud Security Best Practices

- Stay current with cloud security best practices and industry trends.
- Implement security controls such as secure configuration, multi-factor authentication (MFA), and secure APIs.
- Regularly review and update security policies and procedures.

1.19 Threat Intelligence Integration

- Use cloud native security solution to Integrate threat intelligence feeds to stay informed about emerging threats.
- Use threat intelligence to enhance security monitoring and incident response.
- Collaborate with external security communities and information-sharing platforms.

1.20 Security Automation and Orchestration

- Use cloud native security solution to Implement automation for routine security tasks and response actions.
- Orchestrate security processes to streamline incident response.
- Leverage security automation tools and playbooks.

1.21 Cloud Security Posture Management (CSPM)

- Implement Cloud Native CSPM solutions to monitor and control the use of cloud services.
- Enforce security policies for data in the cloud.
- Provide visibility into cloud usage and potential risks.

1.22 Backup and Recovery Planning

- Develop and implement backup and recovery strategies for security configurations.
- Ensure the ability to restore security controls and configurations in case of incidents.

Chapter-3

PRE-QUALIFICATION CRITERIA:

RAILTEL would like to qualify vendors for undertaking the above work as indicated in the brief scope. The detailed bid qualification criteria for short listing vendors shall be as follows:

I. Technical Criteria:

S. No.	BIDDER (LSP) Qualifications Criteria	Documentary proof to be submitted
1	The Bidder should be – A company incorporated under the Indian Companies Act, 2013 or any other previous company law as per section 2 (20) of the Indian Companies Act 2013/ Partnerships Firm registered under the Limited Liability Partnerships or Partnership Act AND b) Registered with the Income Tax (TAN/PAN) and GST (GSTN) Authorities in India with active status	Certified by Authorized Signatory: 1. Copy of Certificate of Incorporation/ Registration issued by registrar of Company (RoC). 2. Copy of GST Registration Certificate issued to bidder; 3. Copy of TAN/PAN card of the bidder
2	The Bidder should have an average annual turnover of at least INR **11.5 Crore in Cloud Services in the last 3 financial years (i.e. FY 2022-23 , FY 2023-24 , FY 2024-25)** as on the date of submission of Bid and cumulative turnover of last 3 financial years should not be less than INR 75 Cr as per the last audited balance sheet. The bidder should have positive Net worth for the preceding 3 Financial years, reckoned from the last date of original bid submission.	Audited Financial Statements or statutory auditor certificate or certificate from Company Secretary of Bidder specifying the net worth for the specified year.
3	Bidder should have completed/in progress at least **three work order with value Rs. 3 Cr or more for Central Government/ PSU /Enterprise in last 3 years** to provide Cloud Services.	Copy of Work Order along with completion certificate.
4	The bidder should be Licensing Solution Partner (LSP) certified by Microsoft.	Undertaking from bidder is required. Can be verified with CSP
5	Bidder should have at least **25 technical resources** having minimum 3-year experience in cloud management/data migration (in active employment)	Undertaking from the HR for all 25 resources is mandatory.
6	The BIDDER should have managed or successfully delivered at least one project of hosting an enterprise grade application on the proposed CSP cloud. The application hosted should at least have a minimum billing value of 3 Cr per year and the project should be running for at least a period of 12 Months in last 3 years.	Copy of Client certificate, work order, completion certificate or extract from the contract mentioning the scope of work along with client completing certificate. Copy of evidence of the user base for the application from a publicly verifiable (source such as newspaper article/website/app downloads etc.) CA certificate confirming the billing value every year from the project.

7	Submission of undertaking that the firm or any of the firm's partner has not been blacklisted by any Indian State/Central Governments Dept. / Public Sector Undertaking of India.	Self-attested Undertaking	
8	Bidder to provide OEM authorization letter/ Manufacturers Authorization Certificate from the MeitY Empanelled OEM quoting this EOI reference number, date and due date of opening along with the bid	OEM Manufacturers Authorization Certificate with empanelment confirmation from MeitY	
9	The bidder must have an association with their CSP for at least 3 years on the date of bid submission with direct relationship with Microsoft as a LSP	Undertaking letter from CSP.	

S. No.	CSP Mandatory Criteria	Documentary Evidence
1	The Cloud Service Provider (CSP) should have been offering cloud services in India from at least last 3 financial years. The average annual turnover of the CSP should be at least Rs. 500 crores as on date of bid submission for the immediately preceding 3 financial years.	Copy of Certificate of Incorporation or Certified copy of Partnership Deed Letter from Statutory Auditors / Certificate from Chartered Accountant on their letterhead mentioning the annual revenue/Balance sheet on CSP letter head mentioning the annual turnover.
2	The Cloud Service Provider (CSP) should be empaneled with the Ministry of Electronics & Information and Technology (MEITY), Government of India for offering both DC & DR with distance >100kms	Undertaking on CSP letterhead confirming the clause
3	CSP shall have published on its public website- cloud services' rates for India, Service Level Agreements (SLAs), dashboard live-status of cloud services' health across global datacentre and outage details (if any) with RCA.	An undertaking from the CSP with the links to its relevant public facing website(s) covering the details
4	· Tier-3 datacenter certification from TIA or equivalent agency (Documentary Evidence-Certificate/)	Copy of Relevant Certificate
	· ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001	
	ISO/IEC 27002 for privacy information management — Requirements and guidelines	

	· ISO 27017 · ISO 27018 · ISO 20000-1 · ISO 9001 · SOC 1,2 and 3 Certificate/audited Report	
5	Submission of "Undertaking of Not Being blacklisted.	Self-attested Undertaking

II Bid EVALUATION

Technical Evaluation would cover Pre-qualification criteria, technical and techno-commercial aspects.
Commercial Evaluation would be the price bid.

. Bids will be evaluated firstly as per pre-qualification criteria and the technical requirements of the EOI .

. Only the price bids of the EMD, technical qualified bidders will be opened and evaluated.

. The Line item in this EOI contains 2 parts (i.e., Part-A and Part-B)

. **Part-A** belongs to the Azure services for all present and future services which is not available with Azure at present or RAILTEL does not require them but may be useful to use in future. The discount% offered during bid will be firm during entire contract period. The rate of such services shall be used as per the Azure published rate as on opening date of EOI or first made generally available for the customer.

. **Part-B** belongs to Managed Services, On-Demand On-Site Resource, Professional Services. The quoted amount by the bidder shall be firm during the entire contract period.

Total Quoted Amount = (Part-A + Part-B)

. The bid evaluation and award of the job will be done on an Overall highest discount percentage on SOR-A and Lowest cost quoted in SOR-B.

CHAPTER-4

SCHEDULE OF REQUIREMENT (SOR-A)

Part A - Discount on Future Workload		
Sr. No	**Description**	**Discount Offerd (in Percentage - %)**
1	IaaS Services	
2	PaaS Services	
3	SaaS Services	
4	Product and Services from Azure Marketplace	
5	Azure standard Support plan (all plans)	
	Taxes - GST __%	
	Total discount after taxes	

1. Bidder should mention Discount Offered (in percentage) on IaaS, PaaS, SaaS and Product & Services available on Marketplace. Discount mentioned will be applicable for entire contract period.

2. Cost breakup to be submitted by the bidder (if applicable):

a. Basic Rate
b. CGST
c. IGST
d. SGST
e. Any other charges

3) Rates for Reserved Instance (RI) will be applicable as per CSP policies. Rate for Reserved Instance (RI) will be paid on actuals.

4) The above mentioned discount is for the purpose of discovery and procurement of Azure services by RailTel for pitching up its business (prospective customers) Percentage mentioned will be considered during the commercial evaluation for discovery of the "L1 Bidder"

5.) If Supplier fails to furnish necessary document i.e. invoices etc, in respect of duties/taxes convertible the amount pertaining to such duties/taxes will be deducted from the payment due to the firm.

6.) User manual, instruction manual, operating manual etc. wherever required shall be submitted by the bidder.

Part B - Managed Services (SOR-B)

Sr. No	Description	Unit of Measure	Offered Unit Price by BIDDERexcluding GST (INR) (D1)
1	Managed Services: Cloud implementation & Management with respect to RAILTEL's cloud environment based on high-level SoW mentioned in Bidder Scope of Work	Per Month	
2	Onsite Manpower (Dedicated On-Site Resource - Nos.1 per month)	Per Month	
3	Bidder Professional Services: Any additional implementation which is not in scope of work	Per Man Day	
		Amount (D4)	**0**
		Taxes - GST __% (D5)	**0**
		Total Amount (D = D4+D5)	**0**

Note:
1) Unit Price offered by the bidder under column "Offered Unit Price by BIDDER (D1)" will be valid for entire contract period.
2) Bidder has to provide additional manpower, if required on the same unit price during entire contract period.
3) Bidder have to provide professional services at the same unit price quoted above during entire contract period, in case additional Man Day required.
4) Professional Services - Any additional activity required to be performed which is not covered in Scope of Work under Section 2.1 and requires dedicated manpower efforts more than 10 man-days at the discretion of RAILTEL team.

Chapter-5

Terms Of Payment

1. PAYMENT TERMS

The Company, in consideration of the successful bidder carrying out and executing the said work to the satisfaction of the company, shall pay to the successful bidder as per the said schedule of rates, subject to deductions, retentions and abatements, if any to be made therefrom in accordance with the provisions of this agreement. The following shall be the payments terms:

- Bidder to produce the certified copy of prices published in CSP's website along with the monthly invoices.
- The billing would start from the date of operational acceptance by RAILTEL.
- No advance payment shall be made for any activity.
- Two consecutive monthly deductions amounting to 50% or more of the bill value on account of any reasons will be deemed to be an event of default and termination.
- If the bidder is liable for any penalty as per the SLA (refer to the related clause of this agreement), the same shall be adjusted from payments due to the successful bidder.
- RailTel shall make payment to selected LSP after receiving payment from Customer for the agreed scope of work. In case of any penalty or deduction made by customer for the portion of work to be done by LSP, same shall be passed on to LSP.
- All payments by RailTel to the LSP will be made after the receipt of payment by RailTel from end Customer organization.
- Jobs awarded under this contract cannot be sub-contracted without the consent of RAILTEL.
- RAILTEL shall not be held responsible for delay in payment under the following circumstance.
- Non-submission of Bank Guarantee as per EOI / PO terms & conditions.
- Deviation in billing pattern (like States / HSN/SAC) after placement of PO.
- Delay in submission of bills.
- All prices quoted should in Indian Rupees (INR).
- Payments would be released by our office at EKN, New Delhi through NEFT. The invoice should be addressed to RailTel Corporation of India Ltd.

END of EOI Document
****