RAILTEL CORPORATION OF INDIA LIMITED

(A Govt. of India Undertaking)

Registered & Corporate Office:

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

Selection of Partner For

"IT services to RCIL Customer"

EOI No: RCIL/EOI/CO/ITB/2025-26/IT services to RCIL customer/1 dated 11.04.25

EOI NOTICE

RailTel Corporation of India Limited Plate-A, 6th Floor, Office Tower-2,
NBCC Building, East Kidwai Nagar, New Delhi-110023

EOI No: RCIL/EOI/CO/ITB/2025-26/IT services to RCIL customer/1 dated 11.04.25

RailTel Corporation of India Ltd., (here after referred to as RailTel) invites EOIs from RailTel's Empaneled Partners for the selection of suitable agency for "IT Services to RCIL Customer".

The details are as under:

Last date for submission of EOIs by bidders	16-04-2025 before 15:00Hrs.
Opening of bidder EOIs	16-04-2025 at 15:30Hrs.
Earnest Money Deposit (EMD)	Rs 5,00,000/- (Five Lakhs) through DD or online transfer to RailTel in following account: Bank Name- Union Bank of India Branch- YUSUF SARAI, DELHI A/C Number - 340601010050446 Account Type- Current Account IFSC Code -UBIN0534064
Number of copies to be submitted for scope of work	01 in Hard Copy
Place of Bid submission	RailTel Corporation of India Limited Plate-A, 6th Floor, Office Tower-2, NBCC Building, East Kidwai Nagar, New Delhi-110023

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

Contact: Naresh Kumar
Position: JGM/IT
Email: naresh.kumar@railtelindia.com Telephone: +91124 2714000 Ext 2222

NOTE:

I. **All firms are required to submit hard copy of their EOI submissions, duly signed by Authorized Signatories with Company seal and stamp.**

II. **The EOI response is invited from empaneled partners of RailTel. Only RailTel empaneled partners are eligible for participation in EOI process.**

1. RailTel Corporation of India Limited–Introduction

RailTel Corporation of India Limited (RCIL), an ISO-9001:2000 organization is a Government of India undertaking under the Ministry of Railways. The Corporation was formed in Sept 2000 with the objectives to create nationwide Broadband Telecom and Multimedia Network in all parts of the country, to modernize Train Control Operation and Safety System of Indian Railways and to contribute to realization of goals and objective of national telecom policy 1999. RailTel is a wholly owned subsidiary of Indian Railways.

For ensuring efficient administration across India, country has been divided into four regions namely, Eastern, Northern, Southern & Western each headed by Regional General Managers and Headquartered at Kolkata, New Delhi, Secunderabad & Mumbai respectively. These regions are further divided into territories for efficient working. RailTel has territorial offices at Guwahati, & Bhubaneswar in East, Chandigarh, Jaipur, Lucknow in North, Chennai & Bangalore in South, Bhopal, and Pune & Ahmedabad in West. Various other territorial offices across the country are proposed to be created shortly.

RailTel's business service lines can be categorized into three heads namely B2G/B2B (Business to Government and Business to Business) and B2C (Business to customers):

Licenses & Services

Presently, RailTel holds IP-1, NLD and ISP (Class-A) licenses under which the following services are being offered to various customers:

CARRIER SERVICES

1. National Long Distance: Carriage of Inter & Intra -circle Voice Traffic across India using state of the art NGN based network through its Interconnection with all leading Telecom Operators
2. Lease Line Services: Available for granularities from E1, DS-3, STM-1 & above
3. Dark Fiber/Lambda: Leasing to MSOs/Telco's along secured Right of Way of Railway tracks
4. Co-location Services: Leasing of Space and 1000+ Towers for collocation of MSC/BSC/BTS of Telco's

ENTERPRISE SERVICES

1. Managed Lease Line Services: Available for granularities from E1, DS-3, STM-1 & above
2. MPLS VPN: Layer-2 & Layer-3 VPN available for granularities from 64 Kbps to nx64 Kbps, 2 Mbps& above
3. Dedicated Internet Bandwidth: Experience the "Always ON" internet connectivity at your fingertips in granularities 2mbps to 155mbps

RETAIL SERVICES

RailWire: RailWire is the retail broadband service of RailTel. RailWire is a collaborative public private local entrepreneur (PPLE) model providing broadband services by leveraging the eco system available with different partners like RailTel, Access Network Provider, Aggregation Network Provider (AGNP) and Managed Service Provider (MSP) to offer high speed & cost-effective broadband to end customers. The model uses RailTel's nationwide Core fiber Backbone Network, Access Network available with Local entrepreneurs, FTTH Infrastructure providers etc. and Managed Service Partners/Application Service Providers having IT & management capabilities. The model has been tested for several years now with about 4 lakh+ home broadband users along with 5200+ local access network partners. It is noteworthy that this approach whereby about 54%

of the revenue is ploughed back into the local community not only serves the underserved but also creates livelihoods and jobs in the local communities.

2. Objective of EOI

RCIL is implementing IT-ICT projects like providing Infra as a Service for its customers. RailTel is in process of selecting suitable empaneled partner for providing customer specific IT services.

3. Scope of Work

The scope of work is to provide "Cybersecurity Solution" on service modal for RailTel's Customer as per Schedule of Requirements (SoR) Clause 10. Detailed scope of work is provided under Annexure-03.

4. Language of Proposals

The proposal and all correspondence and documents shall be written in English. The hardcopy version will be considered as the official proposal.

5. Proposal Preparation and Submission

The Applicant/bidder is responsible for all costs incurred in connection with participationin this EOI process, including, but not limited to, cost incurred in conduct of informative and other diligence activities, participation in meetings/ discussions/presentations, preparationof proposal, in providing any additional information required by RCIL to facilitate the evaluation process or all such activities related to the EOI response process. RCIL will in nocase be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.

6. Bidding Document

The bidder is expected to examine all instructions, forms, terms and conditions and technical specifications in the bidding documents. Submission of bids, not substantially responsive to the bidding document in every aspect will be at the bidder's risk and may result in rejection of its bid without any further reference to the bidder.

All pages of the documents shall be signed and stamped by the bidder including the closing page in token of his having studied the EOI document and should be submitted along with the bid.

7. Payment terms

7.1. Payment terms will be on back to back basis and as per agreement between RailTel and Customer.

7.2. RailTel shall release the payment to selected bidder after receiving payment from Customer and on submission of Tax invoice by selected bidder on back to back basis.

7.3. Any penalty or deduction (LD) from customer shall be passed on to selected bidder on proportionate basis.

Bill passing authority is JGM/IT/CO and Bill payment authority is GM/Finance /CO.

8. Delivery Schedule: Solution should be deployed in Data centre within1 month after issue of PO from RailTel.

9. Compliance requirements

9.1. The interested partner should be an Empaneled Partner with RailTel on the date of bid submission. Copy of RailTel's Empanelment Letter may be submitted in this regard.

9.2. The interested bidder should submit Earnest Money Deposit (EMD) through online transfer and submit the proof of same along with bid.

9.3. The interested bidder should comply to insertion of Rule 144(xi) in the GFR, 2017 vide office OM no. 6/18/2019-PPD dated 23-July-2020 issued by Ministry of Finance, Government of India, including revisions.(Annexure-01)

9.4. The interested bidder should not be blacklisted by any State / Central Government Ministry / Department / Corporation / Autonomous Body in India, on the last date of submission of EOI. (Annexure-02)

9.5. There should not be any ongoing or past, arbitration case(s) between 'RailTel' and 'Interested Bidder' on the last date of submission of EOI. (Annexure-02)

9.6. The interested partner should have a valid Goods and Service Tax Identification Number (GSTIN), as on the last date of submission of EOI.

9.7. The Bidder must have cumulative turnover of minimum 150% of the total quoted SOR price during the last 3 financial years. Bidder should submit audited balance sheets and certificate of CA for preceding three years.

9.8. The interested bidder should have experience in Data Centre or Cyber security project. Bidder should submit PO or work order copy of contract value not less than 60% of total quoted SOR price for the work of SITC during last seven years from any government organization

10. Schedule of Rates

SN	Item Description	Annual Recurring Charges	GST on ARC	Total Amount with GST
1	Cybersecurity Solution services			
SN	Item Description	One-time Charges	GST on OTC	Total Amount with GST
2	One time Cost of installation and solution provisioning			
	Total SOR Cost with tax (OTC and ARC)			

11. Evaluation criteria

Only those offers shall be considered for financial evaluation which fulfills all compliance requirements in clause number 9. Financial Evaluation will be carried on basis of lowest offer quoted by the bidder under Clause-10 (SOR).

12. Liquidated Damages

The timely delivery is the essence of this tender. Liquidated damages will be applicable at the rate of half percent (including elements of taxes, duties, freight, etc.) per week or part thereof for undelivered portion of SOR subject to a maximum of 10% of the cost of Purchase order for any reason whatsoever attributed to failure of tenderer. RailTel will have the right to cancel the order, place order on alternative source besides levying the liquidated damages as above.

13. Bidding Process

The bidder needs to submit the bid in sealed, signed and stamped envelope clearly mentioning of EOI number, EOI name, addressed to the EOI inviting officer as well as Bidding Agency Name and Contact person.

BID should consist the following:

1. Covering Letter
2. RailTel empanelment LOI
3. Signed and Stamped EOI Document
4. GST and PAN documents
5. EMD
6. Duly filled SOR (Clause 10)
7. Solution document
8. DC Infra Sizing requirement
9. Documents with respect to compliance requirement clause (9.1 to 9.8).
10. Deviation statement (if any) as per clause number 24.

14. Period of Validity of bids and Bid Currency

Bids shall remain valid for a period of 180 days from the date of submission of EOI response bid. The prices in the bid document to be expressed in INR only.

15. RCIL's Right to Accept/Reject Bids

RCIL reserves the right to accept or reject any bid and annul the bidding process or even reject all bids at any time prior to award of contract, without thereby incurring any liability to the affected bidder or bidders or without any obligation to inform the affected bidder or bidders about the grounds for RailTel's action.

16. Security Deposit / Performance Bank Guarantee (PBG)

In case RailTel submits BG to customer, Successful bidder has to furnish security deposit in the form of Performance Bank guarantee @ 3 - 10% of issued PO/ LOA value with tax of valid for 3 months beyond the date of completion of all contractual obligations including warrantee obligations. The same should be submitted within 30 days of issue of LOA/PO, failing which a penal interest of 15% per annum shall be charged for the delay period i.e. beyond 30 (thirty) days from the date of issue of LOA/PO. This PBG should be from a Scheduled Bank and should cover warranty period plus three months for lodging the claim. The performance Bank Guarantee will be discharged by the Purchaser after completion of the supplier's performance obligations including any warranty obligations under the contract.

16.1. The Performa for PBG is given in Form No. 1. If the delivery period gets extended, the PBG should also be extended appropriately.

16.2. The security deposit/PBG shall be submitted to Corporate Office & will bear no interest.

16.3. A separate advice of the BG will invariably be sent by the BG issuing bank to the RailTel's Bank through SFMS and only after this the BG will become acceptable to RailTel. It is therefore in interest of bidder to obtain RailTel's Bank IFSC code, its branch and address and advise these particulars to the BG Issuing bank and request them to send advice of BG through SFMS to the RailTel's Bank.

16.4. The security deposit/Performance Bank Guarantee shall be released after successful completion of

Contract, duly adjusting any dues recoverable from the successful tenderer. Security Deposit in the form of DD/Pay Order should be submitted in the favour of "RailTel Corporation of India Limited" payable at New Delhi Only.

16.5. Any performance security upto a value of Rs. 5 Lakhs is to be submitted through DD/Pay order / online transfer only.

16.6. The claim period of PBG shall be 1 year after date of PBG validity

17. Earnest Money Deposit (EMD)/ Bid Security

17.1. The bidder shall furnish a sum as Earnest Money in the form of online transfer or Demand Draft from any scheduled bank in India in favour of "RailTel Corporation of India Limited" payable at New Delhi.

17.2. The EMD may be forfeited if a bidder withdraws his offer or modifies the terms and conditions of the offer during validity period and in the case of a successful bidder, if the bidder fails to accept the Purchase order and fails to furnish performance bank guarantee (security deposit) in accordance with clause 6.

17.3. Offers not accompanied with Earnest Money shall be summarily rejected.

17.4. Earnest Money of the unsuccessful bidder will be discharged / returned as promptly as possible as but not later than 30 days after the expiry of the period of offer / bid validity prescribed by the Purchaser.

17.5. The successful bidder's EMD will be discharged upon the bidder's acceptance of the purchase order satisfactorily and furnishing the performance bank guarantee in accordance with clause 17.

17.6. Earnest Money will bear no interest.

18. Deadline for Submission of Bids

Bids must be submitted to RCIL at the address specified in the EOI document not later than the specified date and time mentioned. If the specified date of submission of bids being declared a holiday for RCIL, the bids will be received up to the specified time in the next working day.

19. Late Bids

Any bid received by RCIL after the deadline for submission of bids will be rejected and/or returned unopened to the bidder.

20. Modification and/or Withdrawal of Bids

Bids once submitted will treated as final and no modification will be permitted. No correspondence in this regard will be entertained. No bidder shall be allowed to withdraw the bid after the deadline for submission of bids. In case of the successful bidder, he will not be allowed to withdraw or back out from the bid commitments.

21. Clarification of Bids

To assist in the examination, evaluation and comparison of bids the purchaser may, at its discretion, ask the bidder for clarification. The response should be in writing and no change in the price or substance of the bid shall be sought, offered or permitted.

22. Bidder's Information

Company Name:	
Type of RCIL Business Partner	
Status of Applicant (Partnership, Company etc.)	
Number of Years of Experience	
Number of office locations in India (Provide details)	
Number of office locations globally (Provide details)	
Number of employees in India and global	

CONTACT DETAILS:			
First Name		Last Name	
Designation			
Address for correspondence			
Contact Number (Office Landline)			
Mobile Number			
Official Email ID			
GSTN No			
PAN No			
Bank Account No			
IFSC Code			
Registered Address of Company			

23. Format for statement of Deviation

The following are the particulars of deviations from the requirements of the Instructions to bidders:

	CLAUSE	DEVIATION	REMARKS (Including Justification)

24. Duration of the Contract Period

The contract duration shall be same as of RAILTEL'S CUSTOMER's contract duration with RailTel until otherwise terminated earlier. The initial contract period is 1 year. The contract duration can be renewed / extended by RailTel at its discretion as per customer requirement, in case RAILTEL'S CUSTOMER extends / renews services with RailTel by virtue of extending / renewing / new issuance of one or more Purchase Order(s) placed by RAILTEL'S CUSTOMER to RailTel.

25. Variation in Contract

+/- 50 % variation may be operated during the period of validity of agreement with the approval of competent authority with similar terms and procedure as specified in the agreement.

26. Restrictions on 'Transfer of Agreement'

The SELECTED BIDDER shall not assign or transfer its right in any manner whatsoever under the contract / agreement to a third party or enter into any agreement for sub-contracting and/or partnership relating to any subject matter of the contract / agreement to any third party either in whole or in any part i.e. no sub-contracting / partnership / third party interest shall be created.

27. Suspension, Revocation or Termination of Contract / Agreement

27.1. RailTel reserves the right to suspend the operation of the contract / agreement, at any time, due to change in its own license conditions or upon directions from the competent government authorities, in such a situation, RailTel shall not be responsible for any damage or loss caused or arisen out of aforesaid action. Further, the suspension of the contract / agreement will not be a cause or ground for extension of the period of the contract / agreement and suspension period will be taken as period spent. During this period, no charges for the use of the facility of the SELECTED BIDDER shall be payable by RailTel.

27.2. RailTel may, without prejudice to any other remedy available for the breach of any conditions of agreements, by a written notice of Three (03) month issued to the SELECTED BIDDER, terminate/or suspend the contract / agreement under any of the following circumstances:

a) The SELECTED BIDDER failing to perform any obligation(s) under the contract / agreement.

b) The SELECTED BIDDER failing to rectify, within the time prescribed, any defect as may be pointed out by RailTel.

c) Non adherence to Service Level Agreements (SLA) which RailTel has committed to RAILTEL CUSTOMER for the pertinent tender.

d) The SELECTED BIDDER going into liquidation or ordered to be wound up by competent authority.

e) If the SELECTED BIDDER is wound up or goes into liquidation, it shall immediately (and not more than a week) inform about occurrence of such event to RailTel in writing. In that case, the written notice can be modified by RailTel as deemed fit under the circumstances. RailTel may either decide to issue a termination notice or to continue the agreement by suitable modifying the conditions, as it feels fit under the circumstances.

f) It shall be the responsibility of the SELECTED BIDDER to maintain the agreed Quality of Service, even during the period when the notice for surrender/termination of contract / agreement is pending and if the Quality of Performance of Solution is not maintained, during the said notice period, it shall be treated as material breach liable for termination at risk and consequent of which SELECTED BIDDER's PBG related to contract / agreement along with PBG related to the Empanelment Agreement with RailTel shall be forfeited, without any further notice.

g) Breach of non-fulfillment of contract / agreement conditions may come to the notice of RailTel through complaints or as a result of the regular monitoring. Wherever considered appropriate RailTel may conduct an inquiry either suo-moto or on complaint to determine whether there has been any breach in compliance of the terms and conditions of the agreement by the successful bidder or not. The SELECTED BIDDER shall extend all reasonable facilities and shall endeavor to remove the hindrance of every type upon such inquiry. In case of default by the SELECTED BIDDER in successful implementation and thereafter maintenance of services / works as per the conditions mentioned in this EOI document, the PBG(s) of SELECTED BIDDER available with RailTel will be forfeited.

28. Dispute Settlement

28.1. In case of any dispute concerning the contract / agreement, both the SELECTED BIDDER and RailTel shall try to settle the same amicably through mutual discussion / negotiations. Any unsettled dispute shall be settled in terms of Indian Act of Arbitration and Conciliation 1996 or any amendment thereof. Place of Arbitration shall be New Delhi.

28.2. The arbitral tribunal shall consist of the Sole Arbitrator. The arbitrator shall be appointed by the Chairman & Managing Director (CMD) of RailTel Corporation of India Ltd..

28.3. All arbitration proceedings shall be conducted in English.

29. Governing Laws

The contract shall be interpreted in accordance with the laws of India. The courts at New Delhi shall have exclusive jurisdiction to entertain and try all matters arising out of this contract.

30. Statutory Compliance

30.1. During the tenure of this Contract nothing shall be done by SELECTED BIDDER in contravention of any law, act and/ or rules/regulations, there under or any amendment thereof and shall keep RailTel indemnified in this regard.

30.2. The Bidder shall comply and ensure strict compliance by his/her employees and agents of all applicable Central, State, Municipal and Local laws and Regulations and undertake to indemnify RailTel, from and against all levies, damages, penalties and payments whatsoever as may be imposed by reason of any breach or violation of any law, rule, including but not limited to the claims against RailTel or its Customer under Employees Compensation Act, 1923, The Employees Provident Fund and Miscellaneous Provisions Act, 1952, The Contract Labour (Abolition and Regulation) Act 1970, Factories Act, 1948, Minimum Wages Act and Regulations, Shop and Establishment Act and Labour Laws which would be amended/modified or any new act if it comes in force whatsoever, and all actions claim and demand arising there from and/or related

thereto.

31. Intellectual Property Rights

33.1. Each party i.e. RailTel and SELECTED BIDDER, acknowledges and agree that the other party retains exclusive ownership and rights in its trade secrets, inventions, copyrights, and other intellectual property and any hardware provided by such party in relation to this contract / agreement.

33.2. Neither party shall remove or misuse or modify any copyright, trade mark or any other proprietary right of the other party which is known by virtue of this EoI and subsequent contract in any circumstances.

32. Severability

In the event any provision of this EOI and subsequent contract with SELECTED BIDDER is held invalid or not enforceable by a court of competent jurisdiction, such provision shall be considered separately and such determination shall not invalidate the other provisions of the contract and Annexure/s which will be in full force and effect.

33. Force Majeure

33.1. If during the contract period, the performance in whole or in part, by other party, of any obligation under this is prevented or delayed by reason beyond the control of the parties including war, hostility, acts of the public enemy, civic commotion, sabotage, Act of State or direction from Statutory Authority, explosion, epidemic, quarantine restriction, strikes and lockouts (as are not limited to the establishments and facilities of the parties), fire, floods, earthquakes, natural calamities or any act of GOD (hereinafter referred to as EVENT) , provided notice of happenings of any such event is given by the affected party to the other, within twenty one (21) days from the date of occurrence thereof, neither party shall have any such claims for damages against the other, in respect of such non-performance or delay in performance. Provided service under this contract shall be resumed as soon as practicable, after such EVENT comes to an end or ceases to exist.

33.2. In the event of a Force Majeure, the affected party will be excused from performance during the existence of the force Majeure. When a Force Majeure occurs, the affected party after notifying the other party will attempt to mitigate the effect of the Force Majeure as much as possible. If such delaying cause shall continue for more than sixty (60) days from the date of the notice stated above, the party injured by the inability of the other to perform shall have the right, upon written notice of thirty (30) days to the other party, to terminate this contract. Neither party shall be liable for any breach, claims, and damages against the other, in respect of non-performance or delay in performance as a result of Force Majeure leading to such termination.

34. Indemnity

34.1. The SELECTED BIDDER agrees to indemnify and hold harmless RailTel, its officers, employees and agents (each an "Indemnified Party") promptly upon demand at any time and from time to time, from and against any and all losses, claims, damages, liabilities, costs (including reasonable attorney's fees and disbursements) and expenses (collectively, "Losses") to which the Indemnified party may become subject, in so far as such losses directly arise out of, in any way relate to, or

result from :

a) Any mis-statement or any breach of any representation or warranty made by SELECTED BIDDER or

b) The failure by the SELECTED BIDDER to fulfill any covenant or condition contained in this contract by any employee or agent of the Bidder. Against all losses or damages arising from claims by third Parties that any Deliverables (or the access, use or other rights thereto), created by SELECTED BIDDER pursuant to this contract, or any equipment, software, information, methods of operation or other intellectual property created by SELECTED BIDDER pursuant to this contract, or the SLAs (i) infringes a copyright, trade mark, trade design enforceable in India, (ii) infringes a patent issues in India, or (iii) constitutes misappropriation or unlawful disclosure or used of another Party's trade secrets under the laws of India (collectively, "Infringement Claims"); or

c) Any compensation / claim or proceeding by ECT or any third party against RailTel arising out of any act, deed or omission by the SELECTED BIDDER or

d) Claim filed by a workman or employee engaged by the SELECTED BIDDER for carrying out work related to this agreement. For the avoidance of doubt, indemnification of Losses pursuant to this section shall be made in an amount or amounts sufficient to restore each of the Indemnified Party to the financial position it would have been in had the losses not occurred.

34.2. Any payment made under this contract to an indemnity or claim for breach of any provision of this contract shall include applicable taxes.

35. Limitation of Liability towards RailTel

35.1. The SELECTED BIDDER liability under the contract shall be determined as per the Law in force for the time being. The SELECTED BIDDER shall be liable to RailTel for loss or damage occurred or caused or likely to occur on account of any act of omission on the part of the SELECTED BIDDER and its employees *(direct or indirect)*, including loss caused to RailTel on account of defect in goods or deficiency in services on the part of SELECTED BIDDER or his agents or any person / persons claiming through under said SELECTED BIDDER, However, such liability of the SELECTED BIDDER shall not exceed the total value of the contract.

35.2. This limit shall not apply to damages for bodily injury (including death) and damage to real estate property and tangible personal property for which the SELECTED BIDDER is legally liable.

36. Confidentiality cum Non-disclosure

36.1. The Receiving Party agrees that it will not disclose to third party/parties any information belonging to the Disclosing Party which is provided to it by the Disclosing Party before, during and after the execution of this contract. All such information belonging to the Disclosing Party and provided to the Receiving Party shall be considered Confidential Information. Confidential Information includes prices, quotations, negotiated issues made before the execution of the contract, design and other related information. All information provided by Disclosing Party to the Receiving Party shall be considered confidential even if it is not conspicuously marked as confidential.

36.2. Notwithstanding the foregoing, neither Party shall have any obligations regarding non-use or non-disclosure of any confidential information which:

a) Is already known to the receiving Party at the time of disclosure:

b) Is or becomes part of the public domain without violation of the terms hereof;

c) Is shown by conclusive documentary evidence to have been developed independently by the Receiving Party without violation of the terms hereof:

d) Is received from a third party without similar restrictions and without violation of this or a similar contract.

36.3. The terms and conditions of this contract, and all annexes, attachments and amendments hereto and thereto shall be considered Confidential Information. No news release, public announcement, advertisement or publicity concerning this contract and/or its contents herein shall be made by either Party without the prior written approval of the other Party unless such disclosure or public announcement is required by applicable law.

36.4. Notwithstanding the above, information may be transmitted to governmental, judicial, regulatory authorities, if so, required by law. In such an event, the Disclosing Party shall inform the other party about the same within 30 (thirty) Days of such disclosure.

36.5. This Confidentiality and Non- Disclosure clause shall survive even after the expiry or termination of this contract.

37. Insurance

The SELECTED BIDDER agrees to take insurances to cover all the elements of the project under this EOI including but not limited to Manpower, Hardware, Software.

38. Waiver

Except as otherwise specifically provided in the contract, no failure to exercise or delay in exercising, any right, power or privilege set forth in the contract will operate as a waiver of any right, power or privilege.

39. Contract Agreement

RailTel shall sign SLA and contract agreement with selected bidder. No modification of the terms and conditions of the Contract Agreement shall be made except by written amendments signed by the both SELECTED BIDDER and RailTel. All other terms and conditions between SELECTED BIDDER and RailTel shall be on **back-to-back** basis as mentioned in Customer agreement.

40. Special terms and conditions

40.1. The Cybersecurity solution for RailTel's customer shall be hosted in RailTel data center Gurgaon or customer data centre in Delhi. The infra for hosting proposed solution shall be provided by RailTel however any license requirement to implement the solution shall be provide by bidder

40.2. Bidder is required to submit DC infrastructure sizing and license details for hosting proposed solution.

40.3. RailTel may ask selected bidder to show demo or POC of proposed solution.

40.4. Bidder should submit detailed solution along with Bid and proposed solution must comply to scope of work (Annexure-03)

Format for COVERING LETTER

COVERING LETTER (To be on company letter head)

EoI Reference No: **RCIL/EOI/CO/ITB/2025-26/IT services to RCIL customer/1 dated 11.04.25**

Date:

To,

JGM/IT
RailTel Corporation of India Ltd.
Plate-A, 6th Floor, Office Tower-2,
NBCC Building, East Kidwai Nagar,
New Delhi 110023

Dear Sir,

SUB: Participation in the EoI Process

Having examined the Invitation for EoI document bearing the reference number _____released by your esteemed organization, we, undersigned, hereby acknowledge the receipt of the same and offer to participate in conformity with the said Invitation for EoI document. I/We also agree to keep this offer open for acceptance for a period of 180 days from the date of submission of EOI response bid to RailTel and in default thereof,

If our application is accepted, we undertake to abide by all the terms and conditions mentioned in the said Invitation for EoI document.

We hereby declare that all the information and supporting documents furnished as a part of our response to the said Invitation for EoI document, are true to the best of our knowledge. We understand that in case any discrepancy is found in the information submitted by us, our EoI is liable to be rejected.

Authorized Signatory
Name
Designation
Contact Details

Annexure – 01

Compliance to Rule 144 (xi) of GFR, 2017 *including amendments till date*

(On Organization Letter Head)

Bid Ref No. :

Date:

To,

Jt.General Manager (IT),
RailTel Corporation of India Limited,
Plate-A, 6th Floor, Office Block Tower-2,
East Kidwai Nagar, New Delhi - 110023

Ref : EOI No. RCIL/EOI/CO/ITB/2025-26/IT services to RCIL customer/1 dated 11.04.25

Dear Sir,

I, the undersigned, on behalf of M/s …….. , have read the clause/para regarding restrictions on procurement from a bidder of a country which shares a land border with India and on sub-contracting to contractors from such countries.

(a) I certify that M/s ……. is not from such a country and will not sub-contract any work to a contractor from such countries unless such contractor is registered with the Competent Authority. I also certify that M/s …… will not offer any products / services of entity from such countries unless such entity is registered with the Competent Authority.

***OR** (Strikeout either (a) or (b), whichever is not applicable)*

(b) I certify that M/s …… is from such a country and has been registered with the Competent Authority. I also certify that M/s ……. has product/services of entity from such countries and these entity / entities are also registered with the Competent Authority.

(Where applicable, evidence of valid registration by the Competent Authority is to be attached with the bid.)

I hereby certify that M/s …… fulfills all requirements in this regard and is eligible to be considered.

I hereby acknowledge that in the event of acceptance of my bid on above certificate and if the certificate is found to be false at any stage, the false certificate would be a ground for immediate termination of contract and further legal action in accordance with the Law.

Signature of Authorised Signatory

Name
Designation

Annexure – 02

Undertaking for Non-Blacklisting & Arbitration Case

(On Organization Letter Head)

Bid Ref No. :

Date:

To,

Jt. General Manager (IT),
RailTel Corporation of India Limited,
Plate-A, 6th Floor, Office Block Tower-2,
East Kidwai Nagar, New Delhi - 110023

Ref : EOI No. RCIL/EOI/CO/ITB/2025-26/IT services to RCIL customer/1 dated 11.04.25

Dear Sir,

I, the undersigned, on behalf of M/s ……..…… , hereby submits that

1. We are not blacklisted by any State / Central Government Ministry / Department / Corporation / Autonomous Body at the time of submission of bid.
2. We are not having any ongoing or past, arbitration case(s) with RailTel at the time of submission of bid.

I hereby acknowledge that in the event of acceptance of bid of M/s …….. on above undertaking and if the undertaking is found to be false at any stage, the false undertaking would be a ground for immediate termination of contract and further legal action in accordance with the Law, including but not limited to the encashment of Bank Guarantee related to Empanelment and Performance Bank Guarantee (PBG), as available with RailTel, related to this EoI.

Signature of Authorized Signatory

Name
Designation

Annexure-03

Scope of Work

1 Scope of Work & Service Level Agreements

CUSTOMER provides most of its business services on Internet through web and mobile applications of CUSTOMER spreading ease and convenience in reserved ticketing, travel & tourism offerings. The Cyber space is full of risks & threats and the situation is always evolving and there are threats that target the reputation and brand value. There is also requirement for take down of phishing domain/website, source code leaks, YouTube hacking tutorials, fake customer service numbers, fake social media profiles, fake mobile applications, phishing campaigns etc.

It is proposed the vendor shall provide the following services:

a) Carrying out brand monitoring activities in cyberspace to provide enriched threat analysis and building a dashboard for cyber security posture and status.

b) Vendor shall search the surface and dark web for cyber threat, data leaks, brand threats, identity threats etc. for defined digital assets and report to the organization for proactive and corrective actions.

c) Vendor shall carryout Infrastructure monitoring for vulnerabilities with recommendations.

d) The work will include the following aspects: -

i. Cyber Threat Intelligence
ii. Periodical Monitoring of ICT Infrastructure (Red Teaming)
iii. Takedown services.
iv. Periodical Threat Monitoring
v. Data Analysis
vi. Digital Risk Protection Services
vii. Threat research report (Analysis & reporting of incidents a required by CUSTOMER)
viii. Integrated Dashboard with user friendly features and aesthetic touch and feel to support easy viewing of all the activities summarized and with drill down facilities.

1.1 Detailed Scope of Work & requirements:

I. Cyber Threat Intelligence

Continuous monitoring of the internet social media, search engine and dark web etc. to identify, classify and neutralize the threats to the Services of CUSTOMER and its brand image. The sources of threat intelligence should include Dark Web, Social Media, Forums & other messaging platforms

(a) Threat intelligence feed collection and distributed to be automated using latest machine learning models and algorithms and should have a documented process to flag and verify the high value threat feeds by human team for further validation.
(b) Vendor shall correlate credible threats from intelligence feeds and carry out validation and analysis of the threat actor capabilities wherever available.
i. Analysis of the threat actor's infrastructure (wherever available)
ii. Analysis of the software binaries and infrastructure (wherever available)
iii. Study of the vulnerabilities in the CUSTOMER infrastructure that are being exploited by the threat actor
(c) Develop suitable remedial actions and share the same with the CUSTOMER team and assist them in implementing remedial actions.

II. Periodical Monitoring of Cyber Infrastructure: Red Teaming.

Analysis of the CUSTOMER Web and the Mobile Application to identify the gaps in the security of the web

application and mobile applications which are exploited by the threat actors is needed periodically. The team should also highlight the issues with the CUSTOMER team and provide assistance in covering the gaps and mitigation. Other scope of work on this topic includes:

(a) Forensic Analysis to identify the origin of threats, mitigation thereof, initiation of measures to prevent recurrence including - Identification of the original threat, conduct Root Cause Analysis & take measures for preventive recurrence.

(b) Monitor, Identify and respond to Clickjacking or similar vulnerabilities in customer websites which can potentially deface customer image.

(c) Dashboard to track the status of the customer's security risk and posturing and action taken.

III. Takedown Services

Vendor shall provide takedown service to initiate and manage takedown of fake/fraudulent websites and rogue mobile applications that are mimicking/defrauding CUSTOMER customers on the various web resources including websites, open web platforms and app stores.

(a) Vendor must provide the related intelligence collection and attribution capabilities in the Deep web and Dark web and various cybercrime forums.

(b) Vendor must provide nontechnical data/information/intelligence related to threat actor, attack campaign, analysis report, tactics, techniques and protocols (TTPs) and profile the Threat Actors.

(c) Vendor must gather Intelligence from the darkweb and open web with deep analysis processing of at least 5+ Languages (English & Indian) in which Threat Actors / Cyber criminals are most active in.

(d) Vendor must provide Intelligence in near real- time as new information or context is gathered from various sources.

(e) Intelligence provided by the vendor must have reference to the source of information should be stored and shared separately to look for evidence

(f) The vendor shall provide services that must able to create, monitor, automate alert and report for threat on Dark Web on frauds/threats/DRP but is not limited to, the following:

- Compromised credentials of CUSTOMER employees
- Sensitive information Leakage such as Usernames, passwords and access keys of the users of the CUSTOMER Platform
- Compromised PII such as Email ID, Phone number and Address of the users
- Sale of user IDs & details of CUSTOMER services
- Malware and Malicious Infrastructure related to Customer domain
- Leaked Source Code or Analysis of the Source code which would be exploited by the threat actors
- Copyright / Trademark infringement of CUSTOMER
- Technical Information / Data that could be used to compromise corporate systems.
- Mentions of IP Addresses and Infrastructure
- Executive Monitoring

- Exposed Executive credentials
- Executive mentions / Discussion on Executive on Dark Web

(g) The vendor should monitor Darkweb for the information and documents related to CUSTOMER and share the data on daily basis in an automated manner

(h) The vendor should incorporate a range of multi-layered monitoring services and analysis techniques and correlates data across a range of resources including:

- Tor. onion and alternative networks
- Dark Net blogs, forums, chat rooms
- Other communication channels suspected to be used by cyber-criminals
- The platform must collect relevant intelligence from Third party technologies including Telegram and P2P monitoring etc.

(i) The vendor all provide service to collect Open source intelligence from various English, Indian and non-English sources that are relevant for the cyber threat.

(j) Vendor's would deploy a portal for sharing the intelligence collected and offer a feature for queries and responses from CUSTOMER by the team.

(k) The vendor's portal should also have a separate module for authorizing take down of any content found objectionable or malicious by the CUSTOMER.

(l) Vendor should provide take down services up on authorisation received on the portal by the CUSTOMER during the period of the contract. The takedown services would be available for the following but not limited to,

i. Global content in case of issues such as: Copyright and trademark violations, , domain name registrations.

ii. Site take down/app removal from play stores, Removal of any other fraudulent or unauthorized content misleading citizens

IV. Data Analysis

Vendor shall provide Data Analysis services for analysis of user profile and/or suspicious transactions and correlating the same with the details such as,

- Suspicious parameters
- Previous Booking behavior
- Dark web, social media etc.

This is not a real time analysis. The Data for analysis will be shared/uploaded in the dashboard.

V. Periodical Threat Modelling

Threat modelling process starts with the collection of data about CUSTOMER and concludes with the evaluation of possible threats in cyberspace along with a priority ranking. This activity is carried out periodically to shape up the course of action to be adopted. The aspects that would be studied for the activity is the CUSTOMER presence in cyberspace and the threats to the CUSTOMER in the cyberspace from the point of view of the threat actors. Based on the observed trends in cyberspace a threat matrix would be prepared and data collection strategies would be designed accordingly.

VI. Digital Risk Protection Services (DRP)

Vendor shall provide DRP, to help CUSTOMER improve its security posture through proactive monitoring of Internet and dark web for:

- Fake Domains and Web Pages: Similar sounding/looking Domains/Websites are a real threat to organization. DRP checks with leading domain registrars like GoDaddy, Google domains and will help you with the takedown of impersonating websites.
- Fake Social Media Profiles: Detect if anyone is trying to impersonate your top executives on social media. Takedown of these are also included.
- Fake Mobile Applications: DRP scans for 3rd Party/official app stores for any fake/rogue apps that resonate with your brand's keyword and also helps in the takedown.
- Fake Customer Service Numbers: Fake customer care numbers are posted on internet forums and Social media to lure users to connect and then share critical details over the unofficial channel and eventually the end-user is compromised.
- Phishing Campaigns: Identify phishing attacks targeting organization and takedown of impostor domains and sites.
- Source Code Leaks: Scan all the major code-sharing platform and would alert as soon as there is a match as per organization's keywords for any source Code Leak.
- Server Credential Leaks: Monitor and report on any server credential leaks.
- Board Member Credential Leaks: Monitor top executive email ID's for any potential credential leaks.
- Wallet Scams: Wallet credentials are sold on Dark web, DRP Services helps detect and report these frauds.
- Hiring Scams: Search for fake job posts across social media as well as the fake website.
- 3rd Party Data Leaks: Identify if any data is leaked by your vendors using your IP's & keywords
- Business Email Compromise Attacks: Identify if any of employee's credentials are leaked online. Keeps updating the list if any new breaches surfaces
- Dark Web Conversations: Most malicious cyberattack planning and activity occur on the dark web. DRP solutions monitor all places where criminal activity is discussed and planned. This is vital to identifying and mitigating threats.
- Telegram Conversation Monitoring: Gather information from IRC (Internet Relay Chat) and Chat Rooms (Telegram channels) to identify if anyone is trying to weaponize/monetize or trying to gather information about CUSTOMER.
- YouTube Hacking Tutorials: Track down if any hacking tutorial has been posted about organisation and would assist with takedowns of these hacking tutorials

- Shadow IT Exposure: Performs daily scan for all Internet-facing infrastructure hence would be able to detect and report if any new server pops up/new sub-domain/new IPs/ new web/apps etc.
- Misconfigured Web Applications: Automatically alerts on any flaws in Internet-facing application, and scans the system thoroughly for any security vulnerabilities.
- Defacement Monitor: Alert if any defacement of web application occurs.
- Takedown Services: Takedown of phishing domain/website, source code repositories, YouTube hacking tutorials, fake customer service numbers, fake social media profiles, fake mobile applications, phishing campaigns etc.

(a) Threats from mobile app stores, including play store as well as third-party app stores,
(b) Fake/phishing domains that infringe upon your brand identity,
(c) Social Media takedown,
(d) DMCA takedowns for Intellectual Property.

The vendor shall provide service that would help Indian Railway Catering and Tourism Corporation by identifying and reporting (a) Cyber threats, (b) Brand threats and (c) Infrastructure threat.

VII. Threat research report (Analysis & reporting of incidents a required by CUSTOMER)

The vendor shall provide CUSTOMER a detailed Threat Research Report on specific incidents/cases on cyber threats. This report will provide detailed, in-depth information about the methodology, modeling, risk/threat score, recommendations.

Provide deep dive investigations including data breach reports, Threat actor profiling & tracking to protect data & brand reputation, preempt bad actor actions and incorrect media publicity by providing fact-based analysis, identifying root causes & providing mitigation measures for persistent threat.

Brand protection: Preempt bad actor efforts or negotiate from a point of strength, Spider web analysis for increased scope coverage & information based on extensive research and pattern recognition

Infrastructure Monitoring: This report will provide recommendations to plug-in vulnerabilities and improved CUSTOMER Security posture

VIII. Integrated Dashboard /Portal

This Integrated dashboard will provide details/visuals/reports as mentioned in above services & requirements of CUSTOMER. MIS reports on these items on daily, monthly, cumulative etc. should be made available.

The dashboard must have capability, or the platform developed must have capability to provide alerts in close to real time for fake customer care numbers, fake CUSTOMER services sites/apps, refund frauds for CUSTOMER with recommendations for takedown etc.

Provide visual report on the Cyber Security Posture of CUSTOMER and also on emerging threats. It shall provide links/summary/feeds to standard threat advisories.

The dashboard will be upgraded and updated as per access and inputs provided by CUSTOMER.

(a) Features of Integrated Dashboard /Portal

Based on the interactions and discussion with the CUSTOMER Team, the Vendor has to provide an integrated dashboard which provides MIS reports of all the analytics, recommendations, matrixes and models related to all the above requirements discussed in the SLA matrix with appropriate visual inputs so as to make the dashboard visually appealing and an easy to use User Interface. The vendor may provide facility to upload data for analytics (SoW # IV).

- **Cyber Threat Intelligence:**
  - Red Teaming and periodical scanning exercises the engagement also includes creation of a dedicated dashboard for CUSTOMER as a part of the portal which provides security risk visualization of CUSTOMER infrastructure for threats with a color coding for the magnitude of the risk posed and the action needed to mitigate the risk. The dashboard would contain the details of the software observed along with their corresponding risk score, severity classification and recommended course of action for its removal or mitigation.

- The platform will also include a visualization of the cyber vulnerabilities observed by the team from the external world and their current status with various analyses including the CVE Score, classification and possible methods to mitigate the vulnerabilities.

- **Brand Threat Intelligence:** Based on the interactions and discussion with the CUSTOMER Team, an automated threat actor intelligence feed based on machine learning will be created which continuously provides the following output via a dedicated custom built portal for CUSTOMER,
  - Source of the threat actor.
  - Modus Operandi of campaign/threat/activity.
  - Sensitive keyword search.
  - Understanding of threat actor code, infrastructure.
  - All the above findings will be available on the portal and a custom report would be generated daily/fortnightly (depending up on the CUSTOMER needs after discussion) based on the observed trends in cyberspace.

- **Take Down Services:** Based on the interactions and discussions with CUSTOMER, takedown services will be offered via the custom made portal. The portal will contain the list of requests for takedown and current status as available with the vendor. The takedown authorizations requests issued on the portal will contain the following details, which will be shared with CUSTOMER depending on the seriousness of the alerts:
  - Latest Threat actor information available with vendor.
  - The mechanism (campaign, tactics, techniques, practices etc) through which the threat actor has attempted to harm CUSTOMER directly or indirectly.
  - Open source intelligence wherever possible regarding the threat actor which is verifiable

1.2 Service Level Agreements : SLA measurement and penalty shall be on back to back basis as per agreement between RailTel and Customer. Tentative SLA details are as below:

1.2.1 SLA

- **Cyber Threat Intelligence & DRP:** Based on the interactions and discussion with the CUSTOMER Team, threats would be categorised into following,
  - Critical
  - High Risk
  - Medium Risk
  - Low Risk
  - Information
  - Critical and High Risk Threats will be communicated at the earliest but not later than 24 hours of identification by the vendor to the customer at the email address provided for communications.
  - Medium and Low Risk threats would be communicated within 48 hours of detection.
  - Informative events would be included in the monthly report along with all other categories of events observed in the month.

- **Red Teaming:** Based on the interactions and discussion with the CUSTOMER Team and after taking necessary inputs and authorizations from the CUSTOMER Team, the vendor has to periodically conduct red teaming of the client infrastructure (Mobile and Web application) to analyze the following:
  - Gaps/loopholes in ICT Infra/Network which can be exploited by threat actors
  - Assisting in Root cause analysis in case of any breach by threat actors and support in advising effective mitigation measures.

If no such analysis is done within 3 months or any other frequency mutually agreed up on, penalty of Rs 25,000/- will be imposed for every 15 days of delay.

1.2.2 SLA on Periodical Reports

- Vendor will also provide a detailed monthly report with CUSTOMER on the vulnerabilities observed and recommendations for mitigation keeping in mind the checking of misuse by threat actors.

- The other aspect of SLA includes a mechanism to monitor any clickjacking attempts, keep count of the attempts and modus operandi of attack and mitigation efforts in case any customer of CUSTOMER has suffered.
- Based on the interactions and discussion with the CUSTOMER Team, Vendor should provide a monthly report consisting of a threat matrix on the different attack vectors of CUSTOMER threat actors. The report should also include attack vectors which may not involve CUSTOMER directly but could cause significant reputational harm for eg: fake websites, fake job email campaigns etc. Different probabilities should be accorded to each attack vector, the mechanisms which can be used according to the attack vector and mitigation measures which need to be taken to mitigate the attacks.
- Based on the interactions and discussion with the CUSTOMER Team, Vendor should provide a monthly list of:
  - Fake domains doing cybersquatting to be blacklisted.
  - Fake social media profiles to be reported and taken down.
  - Fake mobile applications to be taken down.
  - Fake customer service numbers.
  - Source code and server credential leaks in dark and deep web.
  - Board Member credential leaks.
  - List of phishing campaigns.
  - List of fake job campaigns.
  - Users Wallet details leaked.
  - Third party data leaks of user/CUSTOMER data.
  - Fake Email campaigns.
  - List of YouTube hacking tutorials.
  - Telegram Group Chat monitoring reports concerning CUSTOMER services.
  - Reports on dark web conversations/chatter in hacker forums involving CUSTOMER.
- Based on the interactions and discussion with the CUSTOMER Team, the vendor should provide a monthly threat research report which consists of the following things:
  - CUSTOMER Threat Matrix.
  - Data breaches and cyber-attacks on the CUSTOMER infrastructure.
  - Malicious campaigns which have been detected in social media and dark web.
  - Root Cause analysis of attacks, data breaches and successful attempts
  - Recommendations on mitigations required in CUSTOMER cyber infrastructure so that the attacks don't get repeated again.
  - A threat score which can communicate in a single number how risky/safe.
  - A list of all the takedowns initiated or completed.

Delay in the periodical (monthly) reporting will be levied with penalty of Rs 5,000/- for every week of delay.

1.2.3 SLA on Takedown Services

- Takedown action will be undertaken by the vendor after taking necessary authorisation from CUSTOMER. The authorisation for take down will be taken through the portal that is being built. This will cover applications which can tarnish CUSTOMER brand image, cyber infrastructure or cause harm to CUSTOMER users.
- Based on the interactions and discussion with the CUSTOMER Team, the vendor has to initiate the takedown services of the following categories of websites **within 24 hours** of the authorisation received from the portals. Vendors will keep CUSTOMER informed on the status of the takedown periodically.
  - Indian Hosted Site.
  - Foreign Hosted Site (Friendly/DMCA Compliant)
  - Foreign Hosted Site (Non DMCA Compliant)
- The takedown authorisation will contain the following details, which will be shared with CUSTOMER depending on the severity score of the alerts:
  - Latest Threat actor information.
  - The mechanism (campaign, tactics, techniques, practices etc) through which the threat actor has attempted to harm CUSTOMER directly or indirectly.
  - Open source intelligence wherever possible regarding the threat actor which is verifiable.

If the above SLAs are violated for more than 10 times in the course of 6months, the tender is liable to be terminated and can be a ground for no extension.

Proforma for Performance Bank Guarantee Bond

Form No. 1

PROFORMA FOR PERFORMANCE BANK GUARANTEE BOND
(On Stamp Paper of Rs one hundred)

(To be used by approved Scheduled Banks)

1. In consideration of the RailTel Corporation of India Limited, having its registered office at Plate-A, 6th Floor, Office Tower-2, NBCC Building, East Kidwai Nagar, New Delhi-110023 having agreed to exempt ……(Hereinafter called "the said Contractor(s)") from the demand, under the terms and conditions of an Purchase Order No.……dated……made between……and…….. for (hereinaftercalled " the said Agreement") of security deposit for the due fulfillment by the said Contractor (s) of the terms and conditions contained in the said Agreement, on production of a Bank Guarantee for Rs. ……(Rs …….. only). We …… (indicate the name of the Bank) hereinafter referred to as "the Bank") at the request of…….…. Contractor(s) do hereby undertake to pay the RailTel an amount not exceeding Rs……..…. against any loss or damage caused to or suffered or would be caused to or suffered by the RailTel by reason of any breach by the said Contractor(s) of any of the terms or conditions contained in the said Agreement.

2. We, ……. Bank do hereby undertake to pay the amounts due and payable under this Guarantee without any demur, merely on demand from the RailTel stating that the amount is claimed is due by way of loss or damage caused to or would be caused to or suffered by the RailTel by reason of breach by the said Contractor(s) of any of terms or conditions contained in the said Agreement or by reason of the Contractor(s) failure to perform the said Agreement. Any such demand made on the Bank shall be conclusive as regards the amount due and payable by the Bank under this guarantee. However, our liability under this guarantee shall be restricted to an amount not exceeding Rs . ……

3. We, …….. bank undertake to pay to the RailTel any money so demanded notwithstanding any dispute or disputes raised by the Contractor(s) / Tenderer(s) in any suit or proceedings pending before any court or Tribunal relating thereto our liability under this present being, absolute and unequivocal. The payment so made by us under this Bond shall be a valid discharge of our liability for payment there under and the Contractor(s) / Tenderer(s) shall have no claim against us for making such payment.

4. We, ……. Bank further agree that the Guarantee herein contained shall remain in full force and effect during the period that would be taken for the performance of the said Agreement and that it shall continue to be enforceable till all the dues of the RailTel under or by virtue of the said Agreement have been fully paid and its claims satisfied or discharged or till RailTel certifies that the terms and conditions of the said Agreement have been fully and properly carried out by the said Contractor(s) and accordingly discharges this Guarantee. Unless a demand or claim under the Guarantee is made on us in writing on or before the ……..…… We shall be discharged from all liability under this Guarantee thereafter.

5. We,…… (indicate the name of Bank) further agree with the RailTel that the RailTel shall have the fullest liberty without our consent and without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the Agreement or to extend time of to postpone for any time or from time to time any of the powers exercisable by the RailTel against the said contractor(s) and to forbear or enforce any of the terms and conditions relating to the said Agreement and we

shall not be relieved from our liability by reason of any such variation, or extension to the said Contractor(s) or for any forbearance, act or omission on the part of RailTel or any indulgence by the RailTel to the said Contractor(s) or by any such matter or thing whatsoever which under the law relating to sureties would, but for this provision, have affect of so relieving us.

This Guarantee will not be discharged due to the change in the Constitution of the Bank or the Contractor(s) / Tenderer(s).

(indicate the name of Bank) lastly undertake not to revoke this Guarantee during its currency except with the previous consent of the RailTel in writing.

……the day of 2024

for ……..
(indicate the name of the Bank)

Witness

1. Signature Name
2. Signature Name

Note: Claim Period of BG will be 365 days more than the BG Validity date.

RailTel Bank Detail for SFMS are:

- To mandatorily send the Cover message at the time of BG issuance.
- IFSC Code of ICICI Bank to be used (ICIC0000007).
- Mention the unique reference(RAILTEL6103)in field 7037

********End of EOI document ********