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/11 dated 01.12.25

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/11 dated 01.12.25

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	08-12-2025 before 15:00Hrs.
Opening of bidder EOIs	08-12-2025 at 15:30 Hrs.
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 1: Rosy Sharma
Position: AGM/DNM
Email: rosys@railtelindia.com Telephone: +91124 2714000 Ext 2216

Contact 2: 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 & Cloud Services, Application Development, ERP/E-Office Implementation and Consultancy Services for its customers. RailTel is in process of selecting suitable empanelled partner for providing customer specific IT services.

3. Scope of Work

The scope of work is to provide "DC security Solution" on service modal for RailTel's Customer as per Schedule of Requirements (SoR) Clause 10. Technical Specification 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.

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

8. Delivery Schedule: SITC of SOR items shall be within 6-8 weeks of issue of PO.

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 with valid UDIN number for preceding three years.

9.8. The bidder should be profitable organization (on the basis of operating profit after tax for at-least 2 out of last 3 financial years). Bidder should submit copy of audited balance sheets along with profit & loss statement and certificate of CA with valid UDIN for positive net worth during proceeding three years.

9.9. The interested bidder should have experience in Data Centre infra project. Bidder should submit PO or work order copy/copies with completion certificate for the work of SITC of Data Centre Infra project of contract value as under for the work of SITC during last seven years from any government organization:

9.9.1. Three similar works each with value costing not less than than 30% of total quoted SOR price.

9.9.2. Two similar works each with value costing not less than than 40% of total quoted SOR price.

9.9.3. One similar works each with value costing not less than than 60% of total quoted SOR price.

9.10. Bidder is required to submit authorization from OEM (MAF or mail confirmation from OEM).

10. Schedule of Rates

SN	Item Description*	Qty. (Min User Count considered)	Unit	Rate per Unit	Total Rate	GST	Total Rate with Tax
1	Security Service Edge (SSE) SWG, DLP & CASB with 3 years warranty	200	Number				
2	Email Security with 3 years warranty	200	Number				
3	Endpoint Security (EDR) with 3 years warranty	200	Number				
4	Patch Management with 3 years warranty	200	Number				

5	Backup Management with 30 TB NAS and with 3 years warranty	200	Number				
6	**Total SOR**						

SOR Total in words (including tax) : _____

***Technical specification for above SOR items is provided under Annexure-03**

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 on back to back basis. 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. Documents with respect to compliance requirement clause (9.1 to 9.10).
8. Deviation statement as per clause number 23. In case of No deviation, bidder must submit "No deviation" under statement of deviation.

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)

Successful bidder has to furnish security deposit in the form of Performance Bank guarantee @ 5 - 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 (IncludingJustification)

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 for three years from project/services commissioning /Go live . 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.

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/11 dated 01.12.25**

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/11 dated 01.12.25

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/11 dated 01.12.25

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

Technical Specification

Security Service Edge (SSE) Technical Specifications for SWG,DLP, and CASB	
S.No.	**Technical Requirements**
A	**General Platform Features**
1	The proposed SSE platform shall improve cybersecurity posture by implementing Unified, Consolidated Cloud Based SSE Platform and Single End User Client with at least the below functionalities from Day 1:
	1. Secure Web Gateway: For URL/Content Filtering
	2. Cloud Access Security Broker: For Internet/SaaS Application Control and Filtering
	3. Threat Protection: Comprehensive Threat Defense with Anti-Malware, Anti-Virus, Web IPS for Advanced/Targeted Attacks, User Entity Behaviour Analysis.
	4. Data Loss Prevention: To identify, detect and protect sensitive Data from exfilteration (Web,SaaS, IaaS,Email and Endpoint) channel
	5. Zero Trust Network Access: To adopt Identity based Secure Remote Access to Internal Applications
2	The proposed SSE solution OEM should be a Leader in Gartner Security Service Edge (SSE) Magic Quadrant 2024 or latest.
3	The solution must have single light weight user agent and supported on Windows, MAC, Linux, ChromeOS. This Agent must be tamperproof and the User must not be able to disable or uninstall it even if the User has local system Admin Rights.
4	The proposed solution should have CSA STAR, SOC 2, CIS, ISO 27001, ISO 27017, ISO 27018 certification and must be a part of Microsoft Active Protections Program (MAPP) to help integration with O365 services deloyed at .
5	User License for any proposed component must not be limited by any bandwidth or data cap and licensing should not depend on Bandwidth consumed by users.
6	The solution must have granular role based access control (specific admins as like for Threat, data protection and Access Control should be able to monitor and control only their specific policies and reportings).
7	The OEM must perform a Quarterly Analysis of the Product Adoption, Best Practice Policies and Usage, Recommendations to improve the overall SSE Usage and Security Posture Strengthening for . These findings, and recommendations shall be presented to every Quarter and action plan for implementation shall be discussed and gaps against previous quarted actions shall be brought out clearly .
B	**Secure Web Gateway**
Intent: Provide Secured Internet Access to Users & Locations using URL/Content Filtering Policies configured based on URL Categories	
1	The solution must operate in a full-proxy architecture and should perform 100% SSL inspection at scale. The solution must detect and block malware passing in an encrypted HTTPS tunnel. This must include the capability to Inspect the Web Traffic sent by CLI Commands (For ex. S3) and Thick Clients like MS Teams to enable secured transactions without any user experience issues from Day 1.

2	The Secure Web Gateway must provide the granular Visibility and Control on O365 The solution include detailed oversight and management capabilities across multiple instances of O365, including OneDrive for Business, SharePoint, Teams, Yammer, GitHub, AWS etc. The solution must support Activities(Post,upload,dwnnload,Share,Delete, Shutdown,reboot etc.)
3	The proposed solution should be able to provide URL Filtering and must have capability to enforce granular advance activity control as mentioned below:
	a. Webmail Category: Upload, Download, & Attach,Send,
	b. File Sharing / Cloudstorage category: Upload, Download, & Post.
	c. Collaboration Category: Upload, Download, & Post
4	The solution must have the following traffic forwarding methods from Day 1:
	a. User Agent
	b. Encypted Phase 1 and Encrypted Phase 2 IPSec Tunnel
	c. GRE Tunnel
	d. Explicit Proxy / PAC Based
5	The solution must be deployed for securing Internet Access in the following existing scenarios:
	a. Employee Laptops: By deploying User Agent
	b. Servers: By deploying Explicit Proxy or IPSec/GRE Tunnels
	c. Locations (Approximately 50) with Guest WiFi: By deploying IPSec/GRE Tunnels
6	The Solution must have DEM (Digital Experience Management) License for 5,00 Users for minimum 10 SaaS Apps/Probes to find out issues related with Applications, Hop-by-Hop Latency and Network path tracing including hop by hop analysis of all internal and external hops on every probe with ISP/AS Number & Geo details for each hop, Page Load Times, User Device Stats (CPU, Memory, Network, Storage) and effectively reduce mean time to identify root cause of experience/performance issues and help in resolution.
7	The DEM (Digital Experience Management) module must poll/probe the monitored SaaS Applications every 5 minutes or less to ensure consistent and frequent monitoring for efficient troubleshooting.
8	The proposed solution must provide secure and controlled internet access to the guest users who would connect to guest Wi-Fi network for internet browsing. The traffic of guest users must be controlled without any dependency of an endpoint agent or any changes on the user endpoints.
9	The solution must support the validation of internet websites with an untrusted server certificate. It must support OCSP (Online Certificate Status Protocol) to obtain the revocation status of an application/server with an untrusted certificate and take the required action, which includes allowing, blocking, or passing through the access with a warning to the user.
10	The offered solution shall support the following User Authentication methods:
	• Microsoft Active Directory,
	• LDAP
	• SAML
	• ADFS
C	**Inline CASB (Cloud Access Security Broker)**
Intent: Discovering Sanctioned and Unsanctioned SaaS usage (ShadowIT), Internet Risk Analysis and Control using granular Applicaton based policies	

1	The solution should support real-time visibility for minimum 80,000 sanctioned and unsanctioned applications with dynamic risk score based on Cloud Security Alliance Standards. The solution must be able to report the security compliances and certifications achieved by these apps.
2	Solution must be able to determine the Instance/Tenant of Internet/SaaS Applications being accessed and enforce dedicated Access Control and Data Protection Policies for each Tenant/Instance of the same Application. This capability must be supported across hundreds of Internet/SaaS Appliations including MS O365 where the Solution must decrypt the SSL traffic destined to O365 Apps.
3	The Solution must be able to enforce policies based on Granular Activity Control for all well known SaaS Applications.
4	The Solution must support CLI (AWS S3 bucket and WebUI for Specific Services: It is essential to have command-line interface (CLI) and web user interface (WebUI) capabilities for specific services, enabling efficient management and control
5	The solution must be able to enforce granular activity based policies on users trying to access official Internet Apps (O365, Google and more) via an Unmanaged Device like Tablet or Personal Laptops.
6	The solution must provide the granular visibility and control on Azure, AWS allowing monitoring and management of cloud resources within the environment.The solution must support data protection on Azure blob storage, S3 buckets. The solution must support the DLP capabilities accessing S3 buckets via CLI.
7	The solution must provide coach Users: Provide automated and customized coaching messages to educate and guide users regarding undesirable cloud activities and the risks associated with uploading sensitive data to unmanaged cloud services.
8	The solution must provide the granular Visibility and Control on Generative AI applications like (ChatGPT,MS copilot etc. Solution must be able to determine the Instance/Tenant of Generative AI applications being accessed and enforce dedicated Access Control and Data Protection Policies for each Tenant/Instance of the same Applications.
D	**Threat Protection**
Intent: Protection of Users against Web & SaaS Delivered Threats	
1	The solution must have the below threat protection modules to protect against Internet based Threats:
	a. Anti-Malware Engine (for Viruses, Malwares, & Trojans)
	b. Web and Non-web IPS (for Advanced Threat Protection against C&C Servers, DGA botnet attacks, malicious active content, P2P anonymisers)
	c. Inline Sandbox which leverages AI and Machine Learning based analysis and Patient Zero infections across PE (portable executable) file types..
2	The proposed solution must have integration with Third Party Threat feeds and the capability for bi-directional IOC exchange (MD5,SHA.urls etc) through custom rest API's.
3	The solution must be able to inspect & block multilayer zipped / compressed files.
5	The proposed solution must provide open threat intel exchange platform to integrate with customer environment existing security stack such as EDR Solutions, Threat intel exchange solution, SIEM solutions, SSO solutions etc.
7	The solution should have capability to provide UEBA profiling based on the below parameters:

	A. **Data exfiltration**: Capability to detect and alert in case the user downloads file from a corporate instance of SaaS app like OneDrive and transfers the files to Personal Account.
	B. **Location Awareness**: Capability to detect and alert in case the geolocation of the user changes abruptly and in a non-realistic fashion (for ex. India Users suddenly logged in from Russia)
	C. **Bulk Upload and download**: Capability to detect and alert in case the User Uploads or Downloads files from Corporate Applications in Bulk.
	D. **Bulk Deletion of files**: Capability to detect and alert in case the User Deletes files in Corporate Applications in Bulk.
	E. **Login failures**: Capability to detect and alert in case the User makes multiple and continuoius failed login attempts to a corporate application
E	**DLP**
Intent: Protection of Sensitive Data against exfiltration	
1	The DLP solution will include the following features and not be limited to:
	• Must cover all the channels – Email, web, SaaS,IaaS and Endpoint
	a. End points (Desktops, Laptops etc.)
	b. Endpoint include USB, External storage, Print, Bluetooth and Network Share.
	c. Applications & native apps including One drive for business clients.
	d. Email DLP
	e. Support for Office 365
	f. Cloud storage: One drive for Business, Google drive,Blob Storage, S3 Buckets etc.
	g. Virtual desktops – Citrix, virtual systems (VMware's / Virtual Box)
2	The Solution must have DLP Capabilities and must be able to create DLP Policies based on content, keywords, patterns, size, upload URL, user group etc. and a combination of all or some of these. The DLP Capabilities must not be dependent on Browser type and version.
3	The solution must be able identify and protect minimum 500 pre-defined file types based on true file type detection.
4	The solution must Scan outbound email for sensitive data (Attachment, Body, Text and subject).Generate admin alerts/block/quarantine when emails body include the that contains sensitive data Aadhar, PAN etc. information. Generate admin alerts/block/quarantine when emails attachment include the that contains sensitive data PCI,PII,etc. information
5	The solution must have the capability to use new-age technologies like Artifical Intelligence and Machine Learning to understand sensitive documents and protect against data leakages over web channel from day 1. The solution should support the add-on license based capability to use the AI and ML Engines to detect and prevent data leakages happening over Web Channel via Screenshots, Images without using OCR.
6	The solution must be able to detect data leak through thick clients for applications like OneDrive, Teams etc. using the license provided
7	Must support Luhn checks as well as create policies with Boolean logic controls (AND,OR,NEAR), proximity analysis as well as threshold based DLP policies
8	The solution must Govern endpoint device control (USB,Printer,Bluetooth and Network Share policies). The Solution must allow/Block devices base of Device ID, Manufacture, Device Serial number etc.
9	The solution must Govern content (PII,PCI etc.) inspection policies on USB,Printer,Bluetooth etc.

10	The solution must support the multiple actions ,Alert,Block and coach if any sensitive data transfer on USB,Printer,Bluetooth the coach option provide the justifications/reason for data transfer.
11	The solution must support file origin path e.g. if file is download from One Drive and copied in external storage USB etc.
12	The solution must support Monitor endpoint activities and block or trigger alerts when users insert or remove USB storage devices, transfer sensitive files to USB storage devices, set up and configure printers, and print documents
13	The solution must enforce configurable End User notification with Justification popup window while accessing any Internet destination. This justification must be recorded for forensic analysis.
14	The solution must have an inbuilt and dedicated page for DLP Incident Management on the Admin Portal to effectively manage DLP Incident Workflow. The Solution's Incident Management Page must be able to be integrated with variety of ITSM tools from Day 1.
15	The solution must support at least 10+ compliance templates including GDPR, PII, PCI, PHI, source code, etc to ensure necessary compliances.
16	The Solution must be able to inspect Web Traffic from CLI (AWS S3 and more) and Thick Clients (MS Teams and more) and protect any sensitive data from being leaked out from Day 1.
17	The solution must have the functionality to download Original File which violated DLP Policies directly from the Admin Portal. This should be included in the solution from Day 1. If On-Prem components are needed for this, bidder must factor in those.
18	
	The solution must integrate with Third party classification tools e.g MIP for tagging of data.
G	**Device Posture**
Intent**:** *Understanding Device Compliance status based on configured checks and ensuring only compliant devices which pass these parameters get access to critical Internet and Internal Destinations*	
1	The SSE solution must have continuous (every 15 minutes or less) device posture validation for Internet & Internal Apps across multiple parameters like Device Encryption, Registry Check, Process Check, AD Domain Check, and Certificates etc to provide Internal App or Internet Access based on granular policy controls.
H	**Authentication**
Intent: Establishing User Identity before allowing access to the Internet and Internal Applications, typically done via On-Prem AD, SAML Integration	
1	The solution must be able to integrate with any SAML 2.0 IdP (ex. Azure AD, Okta and ADFS etc.) and on-premise AD without any inbound exposure to AD from Internet.
2	The Solution must have a native MFA integration for the Admin Accounts created locally on the SSE Admin Portal to ensure secured and authenticated access.
3	The Admin Consoles of the Solution must only be accessible from Public IPs to avoid any unauthorized access.
I	**Logging and Dashboard**

Intent: For to get Comprehensive Web Usage Dashboards, Visibility into ShadowIT Risk, Predefined, Scheduled & Custom Reports to deal with Security and User Experience	
1	The proposed solution must have in-built End-User Log retention for atleast 90 Days on Admin Portal for all components (SWG, CASB, ZTNA, Threat Protection, DLP etc).
2	SIEM integration should be supported with on-prem and cloud based SIEM solution (Encrypted communication).
3	The solution must provide detailed analytics executive reports and multiple pre-defined dashboards providing overview of SSE platform along with the ability to customise reports as per requirements. The solution must allow scheduled delivery of reports to the admins via email/pdf/csv. The customisation shall be in scope of bidder.
J	**SLA / Support**
1	The solution must provide 99.999% uptime SLA.
2	The proposed solution (including all components) should have direct OEM 24x7x365 support with following Initial Response Time SLA's:
	P1 (Urgent) <= 30 Min
	P2 (High) <= 2 hour
	P3 (Normal) <= 8 hour
	P4 (Low) <= 24 hour
K	**Completeness of the solution**
1	The bidder shall take in to account the above technical requirements along with the BOQ for deciding upon the required licenses, components - software and Hardware to bid for a complete solution even if any particular component is not specifically mentioned but is required to achieve the required functionalities.

Endpoint Protection with EDR	
S.No.	**Technical Requirements**
1	Must offer comprehensive endpoint security by providing protection from virus, spyware, rootkits, bots, grayware, adware, malware and other computer borne threats or mixed threat attacks or any emerging cyber-attacks or zero day attack protection.
2	Solution must clean computers of file-based and network viruses plus virus and worm remnants (Trojans, registry entries, virus files) through a fully-automated process.
3	Must be able to reduce the risk of virus/malware entering the network by blocking files with real-time compressed executable files.
4	The solution should have in built from day one - machine learning technology and ransomware protection.
5	Must provide Real-time spyware/grayware scanning for file system to stop spyware execution or restore if spyware is deemed safe.
6	Solution must have device control capabilities like block Autorun on USB, Allow Programs to execute on restricted USB devices.

7	Must have Assessment mode to allow first to evaluate whether spyware/grayware/ malware is legitimate and then take action based on the evaluation
8	Solution should have these capabilities with a single unified agent- Machine learning(pre-execution and runtime),Behavioral analysis (against scripts,injection, ransomware, memory, and browser attacks),In-memory analysis for identification of fileless malware,malware variants protection,Census check,Web reputation,Exploit prevention (host firewall, exploit protection),Command and control (C&C) blocking,Data loss prevention (DLP),Device and application control, Ransomware rollback,support integrated custom Sandboxing capabilities.
9	To address the threats and nuisances posed by Trojans, the solution should be able to do the following but not limited to: a) Terminating all known virus processes and threads in memory b) Repairing the registry c) Deleting any drop files created by viruses d) Removing any Microsoft Windows services created by viruses e) Restoring files damaged by viruses f) Includes Clean-up for Spyware, Adware etc.
10	Must be capable of cleaning viruses/malware even without the availability of virus clean- up components. Using a detected file as basis, it should be able to determine if the detected file has a corresponding process/service in memory and a registry entry, and then remove them altogether.
11	Must provide suitable Outbreak Prevention Solution either through limit/deny access to specific shared folders and deny write access to specified files and folders on selected customers or equivalent features in case there is an outbreak.
12	Behaviour Monitoring : a) Must have behaviour monitoring to restrict system behaviour, keeping security related processes always up and running b) Enable certification that a software is safe to reduce the likelihood of false positive detections or equivalent
13	Must provide option to prevent users from changing settings or unloading/uninstalling the software
14	Must allow users with the scheduled scan rights to postpone, skip, and stop Scheduled Scan.
15	Solution must have CPU/memory(physical or virtual) usage performance control during scanning : a) Checks the CPU usage level configured on the Web console and the actual CPU consumption on the computer b)Adjusts the scanning speed. c)The CPU usage level is High,Medium or Low d) Actual CPU consumption exceeds a certain threshold
16	Should have a manual outbreak prevention capability that allows administrators to configure deny write access to files and folders manually, deny access to executable compressed files.
17	Should have the capability to assign a customer the privilege to act as a forward relay agent for rest of the agents in the network.
18	Shall be able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)

19	Solution shall be able to scan only those file types which are potential virus carriers (based on true file type)
20	Should be able to detect files packed using real-time compression algorithms as executable files.
21	shall be able to scan Object Linking and Embedding (OLE) File
22	Must provide URL threat protection by the following ways: a) Must be able to protect the endpoints from Web threats by blocking access to and from malicious sites based on the URL's reputation ratings b) Must extend Web threat protection to the endpoints even when they disconnect from the network, i.e. regardless of the location c) Must have the capabilities to define Approved URLs to bypass Web Reputation policies d) Must provide real-time protection by referencing online database with millions of rated Web domains e) Configure Web reputation policies and assign them to individual,several, or all end users machine.
23	Must provide File reputation service a) Must be able to check the reputation of the files hosted in the internet b) Must be able check the reputation of the files in webmail attachments c) Must be able to check the reputation of files residing in the computer
24	Solution must be a leader as per latest report from Gartner/Forrester for Endpoint Protection Platform.
25	Must provide the flexibility to create firewall rules to filter connections by IP address, port number, or protocol, and then apply the rules to different groups of users.
26	Must enable feedback from the customer agents to the threat research Centers of the vendor.
27	Endpoint security solution should provide vulnerability protection & CVE number visibility against vulnerability.
28	Should be able to deploy the Customer software using the following mechanisms: a) Customer installation Package (Executable & Microsoft Installer (MSI) Package Format), should support silent installer, unmanaged customers, specific installer for servers b) Web install page c) Login Script Setup d) Remote installation e) From a customer disk image
29	Must provide a secure Web-based management console to give administrators transparent access on the network
30	The management server should be able to download updates from different sources if required & Management Server should be on premise only & not SaaS (Software as a Service) .
31	Must reduce network traffic generated when downloading the latest pattern by downloading only incremental patterns.
32	Must have the flexibility to roll back the Virus Scanning Patterns if required via the web based management console
33	Should have role based administration with active directory integration

	a) To create custom role type b) To add users to a predefined role or to a custom role
34	Should have integration with the Active directory
35	Shall support grouping of users in groups/domains for easier administration.
36	Establish separate configuration for internally versus externally located machines (Policy action based on location awareness)
37	Must be capable of uninstalling and replacing existing customer antivirus software and to ensure unavailability of any residual part of the software.
38	Security Compliance should leverage Microsoft Active Directory services to determine the security status of the computers in the network
39	Should have a feature similar to Firewall Outbreak Monitor which sends a customized alert message to specified recipients when log counts from customer IPS, customer firewall, and/or network virus logs exceed certain thresholds, signalling a possible attack.
40	System should be configured with the option that endpoints can get updated directly from internet or from local security server. This option can be used with flexibility to allow endpoint to get update from internet or block to stop update from internet.
41	The Solution must support both IPV4 & IPV6
42	Apart from Scheduled Scan, Solution must provide an option to administrator to run remote scan on endpoints whenever it is required.
43	Solution must have following criteria to allow and block an application execution on the endpoint :-
a	Application reputation
b	Certificates
c	Hash values
d	Grayware software
e	File Path
	Capability to enhance security through Endpoint Detection and Response component to provide advanced threat detection, incident response and provide forensic data on incidents like DLP
44	Provides context-aware endpoint investigation and response (EDR), recording and detailed reporting of system-level activities to allow threat analysts to rapidly assess the nature and extent of an attack.
45	The solution should be able support to perform threat sweeping based on the threat feeds received from the integrated sandbox solution as mentioned below
	1. IP Address
	2. Files
	3. URLs
	4. Domain
46	Solution must perform threat sweep across endpoints using rich-search criteria as mentioned below
	1. OpenIOC, STIX & Yara
	2. User-defined criteria like User Name, File - Name, File - Hash (SHA1 and SHA2) IP address, Hostname, Registry Key, Registry Value Name & Registry Value Data

47	The solution should be able to create detailed execution analysis/kill chain for performing the root cause analsysis of an incident. Kill chain also provide reputation of the files from the global threat intelligence as well
48	The solution should provide option to sweep and assess the current(point in time/Live) state of the devices.
	1. Scan disk Files
	2. Scan in memory process
	3. Search registry
49	The solution to provide the advance response capabilities as mentioned below
	1. Kill process
	2. Isolate device
	3. Block process
50	The solution shall allow ingestion of IOCs (Indicators of compromise) like domains,file-hashes and allow blocking of the files/file-hashes/domains/URLs identified by the IOCs
51	Solution should provide visibility and control across your endpoint environment and this may further be extended through integrated endpoint detection and response (EDR) capabilities for detection, investigation, and threat hunting capabilities.
52	Solution should provide protection against zero-day threats with multiple of next-gen anti-malware techniques and the industry's most timely Compensatory control patching.
53	Solution must provide vulnerability protection, application control,device control, data loss prevention and EDR in a single agent, Solution must have certificate based allow/block feature in endpoint Application Control
54	Solution must Respond to attacks with real-time and local threat intelligence updates and a broad API set for integration with third-party security tools.
55	Solution should support to be able to work with connected threat defense system wherein solution should be able to share the suspicious objects/detected IOCs for the unknown threats which are analyzed in custom sandboxed environment.
56	Solution must have C&C callback detection and protection.
57	Solution must support Browser Exploit Protection.
58	The solution must provide Antivirus software having real-time, scheduled and on-demand/ad-hoc remote scanning and detection of known and unknown malware compromising the integrity of critical information infrastructure and endpoints, blocking of various types of threats such as viruses, Trojan and ransom ware,
59	Provide centralised management to monitor and manage security policies across all endpoints, enforce policy including firewall rules, device control, application control, regular updates to ensure protection against latest known vulnerabilities with CVE cross referencing and malware strains.
60	Capability to enhance security through Endpoint Detection and Response component to provide advanced threat detection, incident response and provide forensic data on incidents like DLP
61	The solution should provide Multiple Device Support, USB Device Access Control, block auto-run on USB, allow programs to execute on restricted USB devices, offline support and Monitoring, Workstations, control and regulate the use of printers, web cameras, network shares, PCMCIA devices etc.

62	The Data Loss Prevention component must provide content discovery, policy-based controls, and integration with endpoint security, uses data identifiers to identify sensitive information, provide response and logging.
63	The solution must provide Central Management Console with interfaces for Defining and Managing Configuration, devise Policy and undertake editing of policy settings, Scalability, Exception Management, Application Control (based on file path, certificate, hash value and grey list of applications), Automatic Client Updates, Live Security Alerts, Mass Updates, Remote Software Installation, Updates and Reporting
64	Solution should be a leader in Gartner Magic Quadrant for Endpoint Protection Platforms from last three consecutive latest reports have should have presence in India since last 10 years.
65	Proposed OEM should have contributed 25+ zero-day vulnerabilities in last one year. This information should be publicly available.

Patch Management	
S.No	**Technical Specification**
1	The proposed solution should come along with standard reports and can generate the customized reports as per business requirement. The Patch Management solution should be capable of generating real-time reports on patches deployed, when, by whom, to which endpoints, etc.
2	Dashboard for senior management with Standard Information, customized on demand.
3	Report on installed and missing OS patches
4	Capability to Identify the devices where patches are applied but not yot activated (pending restart)
5	Capability for Bandwidth Throttling during Patching
6	The Solution should be capable of generating different reports based on relevant information from different areas covered under the scope of this RFP.
7	The proposed Solution should support automated patch management for critical security patch deployment on infra including Windows, Linux, MacOS.
8	The proposed solution should support patch evaluation in a test environment before distributing
9	The proposed solution should highlight missing critical patches and should re-attempt failed patches
10	The proposed solution should support mechanism to decline or delay an unnecessary patch that may cause any problem to overall IT infrastructure
11	The proposed solution should support remote patch management
12	The proposed solution should come along with standard reports and can generate the customized reports as per business requirement. The Patch Management solution should be capable of generating real-time reports on patches deployed, when, by whom, to which endpoints, etc.
13	The proposed solution should provide mechanism to centrally set/reset registry value in target Window machine.

14	The proposed solution should be able to provide the package/software deployment as option to centrally deploy in target window machines.
15	The proposed solution should have an option to define multiple deployment policies for deploying patches.
16	The proposed solution should show the system health based on missing patches.
17	The proposed solution should have an customisable dashboard for viewing information like vulnerable systems, missing patches, deployed patches, etc.
18	The proposed solution should able to deploy exe, msi/msp packages and scripts on end machines.
19	Proposed solution should have bundled reporting software so no third party tools would be required to customize reports
20	Proposed solution should be able to provide audit reports
21	Proposed solution should be capable of integrating with one or more Active Directory structures whenever required
22	Proposed solution should support virtualized environment
23	Proposed solution should provide easy to use inplace upgrade procedures for all components through the console
24	Proposed solution should be able to re-deploy the patch on a computer automatically if the initial deployment is not successful and even if the deployed patch is un-installed by the user
25	Proposed solution should support granular control over re-boot process after patch deployment like prompting user, allowing user to differ, rebooting immediately if no one has logged on, etc.
26	Proposed solution should come along with all operational technical manuals along with other related documents
27	Proposed solution should be able to provide patch deployment status monitoring
28	Proposed solution should allow console operators to spread the patch deployment over a pre-defined period of time to reduce overall impact to network bandwidth
29	Proposed solution should be capable of generating reports on patches deployed, when, by whom, to which endpoints, etc.)
30	In the proposed solution reports should be scheduled to be run and sent to administrators at specified times and intervals
31	All of the above features should be provided through the solution's endpoint agent from the same OEM only, without any dependency on any other OEM solution
32	The solution and it's data store should be virtual appliance and deployable on Linux operating systems to reduce the overall TCO

Backup Solution		
S.No	**Topic**	**Specification**
1	**Analyst Rating**	Backup software propsed should be in Gartner's leader quadrant for last five years in gartner Magic Quadrant report for Data Protection / Backup Software.

2	**Licensing**	The proposed Backup software must offer instance based licenses with no restrictions on type of arrays (protecting heterogenous storage technologies), front end production capacity or backup to disk target capacity restrictions. Licenses and associated hardware should be supplied for both primary and DR site.
3	**Reporting Capabilities**	It should provide a centralized dashboard which should give the overall backup score of the enviornment.
		Proposed solution should support 24x7 real-time monitoring, with at-a-glance and drill-down views of health, performance and workload of the virtual hosts.
		Proposed solution should have security and compliance dashboard inbuilt with the product.
		Proposed solution should support automated action for popular alarms (automated or semi-automated), with at-a-glance and drill-down views of health, performance and workload of the virtual hosts.
4	**Data Protection and Recovery in the cloud**	Software should be able to restore VMs to a cloud service provider like Azure and it should provide instant recovery to Azure.
		Software should be able to extend the backup repository to a public cloud service provider by moving older files to any S3 Compatible Object storage or Azure BLOB or AWS repositories.
		Backup software should should have capability to archive data to Amazon Galcier or Microsoft Azure storage Arhive Tier. The Software must have capability to restore the data from archive tier, it should not be dependent on cloud vendor.
		Backup software should support agentless backups of applications reisding in VMs like SQL, Exchange, Sharepoint, Oracle, etc. with non-staged granular recovery of all these applications. It should support crash consistent VM level backup for all other workloads. Backup software should support SAP HANA, MaxDB, MongoDB and DB2 Databases.
5	**Security &Compliance**	The proposed backup software should be installed on Linux operating system and should support backup server in High availability configuration.
		The Backup software should be in iso or ova format. Sofware should be Simple and should have Fast Deployment and should be Pre-Hardened with DISA-STIG script.
		Backup Security Features must be configured such as there should be no root privileges for the Backup server. The architecture should be based on Zero trust.
		The backup software must have YARA rules defined in the system.
		The proposed soloution should have on demand scans available for malaware attacks for windows and Linux system.
		The backup Software must have inline detection & in guest detection via guest indexing againgst any malware attacks.
		The proposed backup software must create a role in the backup server that if any user changes any configuration of backup server, it must be approved by that role and that role should have multi factor authentication.
		The proposed solution should come with pre-defined parameters and to make the backup server a hardened one to limit the attack surface. This security check should be able to run every day with a report being generated for review later
		The proposed solution should be capable of look for Indicators of Compromise (IoC) in protected machines and stop attacks by

		identifying known tools from hackers' toolkit and data exfiltration tools.
6	**Backup support for hypervisors and Applications**	Backup software should be a Hardware Agnostic software and it should support snapshot integration with hypervisors like VMware, Hyper-V, Nutanix AHV, Proxmox, OLKVM, Hyperscale and RHEV and support de-duplication on any storage target. It should be able to backup data to tapes (like LTO) as well for long term retention.
		The proposed backup software should provide Instant recoveries for any backup to Vmware, Hyper-V and Azure Virtual machine. It should also support the Instant VM recovery for AHV workloads as well.
		Backup software should support file level recovery from any backup of any VM or physical server. It should support a full system recovery in case of a system crash, either on a physical system or virtual machine or as a Cloud Instance(AWS, Azure or Google)
		The Proposed backup Software should supprot Syslog and Service Now integration.
		Backup software should support instant database recoveries of MS SQL and Oracle from the backup files.
		Backup software should support Multi factor authentication for accessing Backup console and console auto log-off functionality.
7	**RPO/ RTO and Recovery Assurance**	Backup software must have a feature of data validation, whereby a workload (VM with OS and application) is powered-on in a sandbox environment and tested for its recoverability.
		Recovery verification should automatically boot the server from backup and verify the recoverability of VM image, Guest OS and Application Consistency and then publish automated reports to be used in backup / recovery audits.
		Backup software should provide Backup and Replication capabilities in one console only and also allow users to integrate with RBAC capabilities of the backup server.
		Proposed backup software should be able to Hardened the Linux Repository. This service will prevent backup copies of data from any corruption or ransomware attacks.
		The proposed backup should have object storage backup directly to tape.
		Proposed backup software should have the ability to perform staged restores to enable admins to comply to regulations by selectively deleting files / records which should not be restored from the backup copies. This will help in complying to "right to be forgotten"regulations like GDPR, where user data is deleted from restored backup copies in an auditable manner.
		Backup software should support instant file share recovery in NAS storages to allow users to access files fast after disaster.
8	**Backup and Replication Performance and SLA**	The proposed Backup software must allow to configure the maximum acceptable I/O latency level for production data stores to ensure backup and replication activities do not impact storage Availability to production workloads.
		The software should be Network-efficient, Secure backup data replication with variable-length encryption at the source, along with compression and encryption to ensure that backups are optimized for WAN transmission. This should be ensured with or without need of any other 3rd party WAN Accelerator requirements.

9	**Disaster Recovery Capabilities**	Replication in the software should be a VM level replication and must replicate the VM level data with or without backing it up at the source site. It should also include failover and failback capabilities and should be able to perform automatic acquisition of network addresses at the destination site.
		The Proposed solution should support Continous replication at VM level. The RPO must be less than 5 Seconds and it must deliver Application consistency.
		Backup and replication software must deliver maximum investment protection by supporting replication of workloads between dis-similar systems like hyperconverged infrastructure to stand alone servers and storage running similar hypervisors across sites, thereby creating a Disaster recovery environment for production workloads irrespective of the underlying hardware.
		Backup software should have ability to backup data from one server platform and restore it to another server platform to eliminate dependence on a particular machine and for disaster recovery purposes. This bare metal recovery capability should be built in for the physical servers and should even work on the dissimilar hardware.
		Backup software should have the ability to backing up a Cloud VM running in AWS or Azure and restore it as a valid VM workload back onto a Vmware server farm or other platformas.

Email Security	
S.No.	**Technical Requirements**
A	**General Platform Features**
1	The proposed Email Security Platform shall enhance cybersecurity posture by implementing a unified, AI-driven platform with the following functionalities from Day 1:
	1. Advanced Threat Detection and Phishing Protection using AI/ML.
	2. Behavioral and Intent-based Analysis for detecting Business Email Compromise (BEC).
	3. Automated Phishing Remediation and Message Recall.
	4. Cloud-native API Integration with Microsoft 365 and Google Workspace.
	5. Must have an AI based SPAM filtering mechanism
	6. Threat Intelligence Crowdsourcing for real-time updates.
	7. User Awareness Training and Reporting Tools (e.g., “Report Phish” button).
	8. Zero Trust Access to ensure secure user and admin interactions.
2	The solution shall include the following components with active licensing from Day 1:
	a) Advanced Phishing Protection
	b) AI/ML-based Threat Detection Engine with adaptive self-learning.
	c) Automated Incident Response and Remediation workflows.
	e) API and SIEM Integration (Splunk, Sentinel, QRadar, etc.).
3	The proposed Email Security platform OEM shall be recognized in the Gartner Market Guide for Email Security 2024 or later.

Network Attached Storage		
S.No.	**Parameter**	**Specifications**
1	Form Factor/Mounting	3U/4U, 19” Rack Mounted
2	No. of Controllers per appliance	Minimum 2 nos.
3	Network Connectivity Per Controller	4x 1GbE + 2x 10GBASE-T (Total: 8x 1GbE + 4 x 10GBASE-T with two controllers)
4	Capacity Expansion	Should support 12 or higher JBOD's/Expansion Units or should have minimum 208 HDDs or better support in a single stack
5	Storage Expansion Port per Controller	1 x 12Gb SAS Mini-SAS (SFF-8644)
6	Supported Network Protocols	SMB/CIFS, NFS, FTP, WebDAV etc.
7	Drive Support and Type	16# 3.5" Drives per enclosure
		SAS/NL-SAS/SATA HDD, 7200 RPM or higher
		Supports mix of SAS and SATA drives in the same enclosure
8	Cache/Memory	32 GB per Controller and upgradable to 64 GB per controller
9	Storage Capacity along with expansion using JBODs	30TB usable capacity in a single stack after RAID5 + hot-spare configuration
10	Management Port per Controller	1 x RJ-45 1GbE Ethernet and 1 x Serial Port
11	Green Features	Should support MAID technology to reduces power consumptions and increases the longevity of disk drives
		Efficient 80 Plus Compliant Power Supply
12	Supported OS	Windows Server 2008 or higher, Mac OS X 10.x, Linux (RHEL 6.5 or higher and SLES 11 or higher)
13	Power Supply	Should support Redundant Power Supply
14	RAID configuration	0, 1 , 5, 6, 10, 50, 60
15	Hot Spare Disk	It shall provide at least one hot spare disk per appliance/enclosure
16	General Features	Should support data migration to healthy drive if find un-healthy disk member in array before the disk drive fails.
		Should support remapping of bad sector of disk and SMART error handling
		Should support Asynchronous & scheduled Backup and Cloning of Share & Volume for data backup and recovery

		Should support Write Once Read Many (WORM) feature
		Should support logging of NVRAM error
		Surveillance Buffer Management support and benefit for more cameras supported, Less Frame Drop and Sequential Pattern Recording.
		Should support for Cloud Backup
		The storage system shall come standard with Advanced Battery Flash Backup design.
17	Working Temperature & Humidity	Temperature: 5° to 35°C, Humidity: 20% to 80% (Non-Condensing)
18	Warranty/Replacement	Three(3) years warranty/replacement from OEM for appliance including SAS/NL-SAS HDDs
19	Certifications / Regulatory compliance	BIS

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 ********