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/2024-25/IT services to RCIL customer/17 dated 11.10.24

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/2024-25/IT services to RCIL customer/17 dated 11.10.24

RailTel Corporation of India Ltd., (here after referred to as RailTel) invites EOIs from RailTel's Empanelled 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	16-10-2024 before15:00Hrs.
Opening of bidder EOIs	16-10-2024 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 empanelled partners of RailTel. Only RailTel empanelled 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 Security Solution on lease model initially for 1 year period for RailTel's Customer as per Schedule of Requirements (SoR) Annexure-04. Technical Specification is provided under Annexure-05.

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, preparation of 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 no case 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. Indicative payment terms: 40%advance payment on issue of PO from RailTel. Remaining 60% payment in equal installments on quarterly basis over 1 year period.

7.2. Actual payment terms shall be as per agreement between RailTel and Customer and shall be confirmed at the time of PO issuance.

7.3. 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.

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

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

8. Delivery Schedule: Supply of hardware & software items shall be within 3-4 weeks of issue of PO. Installation & commissioning of hardware & software items shall be within 6-8 weeks of issue of PO

9. Compliance requirements

9.1. The interested partner should be an Empanelled 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 of Rs 30.84 Cr crores during the last 3 financial years. Bidder should submit audited balance sheets and certificate of CA 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 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/Support & Maintenance of Data centre Infra project during last seven years from any government organization as per following details:

i) Three similar works each with value costing not less than ₹6.16 Cr (Incl. GST))
ii) Two similar works each with value costing not less than ₹8.22 Cr (Incl. GST))
iii) One similar work with value costing not less than ₹12.33 Cr (Incl. GST))

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

10. 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 Annexure-04 (SOR).

11. 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.

12. Integrity Pact (IP) Program

12.1. RailTel has adopted Integrity Pact Program and for implementation thereof all EOI/RFPs relating to procurement of OFC, quad cable, pre-fab shelters, electronic equipment and its installation and/or commissioning etc and other item(s) or activity/activities proposed to be carried out or required by the Company for the value ex-ceding Rs. 15 crores at a time including for repair and maintenance of cable/network and any other items required for special works assigned to RailTel will be covered under the Integrity Pact Program and the vendors are required to sign the IP document and submit the same to RailTel before or along with the bids.

12.2. Only those vendors who have purchased the EOI/RFP document and signed the IP document can send their grievances, if any, to the Independent External Monitors (IEMs) and the nodal officer, i.e. Chief Vigilance Officer (CVO), RailTel.

Name of IEMs and contact details:

1.	Mrs. Vinit Kumar Jayaswal	E-Mail: gkvinit@gmail.com
2.	Sh. Punati Sridhar	E-mail: poonatis@gmail.com

Name & Contact details of Nodal Officer (IP) in RailTel:

Chief Vigilance Officer
RailTel Corporation of India Ltd.
Plate-A, 6th Floor, Office Block Tower-2,
East Kidwai Nagar, New Delhi - 110023
e-mail: cvo[at]railtelindia[dot]com

12.3. If the order, with total value equal to or more than the threshold value, is split to more than one vendor and even if the value of PO placed on any/each vendor(s) is less than the threshold value, IP document having been signed by the vendors at bid stage it- self, the Pact shall continue to be applicable.

12.4. Bidder of Indian origin shall submit the Integrity Pact (in 2 copies) on a non-judicial stamp paper of Rs. 100/- or the appropriate value (as the case may be), duly signed by the person signing the bid. If the bidder is a partnership or a consortium, the Integrity Pact shall be signed by all the partners or consortium members.

12.5. Bidder of foreign origin may submit the Integrity Pact on its company's letterhead, duly signed by the person signing the bid.

12.6. The 'Integrity Pact' shall be submitted by the Bidder duly signed in all pages along with the Bid. Bid received without signed copy of the Integrity Pact document will be liable to be rejected. Format of Integrity Pact is enclosed in this Tender document.

12.7. One copy of the Integrity Pact shall be retained by RailTel and the 2nd copy will be issued to the representative of the bidders during bid opening. If the Bidder's representative is not present during the Bid opening, the 2nd copy shall be sent to the bidder by post/courier.

12.8. The Integrity Pact is applicable in this EOI/RFP vide CVC circular no. 10/05/09 dt. 18.05.09 and revised guideline of CVC circular no. 015/VGL/091 dt. 13.01.17 or the latest updated from time to time shall be followed.

12.9. Interested may also refer the URL for IP Program : https://www.railtel.in/tenders/integrity-pact.html

13. Technical Specification Compliance

Bidder should submit compliance to Technical specification as provided under Annexure-05 and submit along with the bids. Bids without technical specification compliance shall not be considered.

14. 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
7. Integrity pact
8. Technical Specification compliance
9. Documents with respect to compliance requirement clause (9.1 to 9.10).
10. Deviation statement (if any) as per clause number 24.

15. 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.

16. 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.

17. 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.

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

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

17.3. 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.

17.4. 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.

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

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

18. Earnest Money Deposit (EMD)/ Bid Security

18.1. 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.

18.2. 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.

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

18.4. 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.

18.5. 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 14.

18.6. Earnest Money will bear no interest.

19. 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.

20. Late Bids

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

21. 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.

22. 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.

23. 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			

24. 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)

25. 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. Tentative contract period is 1 year. The contract duration can be renewed / extended by RailTel at its discretion, 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.

26. 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.

27.Rate Contract

In case of additional requirement of similar services under SOR for same customer project, RailTel may place additional PO/ Sub PO to selected bidder with same commercials and terms & conditions under Rate contract for upto maximum 50% of contract value.

28. 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.

29. Suspension, Revocation or Termination of Contract / Agreement

29.1. 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.

29.2. 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.

30. Dispute Settlement

30.1. 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.

30.2. 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..

30.3. All arbitration proceedings shall be conducted in English.

31. 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.

32. Statutory Compliance

32.1. 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.

32.2. 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.

33. 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.

34. 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.

35. Force Majeure

35.1. 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.

35.2. 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.

36. Indemnity

36.1. 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.

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

37. Limitation of Liability towards RailTel

37.1. 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.

37.2. 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.

38. Confidentiality cum Non-disclosure

38.1. 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.

38.2. 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.

38.3. 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.

38.4. 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.

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

39. 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.

40. 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.

41. 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.

Format for COVERING LETTER

COVERING LETTER (To be on company letter head)

EoI Reference No: **RCIL/EOI/CO/ITB/2024-25/IT services to RCIL customer/17 dated 11.10.24**

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/2024-25/IT services to RCIL customer/17 dated 11.10.24
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/2024-25/IT services to RCIL customer/17 dated 11.10.24

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 Authorised Signatory

Name
Designation

Annexure – 03

PROFORMA FOR SIGNING THE INTEGRITY PACT

(On Stamp paper of Appropriate Value)

RailTel Corporation of India Limited, hereinafter referred to as "The Principal".

And

……., hereinafter referred to as "The Bidder/ Contractor"

Preamble

The Principal intends to award, under laid down organizational procedures, contract/s for …….. . The Principal values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fair- ness/transparency in its relations with its Bidder(s) and /or Contractor(s).

In order to achieve these goals, the Principal will appoint an Independent External Monitor (IEM), who will monitor the EOI/RFP process and the execution of the contract for compliance with the principles mentioned above.

Section 1- Commitments of the Principal

1. The Principal commits itself to take all measures necessary to prevent corruption and to observe the following principles:-

a. No employee of the Principal, personally or through family members, will in connection with the EOI/RFP for, or the execution of a contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.

b. The Principal will during the EOI/RFP process treat all Bidder(s) with equity and reason.

The Principal will in particular, before and during the EOI/RFP process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential/additional information through which the Bidder(s) could obtain an advantage in relation to the process or the contract execution.

c. The Principal will exclude from the process all known prejudiced persons.

2. If the Principal obtains information on the conduct of any of its employees which is a criminal offence under the IPC/PC Act, or if there be a substantive suspicion in this regard, the Principal will inform the Chief Vigilance Officer and in addition can initiate disciplinary actions.

Section 2- Commitments of the Bidder(s) /Contractor(s)

1. The Bidder(s)/Contractor(s) commit himself to take all measures necessary to prevent corruption. He commits himself to observe the following principles during his participation in the EOI/RFP process and during the contract execution.

a. The Bidder(s)/contractor(s) will not, directly or through any other persons or firm, offer promise or give to any of the Principal's employees involved in the EOI/RFP process or the execution of the contract or to any third person any material or other benefit which he/she is not legally entitled to, in order to obtain in exchange any ad- vantage during EOI/RFP process or during the execution of the contract.

b. The Bidder(s)/Contractor(s) will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process.

c. The Bidder(s)/Contractor(s) will not commit any offence under the relevant IPC/PC Act; further the Bidder(s) /Contractors will not use improperly, for purposes of com- petition or personal gain, or pass on to others, any information or document provided by the Principal as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.

d. The Bidder(s)/Contractor(s) of foreign origin shall disclose the name and address of the Agents/representatives in India, if any. Similarly, the bidder(s)/contractor(s) of Indian Nationality shall furnish the name and address of the foreign principals, if any.

e. The Bidder(s)/Contractor(s) will, when presenting his bid, disclose any and all payments he

has made, is committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the contract. Further, details as mentioned in the "Guidelines on Indian Agent of Foreign Suppliers" shall be disclosed by the Bidder(s) / Contractor(s). Further, as mentioned in the Guidelines all the payments made to the Indian agent / representative have to be in Indian Rupees only. Copy of the "Guidelines on Indian Agents of Foreign Suppliers" as annexed and marked as Annexure-A.

2. The Bidder(s)/Contractor(s) will not instigate third persons to commit offences outlined above or be an accessory to such offences.

Section 3: Disqualification from EOI/RFP process and exclusion from future contracts

If the Bidder(s)/Contractor(s), before award or during execution has committed a transgression through a violation of Section 2, above or in any other form such as to put his reliability or credibility in question, the Principal is entitled to disqualify the Bidder(s)/Contractor(s) from the EOI/RFP process or take action as per the procedure mentioned in the "Guidelines on banning of business dealings". Copy of the "Guidelines on Banning of Business Dealings" is annexed and marked as Annexure-B.

Section 4: Compensation for Damages

1. If the Principal has disqualified the Bidder(s) from the EOI/RFP process prior to the award according to Section 3, the Principal is entitled to demand and recover the damages equivalent to Earnest Money Deposit/Bid Security.

2. If the Principal has terminated the contract according to Section 3, or if the Principal is entitled to be terminated the contract according to Section 3, the Principal shall be en-titled to demand and recover from the Contractor liquidated damages of the Contract value or the amount equivalent to Performance Bank Guarantee.

Section 5: Previous Transgression

1. The Bidder declares that no previous transgressions occurred in the last three years with any other company in any country conforming to the anti-corruption approach or with any other public sector enterprise in India that could justify his exclusion from the EOI/RFP process.

2. If the bidder makes incorrect statement on this subject, he can be disqualified from the EOI/RFP process for action can be taken as per the procedure mentioned in "Guidelines on Banning of business dealings".

Section 6: Equal treatment of all Bidders/ Contractors/Subcontractors

1. The Bidder(s)/Contractor(s) undertake(s) to demand from all subcontractors a commitment in conformity with this Integrity Pact, and to submit it to the Principal before contract signing.

2. The Principal will enter into agreements with identical conditions as this one with all bidders, contractors and subcontractors.

3. The Principal will disqualify from the EOI/RFP process all bidders who do not sign this Pact or violate its provisions.

Section 7: Criminal charges against violation by Bidder(s) / Contractor(s) / Sub Contractor(s)

If the Principal obtains knowledge of conduct of a Bidder, Contractor or Subcontractor, or of an employee or a representative or an associate of a Bidder, Contractor or Subcontractor which constitutes corruption, or if the Principal has substantive suspicion in this regard, the Principal will inform the same to the Chief Vigilance Officer.

Section 8: Independent External Monitor / Monitors

1. The Principal appoints competent and credible Independent External Monitor for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.

2. The Monitor is not subject to instructions by the representatives of the parties and per- forms his functions neutrally and independently. He reports to the CMD, RailTel.

3. The Bidder(s)/Contractor(s) accepts that the Monitor has the right to access without restriction

to all project documentation of the Principal including that provided by the Con- tractor. The Contractor will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor is under contractual obligation to treat the information and documents of the Bidder(s)/ Contractor(s)/Subcontractor(s) with confidentiality.

4. The Principal will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the Principal and the Contractor. The parties offer to the Monitor the option to participate in such meetings.

5. As soon as the Monitor notices, or believes to notice, a violation of this agreement, he will so inform the Management of the Principal and request the Management to discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.

6. The Monitor will submit a written report to the CMD, RailTel within 8 to 10 weeks from the date of reference or intimation to him by the Principal and, should the occasion arise, submit proposals for correcting problematic situations.

7. Monitor shall be entitled to compensation on the same terms as being extended to provided to Independent Directors on the RailTel Board.

8. If the Monitor has reported to the CMD, RailTel, a substantiated suspicion of an offence under relevant IPC/PC Act, and the CMD, RailTel has not, within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.

9. The word 'Monitor' would include both singular and plural.

Section 9: Pact Duration

This pact begins when both parties have legally signed it. It expires for the Contractor 10 months

after the last payment under the contract, and for all other Bidders 6 months after the contract has been awarded.

If any claim is made / lodged by either party during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged / determined by CMD of RailTel.

Section 10: Other Provisions

1. This agreement is subject to Indian Law, Place of performance and jurisdiction is the Registered Office of the Principal, i.e. New Delhi.

2. Changes and supplements as well as termination notices need to be made in writing.

3. If the Contractor is a partnership or a consortium, this agreement must be signed by all partners or consortium members.

4. Should one or several provisions of this agreement turn out to be invalid, the remainder of this agreement remains valid. In this case, the parties will strive to come to an agreement to their original intentions.

(For & On behalf of the Principal)
(Office Seal)

Place ——————
Date ——————

(For & On behalf of Bidder/Contractor)
(Office Seal)

Place ——————
Date ——————

Witness 1: _____

(Name & Address) _____

Witness 2: _____

(Name & Address) _____

Annexure-04

Schedule of Rates

Security as a Managed Service model (All solutions shall be dedicated On-Premises and should be scalable)							
SN	**Item Description**	**Qty.**	**Unit**	**Rate per Unit (annual recurring charges)**	**Total Rate**	**GST**	**Torat Rate with Tax(annual recurring charges)**
1	NexGen Firewall for MPLS-VPN and ILL (IPS, Anti-APT, URL Filtering, IP Filtering, Anti-bot etc.). NOTE: 1. Overall firewall throughput should be 25 Gbps along with management console in DC 2. In DR Overall firewall throughput should be 10 Gbps along with management console. (4 at DC and 4 at DR)	8	Number				
2	NexGen Firewall for NDC (both MPLS and ILL) with overall firewall throughput of 10 Gbps with NexGen capabilities of IPS, Anti-APT, URL Filtering, IP Filtering, Anti-bot etc.	4	Number				
3	Client/SSL VPN (Software based)	150	Number				
4	Web Application Firewall along with DDoS protection Overall throughput should be 10 Gbps. (2 at Dc and 2 at DR)	4	Number				
5	Server Security Solution, along with management console (On-Premises solution) at DC	200	Number				
6	NBAD	1	Number				
7	HSM (Hardware) at DC	2	Number				
8	SIEM: Security Information and Event Management (Central Log Management with Analytics) with SOAR, Day 1, EPS 10,000 scalable upto 25,000 EPS and integration of additional log sources as needed. (at DC)	1	Number				
9	Database Activity Monitoring Solution (7 nodes at DC and 4 Nodes at DR)	11	Nodes				
10	Privilege Access Management	50	Users				
11	Training of Selected RailTel Customer official wrt Security Operations using the above-mentioned tools . (officials should be trained twice a year.)	5	Users				

12	IT Support Engineer (L2) (Man month Charges)	144	Man month				
13	Support for Infrastructure for software based solutions	1	LS				
SOR Total (ARC) including tax							

SN	Item Description	Qty.	Unit	Rate per Unit (One time Cost)	Total Rate	GST	Torat Rate with Tax (One time cost)
17	One Time Cost for installation and commissioning for security Infrastructure on Lease	1	LS				
18	One Time Cost for Cable and other accessories	1	LS				

SOR Total (ARC + OTC) including tax	

SOR Total (ARC + OTC) including tax in words :	

Annexure-05

Technical Specification compliance

Firewall (SN-1)

SN	Specifications	Comply (Yes/No)
1	Proposed solution must be dedicated purpose built firewall device which enables the convergence of high performing networking and security across the Security Platform. Solution must deliver consistent and context-aware security posture across network with integrated IPS, application visibility and control, Web security, content security and malware control. All the mentioned features must be quoted as part of overall solution.	
2	Must have 16X GE RJ45, 4X GE SFP, 4x 10 GE SFP+, 2X 25GE SFP28 and dedicated RJ45 Management from Day1. All required transceivers should be populated from day one.	
3	Threat prevention throughput of 20 Gbps in real world/production/enterprise mix environment with all the security engines like IPS, Application control, anti-malware enabled.	
4	SSL VPN throughput of at least 9 Gbps. Should support client based VPN and at least 8000 concurrent SSL VPN users from day 1.	
5	Concurrent connection of 15 million or above and new connection / Sec of 700K or above.	
6	The solution should have 15 Gbps or more of SSL Inspection throughput with 1.5 Million or more concurrent HTTPS session.	
7	The solution should have 25 Gbps of IPS throughput.	
8	IPSEC VPN throughput of at least 50 Gbps or more with support for 2000 Site to Site IPSec tunnels.	
9	The solution should have redundant/dual power supply and should be rack mountable. All required parts and accessories to be included from Day 1.	
10	The proposed solution should support HA in Active/Active and Active/Passive mode. The Firewall in HA should support stateful clustering across sites. HA should be supported on both IPV4 and IPV6. Feature like IPS, Anti malware, Web filtering, DDOS prevention and Traffic Shaping should be available in Active-Active.	
11	Must support NAT (SNAT and DNAT) with following modes Static, Dynamic, PAT, Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4), Nat46 (IPv4- to-IPv6) , DNS64 & DHCPv6 functionality.	
12	Firewall appliance must have at least 10 virtual firewall/domains/instances (active from day-1) with each virtual firewall/domains/instances having a separate administrative control OR equivalent, Security zones and VLAN. Associated Licenses, Software and Hardware towards Virtual domains / Virtual Firewalls/ Virtual instances shall be provided from day 1	
13	The following features must be available in each virtual firewall domain/instant context environment: Firewall, IPSEC and SSL VPN, IPS, Web and Application Control, Anti-Malware, Traffic Shaping & policy based routing, DDOS, User and Group management, Logging and Reporting.	
14	The Firewall solution should support Static Routing, Policy based Routing, BGP, OSPF, VXLAN Inspection.	
15	Must support DNS client and NTP client. Firewall should also have capability to be configured as DNS server for the LAN/segments/zones.	
16	The firewall must have the capability to create DOS prevention policy to prevent against DOS attacks on per zone basis (outbound to inbound, inbound to outbound) and ability to create and define DOS policy based on attacks like UDP Flood, ICMP Flood, SYN Flood, IP Address Sweeps, IP Address Spoofs, port scan, Ping of Death, Teardrop attacks, unknown protocol protection etc.	
17	Should be able to call 3rd party threat intelligence data on malicious IPs, URLs and Domains to the same firewall policy to block those malicious attributes and list should get updated dynamically with latest data.	

18	Solution providing real-time monitoring, event logs collection, policy enforcement over a GUI interface on HTTPS or equivalent secure mechanism. Management of the appliances must also be available using SSH and direct console access.	
19	The bidder should provide a central & dedicated logging & reporting appliance to be deployed with solution. The log & reporting server should support minimum 3 months of active logs	
20	Solution can be dedicated hardware appliance or VM. If VM is provided necessary licenses and hardware server to be provided by bidder.	
21	Should allow the report to be exported into other formats such as PDF, HTML, CSV/XML etc.	
22	The Firewall should support integration of on-prem sandbox of same OEM in future.	
23	Firewall configuration changes / commands issued must be logged. Also provision for exporting to external syslog solution.	
24	Solution should conform to EN 55032:2015 /EN 55035: 2017/EN 300 328/IEC 62368-1.	
25	Should be USGv6/IPv6 certified.	
26	The solution should be quoted with support for all necessary licenses for IPS, Advanced Malware Protection, Application Control, URL, DNS Filtering & Antispam signatures. The support should include hardware warranty and technical support from OEM.	
27	The OEM of the offered products must have a valid ISO 9001:2015 and ISO27001. Certificate from OEM should be attached with the technical bid.	
28	The Proposed solution should be among the leaders in Gartner Magic Quadrant for Network Firewalls in the latest Gartner report.	
29	The OEM should not have been blacklisted/debarred by Central/State/PSU or any government body in last 3 years.	

Firewall (SN-2)

SN	**Specifications**	**Comply (Yes/No)**
1	Porposed solution must be dedicated purpose built firewall device which enables the convergence of high performing networking and security across the Security Platform. Solution must deliver consistent and context-aware security posture across network with integrated IPS, application visibility and control, Web security, content security and malware control. All the mentioned features must be quoted as part of overall solution.	
2	Must support NAT (SNAT and DNAT) with following modes Static, Dynamic, PAT, Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4), Nat46 (IPv4- to-IPv6) , DNS64 & DHCPv6 functionality.	
3	The Firewall solution should support Static Routing, Policy based Routing, BGP, OSPF, VXLAN Inspection.	
4	Must support DNS client and NTP client. Firewall should also have capability to be configured as DNS server for the LAN/segments/zones.	
5	The firewall must have the capability to create DOS prevention policy to prevent against DOS attacks on per zone basis (outbound to inbound, inbound to outbound) and ability to create and define DOS policy based on attacks like UDP Flood, ICMP Flood, SYN Flood, IP Address Sweeps, IP Address Spoofs, port scan, Ping of Death, Teardrop attacks, unknown protocol protection etc.	
6	Should be able to call 3rd party threat intelligence data on malicious IPs, URLs and Domains to the same firewall policy to block those malicious attributes and list should get updated dynamically with latest data.	
7	Solution providing real-time monitoring, event logs collection, policy enforcement over a GUI interface on HTTPS or equivalent secure mechanism. Management of the appliances must also be available using SSH and direct console access.	
8	The bidder should provide a central & dedicated logging & reporting appliance to be deployed with solution. The log & reporting server should support minimum 3 months of active logs	
9	Solution can be dedicated hardware appliance or VM. If VM is provided necessary licenses and hardware server to be provided by bidder.	
10	Should allow the report to be exported into other formats such as PDF, HTML, CSV/XML etc.	

11	Firewall configuration changes / commands issued must be logged. Also provision for exporting to external syslog solution.	
12	The solution should be quoted with support for all necessary licenses for IPS, Advanced Malware Protection, Application Control, URL, DNS Filtering & Antispam signatures. The support should include hardware warranty and technical support from OEM.	
13	The OEM of the offered products must have a valid ISO 9001:2015 and ISO27001. Certificate from OEM should be attached with the technical bid.	
14	The Proposed solution should be among the leaders in Gartner Magic Quadrant for Network Firewalls in the latest Gartner report.	
15	The OEM should not have been blacklisted/debarred by Central/State/PSU or any government body in last 3 years.	

Privilege Access Management

SN	Technical Specification	Compliance (Yes/No)
1	Proposed PAM solution should have capability of multitenancy so that the same can be offered "as a service" to other customers.	
2	The proposed solution architecture support spanning multiple data centres across on-prem and private cloud resources	
3	The proposed solution should support on-prem implementation for 200 users and there will be no restriction on no. of devices. Bidder needs to supply all necessary license including Microsoft RDS CAL, OS licenses, DB licenses etc. for providing it as a solution	
4	The proposed solution should have password vaulting technology to secure Privilege credentials with multi-encryption techniques (AES-256)	
5	The proposed solution should be FIPS 140-2, ISO/IEC 27002 compliant	
6	The proposed solution should be 100% agent less solution for password and session management. There should not be a need to install agents on target devices.	
7	The proposed solution must include components to distribute workloads across an environment.	
8	The proposed solution should support Ad Hoc Just-in-Time Access to servers. Only permit access when it is requested and granted, which should be governed by workflows and policies.	
9	The proposed solution should allow users/admins to use their native client like RDP and Putty to connect target machines onboarded in PAM.	
10	The proposed solution should support complete active configuration at all infrastructure components. It should support high availability Vault environment since this is crucial for the Vault availability	
11	The proposed solution should support Disaster Recovery Site so that should be able to continue functioning without losing any data as a result of the failure	
12	The proposed OEM solution should have capability for securing endpoints, securing cloud, workforce lifecycle management, securing devops, etc as a pre-integrated but loosely coupled solution for easy administration from future projects around identity security	
13	The proposed solution should provide Scan utility which should scan our on-prem infrastructure and provides the report with the list of all the privilege accounts and SSH keys at our environment. Also, it should tell about compliance status for each account.	
14	The proposed solution should support scheduled automatic scanning to identify newly created accounts.	
15	The proposed solution should support automatic onboarding for newly created admin account.	

16	The proposed solution should be able to discover and detect windows dependencies like Windows Scheduled accounts, Scheduled tasks accounts, IIS Application pool accounts and automatically onboard them in the vault	
17	The proposed solution should be able to onboard credentials from INI file, XML file, database string, etc. in the vault.	
18	The proposed solution should be able to manage the passwords of privilege accounts for below target devices: - - OS accounts (all Flavors) - Windows local and domain account - Unix admin accounts and SSH keys - Databases (with clients like Toad, SQL Plus, SQL Server Management Studio and more) - Network and Security devices - Admin web console for applications - Cloud resources - Cloud console and access keys - VM infrastructure and ESXi	
19	The proposed solution should perform the session recordings and keystrokes capture for all above devices to monitor the privilege activities	
20	The proposed solution should provide high compression ratio to ensure that session recordings will not utilize huge storage	
21	The proposed solution should support session recordings that are searchable on the basis of time frame, username, IP address, hostname and as well as with executed commands and events	
22	The proposed solution should capability of Risky keystrokes or command to be blocked so that no one can able to execute those keystrokes.	
23	The proposed solution should support Time and IP based restriction for users/admins to log into PAM	
24	The proposed solution should support approval workflow	
25	The proposed solution should support One time password and Exclusive access feature for check in/out the passwords	
26	The proposed solution should have User Based Analytics so that it can trigger a real-time alert in case of any unusual behaviour of user or anomalous activities like alert in case any admin tries to access target machine during irregular hours, irregular IP, Dormant user, Anomalous access to multiple machines, unusual geographical region etc	
27	The proposed solution must support a smooth upgrade process and be performed without any additional cost to RailTel.	
28	The proposed solution must run on the latest and fully patched version of Operating System at all times.	
29	The proposed solution's Active Directory and LDAP based Integration must allow for a configurable synchronization schedule to automate onboarding new users	
30	The proposed solution should be able to automatic onboard newly created accounts immediately and trigger password change.	
31	The proposed solution must raise immediate alert in case of suspicious password change, like request to change or reset a password after bypassing the Password Manager. Automatic Remediation by rotating credentials.	
32	The proposed solution must support masking available login domains during the login process from the user	

33	The proposed solution must able to identify unconstrained delegation Accounts (unconstrained delegation are accounts that are granted permissive delegation privileges and thereby expose the domain to a high risk.)	
34	The proposed solution must have separate dashboard for the events and alerts related to threat analytics	
35	The proposed solution must have capability to forward Threat Analytics alerts and notification over email and SIEM solution like ArcSight etc.	
36	The proposed solution should support Just-In-Time provisioning	
37	The proposed solution should support Password less authentication	
38	The proposed solution should support Bio-metric authentication	
39	The proposed solution must support a custom informational banner at the login screen without CSS modifications.	
40	The proposed solution provides MFA not only for PAM consoles but for other applications as well	
41	The proposed solution should support MFA that can be utilized for endpoints and laptop security and authentication	
42	The proposed solution should provide SSO feature for users to onboard and access multiple applications	
43	The proposed solution should be able to manage the passwords for local admin account for endpoints such as laptop, workstations etc.	
44	The proposed solution should provide out of box Operations reports which should contain information about the information stored in Vault and users, and the operational connections between them	
45	The proposed solution should provide out of box Audit/compliance reports which should contain information that enable to track vault activities and, specifically, password use in order to meet audit requirements	
46	The proposed solution should provide out of box reports for audit and compliance like: - - Inventory report - Activity report - Compliance report - User list report	
47	The proposed solution should provide reports to track PAM component utilization, compliance status of managed credentials, and license utilization for deployments and more.	
48	The proposed solution should support integration with SIEM (ArcSight etc.), LDAP, SMTP, SNMP etc.	
49	The proposed solution must include a tamper-proof, robust, audit of all activities within and against the platform.	
50	The Behaviour Analytics platform must provide a rich set of informative dashboards include top users, top accounts, IP address mapping, alerts, etc	
51	The proposed solution must support terminating an active user session	
52	The proposed solutions account discovery function must provide out-ofthe-box support for Active Directory Accounts, Windows Accounts, Linux Accounts, Unix Accounts, Hypervisor Accounts.	
53	The proposed solution must provide workflow and policy management for the request, provisioning and decommissioning of discovered and newly created service accounts.	

54	The Behaviour Analytics platform must provide a watchlist for newly onboard users and existing users whose activity may be suspicious.	
55	The Behaviour Analytics platform must provide an indefinite audit trail of activity within the platform.	
56	The Behaviour Analytics platform must provide an access graph interface to visualize communities of users who access similar accounts.	
57	The Behaviour Analytics platform must provide an access IP map interface to visualize anomalous behaviour on a world map overlay GUI.	
58	The Behaviour Analytics platform must provide an overview of users with active mobile-cached accounts.	
59	The proposed solution's account discovery function must support rules to automate onboarding of all discovered accounts.	
60	The solution must provide a single-pane of glass interface for all access and configurations for all functions, e.g., administration, auditing, reporting, vaulting, access policies, privileged sessions, discovery, and API	
61	The solution should provide custom terminal banners after a successful login with available commands to be displayed.	
62	Bidder must provide support for the features required in implementing use cases which is available in proposed solution.	
63	Bidder has to submit the technical solution document including design, architecture, flow, virtual machine requirement, software's, license, OS etc. RailTel shall provide required virtual machines at DC and DR to deploy the solution however bidder has to provide all software's, licenses, Operating Systems etc. required to implement the proposed PAM Solution at both DC and DR without any additional cost to RailTel.	
64	Bidder has to provide Installation, configuration, Management Training and OEM certification (medium level) of at least 10 employees of RailTel.	
65	RailTel may ask to showcase (PoC) for all the above features to comply with technical specs asked if required.	

Database Activity Monitoring Solution

SN	Specification Required	Compliance Yes / No
1	The solution proposed should be an Intelligent Next Generation SIEM and must be able to detect any anomalies, report in real time and take action as programmed having SIEM, UBA and SOAR capabilities accessible within single User Interface.	
2	The SIEM solution should be software based with a clear logical and physical separation of the collection module, logging module and correlation module.	
3	The SIEM Solution should be EPS based at both log management and Correlation layer and must support logs from unlimited devices or sources	
4	The SIEM solution support high availability feature and should be proposed in HA mode for all layers at DC	
5	The SIEM Solution should support security data lake concept for future scalability and expansion perspective.	
6	The proposed solution must provide inline options to reduce event data at the source by filtering out unnecessary event data. Filtering must be simple string-based or regular expressions and must delete the event data before it is processed. Log Filtering needs to be available across all tier to filter out logs as wherever required.	

7	SIEM solution should be based on open architecture so that it can be used to feed data to 3rd party analytic solutions i.e. Solution should support standard CEF or equivalent technology which is accepted globally not the proprietary one.	
8	Proposed SIEM solution must have atleast 3 deployments for more than 100K EPS in Govt of India organizations. (Atleast 3 sign-off copies must be provided for more than 100K EPS from any Government of India organizations)	
9	Proposed solution's OEM must have its presence in India including development center and support centre.	
10	**Log Management - Collection, Compliance, Forensics, Integrations, Reporting & Searching and Storage**	
11	Solution must be agentless and should not require any agents to integrate with end devices	
12	SIEM solution must support OOB of the box integration with well known technologies e.g. firewall, AD, Switches, routers, TI etc. for creating response to an incidence	
13	The solution should have connectors to support the listed devices / applications. In case device is not supported out of box it must have GUI Based SDK kit to create Parsers.	
14	Solution should consist Un-obfuscated parsers natively available with log connector to modify existing parser as when required by security operations team.	
15	All logs should be Authenticated (time-stamped), encrypted OR transmitted over a secure encrypted channel and compressed before / after transmission. No performance deggration should happen	
16	The solution should have the capability to compress the logs by at least 80 % for storage optimization.	
17	The proposed solution should have capability to provide centrally or remotely log collector installation to integrate event sources. This is to ensure to reduce time of implementation as well as any changes to be made later through single click push from central site.	
18	The solution must provide the ability to reduce event data through filtering or aggregation before it is sent to the log management system. License count should be performed post filtering of logs.	
19	Caching & Batching: The proposed solution must support local caching and batching and batching at collection level in case of connectivity failures.	
20	In case the connectivity with SIEM management system is lost, the collector should be able to store the data in its own repository. The retention, deletion, synchronization with SIEM database should be automatic but it should be possible to control the same manually.	
21	Any failures of the event collection infrastructure must be detected and operations personnel must be notified as per SLA. The device Health monitoring must include the ability to validate that original event sources are still sending events	
22	Solution should have the ability to perform free text searches for events, incidents, rules and other parameters.	
23	Proposed solution should support searching of Data/artifacts associated with historical incidents.	
24	The proposed solution must be capable of processing and storing large volumes of historical log data that can be restored and analyzed for forensic investigation purposes.	
25	The solution should have the capability to identify / remember frequently used queries	
26	The solution should include compliance reports for standard - ISO 27001/02. The solution should also generate reports for these standards	
27	The solution must provide real-time analysis of events. Mention lag, if any, between the actual event and its reporting with analysis	

28	The proposed solution must have search criteria to be saved as dashboard or reports.	
29	Solution must support searching and reporting of logs at logging layer with machine learning capabilities.	
30	Proposed solution should support predictive analyis (data science enabled) by creating custom data models in log reporting.	
31	Proposed solution should have data science engine that enables users to perform predictive analysis by allowing adding additional variables and columns to report for further scrutiny.	
32	Solution should have 6 month's log retention, storage needs to provisioned for the same.	
33	It must have auto archive feature to archive logs on secondary storage from offline storage perspective. (I.e NAS/DAS/NLSAS)	
34	All logs must get auto archived on centralized storage directly from Log management layer and archived logs must be readable from archival/ central storage directly	
35	**Licensing**	
36	Proposed SIEM, UBA & SOAR solution should be software based solution.	
37	SIEM Solution license should be proposed for 10000 EPS from Day 1, while solution hardware needs to be proposed for 25000 EPS from Day 1. Solution should not drop or queue logs in case of license exceeds in case of suddden rise in EPS during any unwanted situation (eg. Cyber-attack).	
38	No Events should be dropped during Spikes, even if license limits gets exceeded: The proposed solution must not, under any circumstances, drop incoming events. This is essential to ensure compliance/audit integrity and preserve necessary data to detect and mitigate threats during an attack or other unforeseen spikes in event volumes.	
39	UBA shall be inbuilt solution within SIEM and shall be sized for 1000 Users	
40	SOAR solution can be from same or different OEM, however there should be out of the box integration avialble between both SIEM & SOAR. The SOAR solution shall be licensed for atleast 15 analysts	
41	Solution shall be able to ingest Threat Intel feeds from both SIEM OEM (in-built feeds) & also third party (open source feeds)	

SIEM

SN	Specification Required	Compliance Yes / No
1	The system/solution should have the ability to correlate all the fields in a log	
2	The proposed system should have the real-time correlation capability. The system should be updated with customizable correlation rules based on new identified attack patterns and threats. It must be possible to create Customized corelation rules.	
3	The system should have out of the box rules for listed IDS/IPS, firewalls routers, switches, VPN devices, antivirus, operating systems, Databases and standard applications etc.	
4	The system should permit setting up geographical maps/images on real time dashboards to identify impacted areas and sources of alerts.	
5	The event should reach the SOC monitoring team in near real-time of the log being captured	
6	The solution should generate the following reports (but not restricted to): User activity reports, Configuration change reports, Incident tracking report, Attack source reports etc. In addition, the solution should have a reporting writing tool for development of any ad-hoc reports.	

7	All the dashboards for SIEM monitoring should be completely customizable and shall have the feature for restricted access depending on user / group based. Dashboard should be hosted at DC premises.	
8	Solution should be able to perform the following correlations (but not limited to): Rule based, Vulnerability based, Statistical based, Historical based, Heuristics based, Behavioral based, Risk based etc.	
9	Solution should have capability to detect identity breaches and threats even when the account is not active	
10	Solution should provide a heatmap dashboard against all use cases which are active in the system which should help to strategies the security posture.	
11	SIEM solution must provide threat intelligence to enrich/correlate events collected. This TI feed must be from OEM but solution should support integration with Opensource/3rd party TI feeds as well.	
12	Solution should have ability to gather information on real time threats and zero day attacks issued by anti-virus or NGFW vendors or audit logs and add this information as intelligence feed in to the SIEM solution via patches or live feeds	
13	SIEM platform must support MITRE For threat intelligence.	
14	Solution must support integration with 3rd party VA solutions that provides the Vulnerability database information such as Nessus, Rapid7 etc.	
15	SIEM solution must support API integration with 3rd party solutions.	
16	SIEM solution must provide built in ticketing system to track incident from creation to closure, provide reports on pending incidents and permit upload of related evidences such as screenshots etc at the Incident management tool manually. Also it should be able to integrate with 3rd party ticketing tools.	
17	The solution should offer a means of escalating alerts between various users of the solution, such that if alerts are not acknowledged in a predetermined timeframe, that alert is escalated to ensure it is investigated.	
18	The solution should be capable monitoring user suspicious activites and providing but not limited to following use cases 1. User activity monitoring 2. Suspicious activity monitoring 3. Privileged use monitoring etc.	
19	Solution must support detection of zero day attacks and must leverage MITRE Attack framework to provide full visibility/detection of various attacks.	
20	Solution must leverage MITRE Att&ck framework to provide full visibilty/detection of various attacks.	
21	Proposed SIEM must be capable of integration without third party tools to existing running SIEM in Railtel to collaborate cyberIntelligence and future proofing.	
22	**SOAR - Security Orchestration and Automated Response**	
23	SOAR solution must provide MTTR and MTTD reports/dashboards.	
24	Solution should have security orchestration and automated response engine bi-directionally integrated to reduce security incident MTTR (Mean Time To Respond) and automate L1/L2 security activities.	
25	SOAR solution must support automation and response by OOB readily available playbooks (auto and semi), but at the same time there should be scope to customize and create new playbooks	
26	SOAR solution should have an inbuilt threat indicator repository which can be used for active threat hunting using automated playbooks. Threat indicator repository should be able to integrate with third party intelligence sources as well.	
27	SOAR solution should collect real time global threat intel data, dedupe, aggregate, normalize, enrich, and process threat intelligence in a holistic and actionable manner.	
28	Proposed SOAR technology should have Threat intel platform inbuilt with OEM threat intel feeds and support for both commercial and open source threat intel feeds.	
29	The solution should provide option to manually invoke selected playbook based on any selected or set of selected events.	

WAF

SN	Specification Required	Compliance (Yes/No)
1	**General Requirements:**	
2	Web application firewall should be VM/Hardware based solution and provide specialized application threat protection.	
3	Should be ICSA /Equivalent Certified.	
4	Should protect against application-level attacks targeted at web applications.	
5	Should provide controls to prevent identity theft, financial fraud and corporate espionage.	
6	Appliance should have unlimited application licenses.	
7	**Performance requirements**	
8	Should support 250K HTTP transactions per second & at least 200K HTTPs transactions per second	
9	Should deliver at least 10 Gbps of WAF throughput with HTTP & HTTPs traffic.	
10	**Feature specifications.**	
11	The appliance should be able to perform in multiple modes such as Active mode, passive mode, Transparent mode, proxy mode,	
12	Should have a Web Vulnerability Scanner to detect existing vulnerabilities in the protected web applications.	
13	Provide controls to meet PCI compliance requirements for web application servers.	
14	Should have controls for Anti Web Defacement and provide ability to check the authorized version of the website content.	
15	Ability to create custom attack signatures or events	
16	WAF should support Normalization methods such as URL Decoding, Null Byte string, termination, Converting back slash to forward slash character etc..	
17	For mobile clients that cannot execute Java script or CAPTCHA, the solution should be able to verify the legitimate request by verifying the token a mobile application carries when it access a web server	
18	The solution should be able to protect the Mobile APIs from malicious attacks by verifying the mobile device authenticity	
19	The WAF should support IP Reputation Service and able to provide up to date information about threatening sources.	
20	Support IPv6 for Reverse Proxy deployments and It should also Support IPv4 to IPv6 and IPv6 to IPv4 communication	
21	Device should able to control BOT traffic and It should able to block known bad bots and fake search engine requests, The solution should be able to support deception technique to identify bots through inserting a hidden link into response page.	
22	The solution should be able to verify bot clients by monitoring events such as mouse movement, keyboard, screen touch, and scroll, etc	
23	The solution should have inbuild Antivirus module for scanning malicious content in file and uploads to APT Solution in future.	
24	Should support machine learning that detects and blocks threats while minimizing false positives	
25	Should be able to protect Cookie Poisoning and Cookie Tampering.	
26	Should validate header length, content length, Body length, Parameter length, body line length etc..	
27	**SSL**	
28	Appliance should be able to terminate SSL	
29	Client certificates should be supported in passive mode and active mode.	

30	In termination mode, the backend traffic (i.e. the traffic from the WAF to the web server) can be encrypted via SSL	
31	**High Availability and load balancing**	
32	Should support High Availability in Active-Active HA Clustering	
33	WAF appliance should have application-aware load-balancing engine to distribute traffic and route content across multiple web servers.	
34	WAF appliance should support Data compression for better response time to users	
35	**OEM Eligibility**	
36	OEM should have an affiliated entity and should have a presence in India for at least 15 years.	
37	OEM should have TAC and R&D centre in INDIA.	
38	OEM should not be blacklisted with in last 3 years in any of the government organization	

Server Security Solution

Sn	Specifications	Comply (Yes/No)
1	Support protection over a wide range of (i) platforms such as Windows, Linux, etc. & (ii) servers such as directory services, databases, mail services, DNS, cloud services, etc.	
2	Should have modules such as (i) state full Inspection Firewall, (ii) Anti-Malware, (iii) Vulnerability Protection, (iv) Application control and File Integrity Monitoring within a single package.	
3	Should support IP-based protocols (TCP, UDP, ICMPetc.), all frame types (IP, ARP, etc.) with fine-grained filtering (IP and MAC addresses, ports).	
4	Should have features such as network content inspection on host machine, boot protection, File Server Protection, System monitoring such as registry entries & critical directories, etc.	
5	Should be able to monitor critical operating system and application files such as directories, registry keys, and values, etc. to detect & report malicious changes.	
6	Should have functionality to reduce the attack surface on the servers by blocking or only allowing the trusted applications.	
7	Should monitor behaviour of a host and events occurring within that host for any suspicious activity. The characteristics which need to be monitored include network traffic, system logs, running processes, file access & modification, and system & application configuration changes.	
8	Should allow creation and deployment of user defined firewall policy for server to permit or deny network access based on IP Address, logical Ports, and Services on a single IP Address, range, and segments.	
9	Should provide automatic recommendations scans against existing vulnerabilities and deploy corresponding protection on the servers.	
10	Should provide Server based Intrusion Prevention System to proactively monitor, block and safely eliminate malware and potentially unwanted risks from servers.	
11	Should provide targeted prevention policy to respond to server incursion, also protect database servers against SQL injection attacks.	
12	Should allow for creating whitelisting of application programs and block all remaining programs, or vice versa.	

NABD

Sn	Specifications	Comply (Yes/No)

1	Proposed solution should be a purpose-built Network Based Threat Analytics solution hardware and must not be part or component of devices like NGFW and UTM. Solution should be able to detect zero day threats	
2	Proposed solution must be able to have options from 1 Gbps to 4 Gbps of traffic capacity for inspection. Solution should be able to provide deployment methods like out of the band (TAP/SPAN).	
3	Proposed solution must have minimum 4 x 1G Base-T Ethernet ports & 4*10 Gb SFP ports. It should be able to monitor the traffic from multiple LAN segments. Proposed solution should have dedicated management port.	
4	The proposed solution should be able to inspect multiple protocol to detect and flag the suspicious activity including suspicious file downloads through the web, the suspicious mail attachment and internal infections happening via lateral movement(RDP, SMB, CIFS and etc.). Solution should be able to inspect most used (more than 70)protocols which are used by adversaries to perform stages of targeted attacks in case of out of band deployement	
5	The proposed solution should be able to detect the persistent threats(which come through executable files, PDF files , Flash files, RTF files and/or other objects). The proposed solution should have multiple engines and advanced techniques like Machine learning , vulnerability/exploit inspection to detect and prevent advanced persistant threats(Multistage, well-planned, and organized attacks), and should provide full visibility of complete network.	
6	Proposed solution should perform advanced network detection and analysis of the network(east-west) traffic without relying on the agents on endpoints or servers. The detections in the solution shall be mapped with MITRE attack framework.	
7	The proposed solution should be able detect C&C communication , data exfiltration attempts , DNS callbacks/Queries by deeply inspecting the network traffic. Solution should have functionality to exchange threat intelligence like IP/URL domain etc. using API or STIX/TAXII protocol.	
8	Should detect targeted attacks , advanced threats , ransomware associated binaries , Zero-day malware and exploits in the document , suspicious behaviour and network activity , web based threats including exploits and drive-by downloads, email threats like spear phishing , Bots, Trojans, worms, keyloggers.	
9	Proposed Solution shall have extensive detection techniques with capability to analyse web, IP, mobile application reputation in addition to heuristic analysis, perform advanced threat scanning, custom sandbox analysis, and correlated threat intelligence to detect ransomware, zero-day exploits.	

VPN

SN	Specifications	Compliance(Yes/No)
1	The solution must Support 100 concurrent users from day1 and scalable up to 500 concurrent users on same setup.	
2	Solution must support Access control options based on:- a) User and group, b) Source IP and network, c) Destination network ,e) Service/Port, f) Host name or IP address ,g) IP range, h) Subnet and domain, I) Day, date, time and range.	
3	The solution must provide machine authentication based on combination of HDD ID, CPU info and OS related parameters i.e., mac address to provide secure access to corporate resources.	
4	The solution should support Machine based authentication based on AD/LDAP group membership.	
5	The appliance should provide detailed logs and graphs for real time- and time-based statistics	
6	OEM Should have local India TAC support should be preferred.	

7	Seamless Experience while switching from Client to Browser or vice versa : The user should not face any difference in experience while using VPN through client or browser. e.g. if DSC or any third party services are seamlessly allowed over client, same should be the case for Browser based access also and vice-versa.	
8	Multi-Factor Authentication: SMS through http and API, OEM App Based (With customization allowed for RailTel branding), Third Party App Based (G-Auth etc.)	
9	Forgot Password Option: The solution should allow users to change their password (1st Level), in case they forgot it or want to make new, through option of 'Forgot Password' or through publishing the external link on login page.	
10	End Point Control : Should allow to set policy for access e.g. MAC binding, Mother Board ID/ CPU ID/IMEI No. or any other unique IDs of an electronic device and universally accepted. The solution should also to enable access from a defined geography (location), traffic from a mentioned Public IP and push alert to End User if logging is happening from outside of defined parameters. Solution should also allow to define 'Session Time' and accordingly forceful logout due to long idle session.	
11	Self-Service Portal: The solution should allow RailTel as well as Admin of End User Organization to add / delete / ration end users basis on parameters as mutually agreed between RailTel and End User Organization	
12	Installation configuration and Management training to be provided by the OEM of supplied product.	

Hardware Security Module (HSM)

Sr. No.	Requirements	Compliance (Yes / No)
1	Should support Windows 2008 or higher, Linux	
2	Appliance should have Cryptographic boundary module which should comply to standards FIPS 140-2 Level 3	
3	Key Exchange Symmetric Algorithm: AES, Triple DES (No separate license of Alogrithm to be charged)	
4	Support for Hash Message Digest HMAC, SHA1 SHA2 (224-512)	
5	Support for various cryptographic algorithms: Asymmetric Key RSA (2048-4096 bits)ECDSA , ECC (No separate license of Algorithm to be charged)	
6	Random Number Generation –FIPS 140-2 approved	
7	Should Published API for various above functionalities for integrating with the Application software	
8	Should have PKCS11 ,JAVA JCA and RestAPI's for connectivity	
9	Keys must be stored in Crypto memory of hardware within FIPS boundary of HSM	
10	Onboard key generation, signing inside the HSM	
11	Minimum keys storage should be 1000 RSA keys of 2048 bits within FIPS 140-2 Level 3 certified crypto memory only (storage on NVRam not allowed)	
12	Concurrent 100+ Keys should be usable for Signing and Encryption	
13	The backup and recovery of the all keys should be automatic between HA and DR devices over network cluster (Without any backup device)	
14	The solution should also support automatic synchronisation of keys between deployed HSM Systems in DC and DR	

15	HSM should be capable of overall key management (creation, access, archival, destruction)	
16	Support for minimum 500 Transaction per Second @ RSA 2048 bits	
17	HSM should be field upgradable to higher TPS and higher key storage	
18	HSM should have 10+ logical user partition, each user partition should have its own Username and PIN	
19	HSM once divided in partition TPS should be proportionally divided among the partition & HSM performance should not lower in case of concurrent useage of partition	
20	Appliance should have Dual network port	
21	Appliance should support IPv4 & IPv6	
22	Should support SNMP	
23	Appliance should be 2U rack size	

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 (hereinafter called " 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 ********