RAILTEL CORPORATION OF INDIA LIMITED
(A Govt. of India Undertaking)

ELECTRONIC TENDER DOCUMENT

FOR

Supply and Supervision of Installation, Testing & Commissioning of DDOS detection and Mitigation for MPLS Network (Two Packet)

OPEN E-TENDER NO.RAILTEL/TENDER/OT/CO/DNM/2016-17/DDOS/330 Dated: 20.05.2016

Cost Tender Document: Rs.10,000/-(Including VAT)

Sold to _____

RailTel Corporation of India Ltd.
Plot No. 143, Institutional Area, Sector -44
Gurgaon-122003, Ph: 0124-4236085-86, Fax: 0124-4236084

E-Tender Notice No.: RAILTEL/TENDER/OT/CO/DNM/2016-17/DDOS/330 Dtd.20.05.2016

RailTel Corporation of India Ltd. (RailTel) invites Tenders for **"Supply and Supervision of Installation, Testing & Commissioning of DDOS detection and Mitigation for MPLS Network"**.

a)	Opening date of Tender downloading	20.05.2016
b)	Pre-bid Enquiry Date	03.06.2016 1500 hrs.(Offline)
b)	Submission date of bids	21.06.2016 up-to 1500 hrs.(Offline)
c)	Opening of bids	21.06.2016 at 1530 hrs (Offline)
d)	Approximate cost of Tender	Rs 03.07 Crore (aprox.)
e)	Earnest Money (EMD)	Rs 5,00,000/- to be made in favor of RailT Corporation of India Ltd. in the form of D payable at New Delhi.
f)	Cost of Tender Document is Rs.10, 000/-(Including VAT)	

Small scale Units registered with NSIC under single point registration scheme are exempted from cost of Tender Documents.

Note: Tender Notice and Tender Document are available on RailTel's website and can be downloaded from www.railtelindia.com or from the e-Tendering portal https://www.tcil-india-electronictender.com. For online bid submission the tenderer will have to necessarily download an official online copy of the tender documents from TCIL's e- portal. All future Information viz. corrigendum /addendum/ amendments etc. for this Tender shall be posted on the e-Tendering Portal only. Printed copy of Tender document will not be sold from RailTel office.

The bidder shall bear all costs associated with the preparation, submission/participation in the bid. Purchaser in no way will be responsible or liable for these costs regardless of the conduct or outcome of the bidding process.

INDEX

Chapter	Contents	Page No.
Chapter 1	Offer letter	4
Chapter 2	Schedule of Requirement	5-6
	Annexure-A: Price Schedule for Indigenous Items	7
	Annexure-B: Price Schedule for Imported Equipment	7
Chapter 2A	E- Tendering instructions to bidders	8-13
Chapter 3	A. Scope of Work	14-35
	B. INSPECTION AND INSTALLATION, TESTING & COMMISSIONING	36-41
	C. TRAINING, VENDOR DATA REQUIREMENT, DOCUMENTATION, AND DESIGN GUIDELINES	42-45
Chapter 4	Commercial Terms and Conditions	46-58
Chapter 5	Bid Data Sheet (BDS)	59-63
Chapter 6	Form No. 1: Performa for Performance Bank Guarantee	64
	Form No. 2: Performa for System Performance Guarantee	65
	Form No. 3: Performa for the Long term Maintenance Support	66

CHAPTER-1

OFFER LETTER

RailTel Corporation of India Ltd.
Plot No. 143, Institutional Area,
Opposite-Gold Souk,
Sector-44, Gurgaon-122003

1. I/We _____ have read the various conditions detailed in tender documents attached here to and hereby agree to ABIDE BY THE SAID CONDITIONS. I/We also agree to keep this offer open for acceptance for a period of 120 days from the date of submission and in default thereof. I/We will be liable for forfeiture of my/our Earnest Money. I/We offer to supply various equipment at the rates quoted in the attached schedules and hereby bind myself/ourselves to complete the work of **"Supply and Supervision of Installation, Testing & Commissioning of DDOS detection and Mitigation for MPLS Network"** within 180 days from the date of issue of Purchase Order. I/We also hereby agree to abide by the Various Conditions of Contract and to carry out the supplies according to the Specifications for materials and works laid down by the RailTel.

2. A sum of **Rs. 5,00,000/- (Rs. Five lacs)** as an Account Payee Demand Draft in favour of RailTel Corporation India Ltd. No._____ dated_____ issued by _____is herewith forwarded as "Earnest Money". The full value of Earnest Money shall stand forfeited without prejudice to any other rights or remedies if, I/We withdraw or modify the offer within validity period or do not deposit the security deposit (Performance Bank Guarantee) within 15 days after issue of Purchase Order.

SIGNATURE OF SUPPLIER (S)

Date:

CONTTRACTOR (S) ADDRESS

SIGNATURE OF WITNESS:

1.

2.

CHAPTER- 2

SCHEDULE OF REQUIREMENT

SCHEDULE OF REQUIREMENT-A (Supply)

SN	Description	Qty	Unit Rate		Total cost	
			In Fig	In Words	In Fig	In Words
1	DDOS Detector/Flow Collector system as per technical specification mentioned in Chapter-3	2				
2	DDoS Mitigation system as per technical specification mentioned in Chapter-3	2				
3	License Cost per Core/Peerring Router	1				
4	License cost per Edge router	1				
5	Additional unit License cost per 10 Gbps of mitigation capacity for Upgradation	2				
6.	Additional Unit License Cost per 50K Flows per Second for Detection system for Upgradation	2				
7.	License cost for 25 Simultaneous user logging license for self service portal for Upgradation	1				
8.	License cost for 500 Monitored Entities for Upgradation	1				
9.	Router (In case of non router based mitigation appliance is quoted) as per the speciation's given in chapter 3	2				
10	Supply of any other items, equipment, cards considered necessary to meet the end objectives as detailed in the tender document.	Lot				
	Total (In Rs) of SOR A					

SCHEDULE OF REQUIREMENT-B (Services)

SN	Description	Qty	Unit Rate		Total cost	
			In Fig	In Words	In Fig	In Words
1	Installation and Commissioning	1				
2	Resident Engineer(for 1 Year)	1				
	Total Value of SOR-B					

SCHEDULE OF REQUIREMENT-C (AMC)

SN	Description	Unit	Qty	Unit Rate for One year		Total cost for Four year	
				In %	In Fig	In %	In Fig
1	2	3	4	5	6	7	8
1	Incremental % AMC cost in addition to 3.5 % mentioned in clause 3 of Chapter-4	Years	4				

	Total Value of SOR-A,B & C						

Note:	
I.	a) Unit rate quoted against SOR above should be CIP destination inclusive of all duties, taxes, insurance and freight etc (with tax break-up as per Performa attached as Annexure-A&B).The materials as per SOR are required to be delivered within the delivery period as indicated in Bid Data Sheet (BDS, Chapter 5) to the sites as per Annexure-I b) It shall be the responsibility of Tenderer to transport the equipment to site for Installation & Commissioning.
II.	Tenderers should submit the detailed configuration of each type of equipment indicating quantities of various modules/sub modules/cards/Licenses/sub racks including the vacant slots in the sub racks/chassis for further expansion. Detail BOM of each equipment supplied under the contract shall be submitted along with the bid and the same shall be duly vetted by the OEM. Tenderer should do the field analysis including power (AC/DC) and recommend the solution as per power available in the field/POPs/DC and quote as per the solution. The hardware/appliance should be of the scalable configuration at the time of deployment form the Day-1.
III.	The Tenderer shall attach Unit Rate Analysis of Schedule of Requirements (cost of each sub-assembly, card, module, Licenses etc.) in their Price Bid. The quoted Unit Rates should correspond to the referred unit Rate.
IV.	It is mandatory for Tenderer to quote for all items of the schedule. Any bid not having quote for all the item of the schedule may not be considered.
V.	Tenderers should provide one dedicated Resident Engineer Level II for 1 year on purchaser premises. Purchaser has right to select the appropriate resident Engineer who has to manage and operate the DDOS Detection and Mitigation system.
VI.	Tenderer must also furnish unit rate of all the supply of items mentioned in the SOR-A , which will be required for the Solution. These will also form part of the Rate Contract for procurement of items for up gradation as per Railtel requirement in future.

****

Annexure-A
Tax Breakup for SOR A.

S N	Descri ption	Total Qty	EX-Factory Price (Basic Unit Price exclusive of all levies and charges)	Pkg & Forwardin g Charges		Excise Duty		Sales Tax		Frieght & Insurance Charges		Other Charges and Levies	Price Per Unit (all inclusive) for delivery at destination (4+6+8+10 +12+13)
				%	Am t	%	Amt	%	Amt	%	Amt		
1	2	3	4	5	6	7	8	9	10	11	12	13	14

Annexure-B
Tax Breakup for SOR B &C.

SN	Description	Total Qty	Service Tax		Any Other Charges and Levies	Price Per Unit (all inclusive) (4+6)
			%	Amt		
1	2	3	4	5	6	7

Chapter - 2-A

E-tendering Instructions to Bidders

Note:-E-Tendering Instructions to Bidders terms given in others chapters shall be superseded by the terms given in Chapter-2 A.

Submission of Bids only through online process is mandatory for this Tender.

E-Tendering is a new methodology for conducting Public Procurement in a transparent and secured manner. Now, the Government of India has made e-tendering mandatory. Suppliers/ Vendors will be the biggest beneficiaries of this new system of procurement. For conducting electronic tendering, RailTel has decided to use the portal https://www.tcil-india-electronictender.com through TCIL, a Government of India Undertaking. This portal is based on the most 'secure' and 'user friendly' software from Electronic Tender®. A portal built using Electronic Tender's software is also referred to as Electronic Tender System® (ETS).

Benefits to Suppliers are outlined on the Home-page of the portal.

1. Tender Bidding Methodology:
   Sealed Bid System - 'Two stage Two Envelope". In this, bidder has to submit Techno-commercial bid and Price-Bid in two envelopes "ON-LINE."

2. Broad outline of activities from Bidders Perspective:
   2.1. Procure a Digital Signing Certificate (DSC)
   2.2. Register on Electronic Tendering System® (ETS)
   2.3. Create Users and assign roles on ETS
   2.4. View Notice Inviting Tender (NIT) on ETS
   2.5. Download Official Copy of Tender Documents from ETS (Important)
   2.6. Clarification to Tender Documents ETS Query to RailTel (Optional)
   View response to queries posted by RailTel, as addenda.
   2.7. Bid-Submission on ETS
   2.8. Attend Public Online Tender Opening Event (TOE) on ETS.
   2.9. View/Post-TOE Clarification posted by RailTel on ETS (Optional), Respond to RailTel's Post-TOE queries

   For participating in this tender online, the following instructions need to be read carefully. These instructions are supplemented with more detailed guidelines on the relevant screens of the ETS.

3. Digital Certificates
   For integrity of data and its authenticity/ non-repudiation of electronic records, and be compliant with IT Act 2000, it is necessary for each user to have a Digital Certificate (DC). also referred to as Digital Signature Certificate (DSC), of Class 2 or above, issued by a Certifying Authority (CA) licensed by Controller of Certifying Authorities (CCA) [refer http://www.cca.gov.in].

4. Registration

   To make use of the Electronic Tender® portal (https:// www.tcil-india-electronictender.com), vendor needs to register on the portal (if not registered earlier). Registration of each organization is to be done by one of its senior persons who will be the main person coordinating for the e-tendering activities. In ETS terminology, this person will be referred to as the Super User (SU) of that organization. For further details, please visit the website/portal (https://www.tcil-india-electronictender.com), and click on the 'Supplier Organization' link under 'Registration' (on the Home Page), and follow further

instructions as given on the site.

Pay Annual Registration Fee as applicable.

Note: After successful submission of Registration details and Annual Registration Fee (as applicable), please contact TCIL/ ETS Helpdesk (as given below), to get your registration accepted/activated.

TCIL Helpdesk
Contact PersonTelephone/ MobileE-mail ID
Helpdesk Executives: 011-2624 1071, 011-2624 1072
ets_support@tcil-india.com
(Mobile Nos. for Emergency Help): 9868393775,9868393717,9868393792.

RailTel Contact-1 (for general Information)
RailTel's Contact Person
Pawan Kumar Sharma:Jt.GM/DNM
Telephone 0124-2714000
Mobile : 9717644497
E-mail ID: pawan@railtelindia.com

RailTel Contact-II (for general Information)

RailTel's Contact Person
A.K.Sablania: GGM/DNM
Telephone 0124-2714000
Mobile : 9717644015
E-mail ID :asablania@railtelindia.com

5. Bid related Information for this Tender (Sealed Bid)
The entire bid-submission would be online on ETS.

Broad outline of submissions are as follows:

1. Submission of Bid Security/ Earnest Money Deposit (EMD)
2. Submission of digitally signed copy of Tender Documents/Addenda
3. Single Envelope (including Technical +Financial part)
The electronic envelope consists of Main bid and Electronic Form (both mandatory) and Bid Annexures (Optional).
4. Online response to General Terms & Conditions (GTC) and Special Terms & Conditions (STC)
5. (Optional) Online Submission of modification, substitution bids for technical or financial parts, or withdrawal bid.

NOTE: Bidder must ensure that after following above, the status of bid submission must become "Complete" indicating successful submission of the online bid.

6. Offline Submissions:

The bidder is required to submit the following documents offline to RailTel Corporation of India Ltd, Institutional Area Plot 143, Sector 44, Gurgaon before due date & time of submission of bids specified in covering letter of this tender document, in a Sealed Envelope. The envelope shall bear (the tender name), the tender number and the words 'DO NOT OPEN BEFORE' (due date & time).

a) EMD-Bid Security in Original, in favour of RailTel Corporation of India, Payable at New Delhi. (with Tender No., Name of Firm & Mob. No. written on back side of DD)

b) DD/ Bankers cheque in original against payment of tender fee in favour of RailTel Corporation of India, Payable at New Delhi.. (with Tender No., Due date of Opening of Tender, Name and contact No. of Firm written on back side of DD)

c) Power of attorney to be submitted in accordance with Tender Conditions.

d) In case bidder happens to be a NSIC bidder, the documentary evidence for same shall be submitted.

NOTE: The Bidder has to upload the Scanned copy of all above original documents as Bid-Annexure during Online Bid-Submission.

7. Submission of Eligibility Criteria related documents

Eligibility criteria related documents as applicable shall also be scanned and submitted ON LINE. Copy of these documents shall also be submitted before Tender opening date. Bids without these off line submissions will be summarily rejected.

8. Special Note on Security of Bids

Security related functionality has been rigorously implemented in ETS in a multi-dimensional manner. Starting with 'Acceptance of Registration by the Service Provider', provision for security has been made at various stages in Electronic Tender's software. Security related aspects as regard Bid Submission are outlined below:

As part of the Electronic Encrypter™ functionality, the contents of both the 'Electronic Forms' and the 'Main-Bid' are securely encrypted using a Pass-Phrase created by the Bidder himself. Unlike a 'password', a Pass-Phrase can be a multi-word sentence with spaces between words e.g. (I love this World). A Pass-Phrase is easier to remember and more difficult to break. It is recommended that a separate Pass-Phrase be created for each Bid-Part. This method of bid-encryption does not have the security and data-integrity related vulnerabilities which are inherent in e-tendering systems which use Public-Key of the specified officer of a Buyer organization for bid-encryption. Bid-encryption in ETS is such that the Bids cannot be decrypted before the Public Online Tender Opening Event (TOE), even if there is connivance between the concerned tender-opening officers of the Buyer organization and the personnel of e-tendering service provider.

Typically, 'Pass-Phrase' of the Bid-Part to be opened during a particular Public Online Tender Opening Event (TOE) is furnished online by each bidder during the TOE itself, when demanded by the concerned Tender Opening Officers who will open the bid. Else Tender Opening Officer may authorize the bidder to open his bid himself. There is an additional protection with SSL Encryption during transit from the client-end computer of a Supplier organization to the e-tendering server/ portal.

(Mandatory Additional Methods of passphrase submission):

Additionally, the bidder shall make sure that the Pass-Phrase to decrypt the relevant Bid-Part is submitted to RailTel in a sealed envelope before the start date and time of the Tender Opening Event (TOE) along with other offline submissions.

9. Public Online Tender Opening Event (TOE)

ETS offers a unique facility for 'Public Online Tender Opening Event (TOE)'. Tender Opening Officers as well as authorized representatives of bidders can attend the Public Online Tender Opening Event (TOE) from the comfort of their offices. For this purpose, representatives of bidders (i.e. Supplier organizations) dully authorized are requested to carry

a Laptop and Wireless Connectivity to Internet.

Every legal requirement for a transparent and secure 'Public Online Tender Opening Event (TOE)' has been implemented on ETS. As soon as a Bid is decrypted with the corresponding 'Pass-Phrase' as submitted online by the bidder himself (during the TOE itself), salient points of the Bids are simultaneously made available for downloading by all participating bidders.

ETS has a unique facility of 'Online Comparison Chart' which is dynamically updated as each online bid is opened. The format of the chart is based on inputs provided by the Buyer for each Tender. The information in the Comparison Chart is based on the data submitted by the Bidders in electronic forms. A detailed Technical and/ or Financial Comparison Chart enhance Transparency. Detailed instructions are given on relevant screens.

ETS has a unique facility of a detailed report titled 'Minutes of Online Tender Opening Event (TOE)' covering all important activities of 'Online Tender Opening Event (TOE)'. This is available to all participating bidders for 'Viewing/ Downloading'.

There are many more facilities and features on ETS. For a particular tender, the screens viewed by a Supplier will depend upon the options selected by the concerned Buyer.

NOTE: In case of internet related problem at a bidder's end, especially during 'critical events' such as - a short period before bid-submission deadline, during online public tender opening event, during e-auction, it is the bidder's responsibility to have backup internet connections.

In case there is a problem at the e-procurement/ e-auction service-provider's end (in the server, leased line, etc) due to which all the bidders face a problem during critical events, and this is brought to the notice of RailTel by the bidders in time, then RailTel will promptly re-schedule the affected event(s).

10. Other Instructions

For further instructions, the vendor should visit the home-page of the portal (https://www.tcil-india-electronictender.com), and go to the User-Guidance Center.

The help information provided through 'ETS User-Guidance Centre' is available in three categories - Users intending to Register / First-Time Users, Logged-in users of Buyer organizations, and Logged-in users of Supplier organizations. Various links are provided under each of the three categories.

Note: It is strongly recommended that all authorized users of Supplier organizations should thoroughly peruse the information provided under the relevant links, and take appropriate action. This will prevent hiccups, and minimize teething problems during the use of ETS.

11. The following KEY INSTRUCTIONS for BIDDERS' must be assiduously adhered to:

    1. Obtain individual Digital Signing Certificate (DSC or DC) well in advance of your first tender submission deadline on ETS.
    2. Register your organization on ETS well in advance of your first tender submission deadline on ETS.
    3. While registering your organization on ETS Portal of TCIL, pl. make sure that the email id of Super user provided for registration and email-id on which Digital

Signature Certificate of the Super user is issued are exactly the same.

4. Get your organization's concerned executives trained on ETS well in advance of your first tender submission deadline on ETS.
5. Bidder should ensure that official copy of tender document has been downloaded by clicking the radio button for confirmation else e-Procurement system will not permit the bidder to participate in the tendering process.
6. Submit your bids well in advance of tender submission deadline on ETS as there could be last minute problems due to internet timeout, breakdown, etc.

12. Minimum Requirements at Bidders end

- Computer System with good configuration (Min P-IV, 1 GB RAM, Windows XP)
- Broadband connectivity.
- Microsoft Internet Explorer 6.0 or above
- Digital Certificate (s) for users.

13. Vendors Training Program

One day training (10:00 to 17:00) on how to use the ETS Portal for e-Tendering would be provided. Training is optional. However, if a vendor has not already attended ETS Vendor Training earlier, it is highly recommended that the vendor attends this training positively to be able to submit the e-Tender smoothly without any problem.

Vendors are requested to carry a Laptop and Wireless Connectivity to Internet while attending the ETS Vendor Training.

Tentative Dates

Date of uploading of Tender document + 7 days

Venue

RailTel Corporation of India Limited,

Plot No. 143, Sector-44,
Opp. Gold Souk Mall,
Gurgaon -122003.

Vendors Training Charges :Rs. 2,500/-(Per Participant) per training day (plus Service Tax as applicable), i.e., Rs. 2,862/- Per Participant.
Mode of Payment of Fees: DD drawn in favour of M/s TCIL, New Delhi & payable at New Delhi.

1. INTRODUCTION

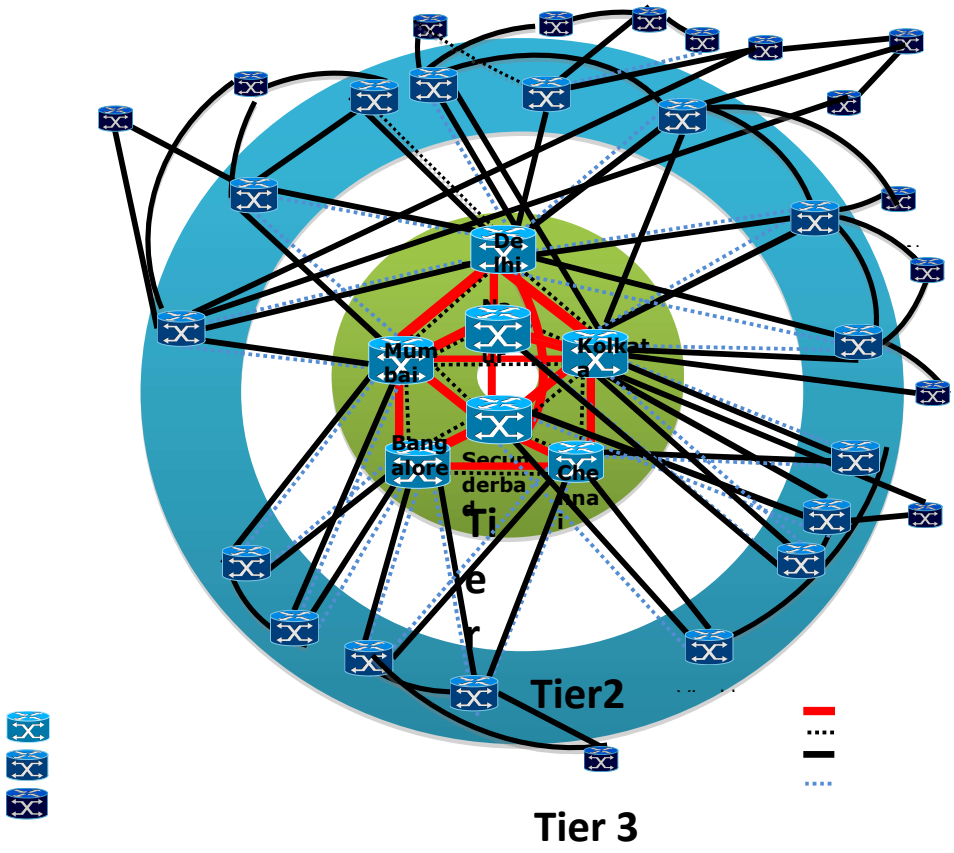
RailTel Corporation of India Limited, a Public Sector Undertaking under the Ministry of Railways, Govt. of India, is a national telecom service provider having NLD, ISP and IP1 licenses and has built a nation-wide optical fiber network. RailTel's objective is to create a nation-wide broadband telecom and multimedia network.
The Corporation was formed in Sept 2000 with the vision 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 significantly contribute to realization of goals and objective of national telecom policy 1999. RailTel is a wholly owned subsidiary of Indian Railways.

1.1. RailTel Telecom Network

RailTel is building State of the art multimedia telecom network using SDH/DWDM based transmission systems and high end MPLS-IP routers. RailTel has created countrywide state of the art SDH/DWDM backbone optical transport network using latest technology. More than 400 cities covering over 42,000 RKMs across the country are connected on the network with multiple STM-16 (n x 2.5 Gbps) connectivity. RailTel has also implemented ultra-high capacity DWDM network over 10,000 RKM to provide 400 Gbps which is further upgradable to 800 Gbps in future. The PAN India DWDM network has been operational since 2012.
RailTel's backbone Transport Network has been configured in multiple 'Self-Healing' Ring architectures which provide for redundancy by automatically redirecting and switching traffic from failed/ degraded routes for an uninterrupted service ensuring maximum up time and service reliability. The network supports multiple ring protection schemes. The network has been designed in such a way that full redundancy is available for bandwidth between any two points.
The whole network is managed by centralized Network Management System (NMS) centrally located at New Delhi with back up facilities at Secundrabad / Kolkata / Mumbai. RailTel has got unique advantage to offer the best quality service (QoS) from a single unified network with PAN India presence. The state of art network enables point and click provisioning of the bandwidth and other services from anywhere to anywhere in the country. It enables provisioning of traffic in any granularity from 2 MBPS to multiple of Gbps (n x Gbps) from its country wide strong backbone network.

1.2. MPLS Backbone

RailTel has implemented country wide MPLS-IP backbone network to provide whole range of VPN & Internet services. The network has been built using high end routers of Juniper network. The network supports services like Layer 3 and Layer 2 VPN services, broadband internet access, multicast services etc. The MPLS network has POPs at 150 cities across the country and is in the process of being extended to other important cities/towns also. The IP services at about **4000 POPs** in the country will be extended through Ethernet interface available in the SDH networks at these locations which will in turn be connected to MPLS –IP backbone network at the 150 cities. RailTel has recently started targeting the retail customers through Railwire using MPLS-IP backbone network, which provides quality broadband services.



1.3. **NGN based NLD Network**

RailTel has also rolled out NLD (National Long Distance) Services for carriage of Inter-Circle voice traffic based on the State of the Art NGN (Next Generation Network) platform. NLD backbone of RailTel has currently been rolled out in 56 cities having POIs (Point of Interconnection) with all Operators including BSNL/MTNL, Airtel, TTSL, Idea, Vodafone, Reliance, etc. The cities under Phase-I are Bangalore, Chennai, Mysore, Coimbatore, Hyderabad, Cochin, Mumbai, Pune, Ahmadabad, Nagpur, Delhi, Chandigarh, Jaipur, Jallandhar, Luck now, Kolkata, Bhubaneswar and Patna. Additional 36 cities covering all 23 Circles have been added last year. With its PAN India NLD network, RailTel will be able to carry calls to even the remote and rural parts of the country.

1.4. Licenses & Services

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

1.5. Network Support

RailTel has an excellent team of highly qualified engineers working to support our customers on 24x7x365 basis. Proactive maintenance and monitoring is done regularly by engineers thus ensuring better service support. Our state of the art Network Operating Center (NOC) at New Delhi, Mumbai, Kolkata & Secundrabad is capable to generate

online reports for monitoring of SLA (Service Level Agreement) parameters on a periodic basis.

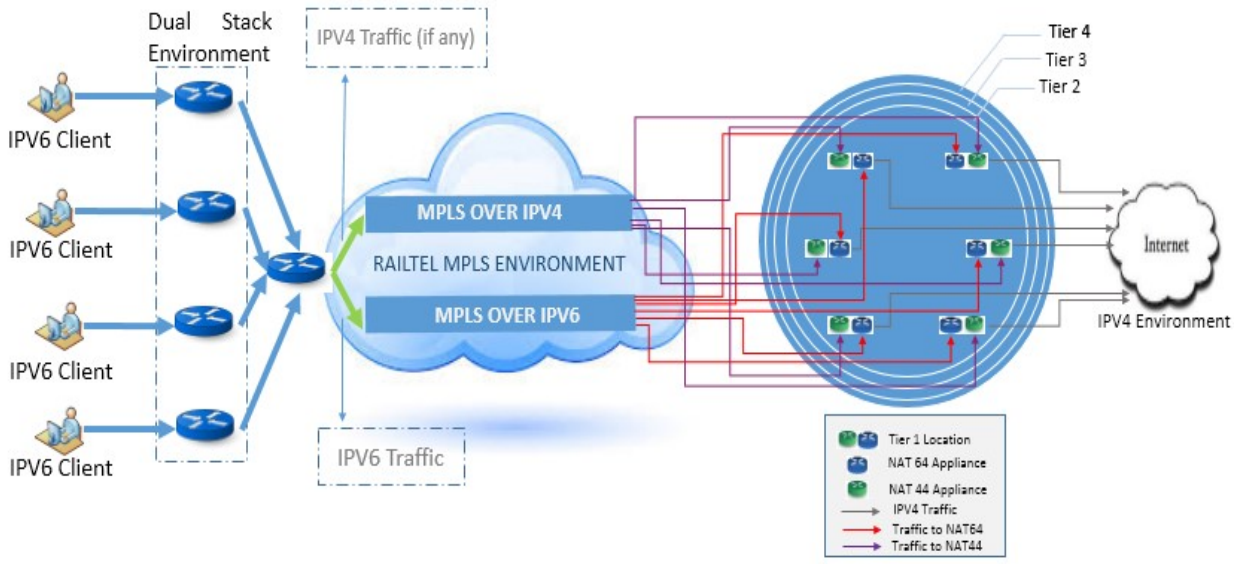
RailTel has presently a work force of approx 500 technically qualified personnel from the field of telecommunication and management. Senior management of RailTel is entirely drawn from Indian Railway and has extensive experience in project, operations and maintenance of telecom network. RailTel has also recruited engineers for operations and maintenance and is in the process of recruiting more technically qualified personnel.

1.6. CGNAT Network

1.6.1. RailTel's Network Architecture

RailTel has a layered network architecture which comprises of four tiers. Tier 1 contains six internet gateways connected in a near full-mesh configuration. Tier 2 consists of 16 cities with every Tier 2 city connected to at least two Tier 1 cities. Tier 3 consists of 16 cities with every Tier 3 city connected to atleast 2 Tier 1 or 2 cities. Tier 4 cities are connected to at least two Tier 1/Tier 2/Tier 3 locations.

With the expansion of internet, Internet Protocol version 4 (IPv4) addresses have exhausted. The ever increasing number of subscribers can only be supported by Internet Protocol version 6 (IPv6) addresses. Being one of the latest entrants in the telecom space, RailTel has got limited number of IPv4 series public IP addresses and intends to use IPv6 series IPs to the extent possible. Telecom Regulatory Authority of India (TRAI) regulations also mandates that all major ISPs should be ready to handle IPv6 traffic and offer IPv6 services. RailTel also intends to leverage on other advantages of IPv6.



The CG-NAT solution has been deployed at the six internet gateway locations located in the Tier1 of the network topology. RailTel has developed an independent MPLS backbone for supporting IPV4 traffic and IPV6 traffic. When the data packet form the subscriber reaches RailTel's network, it is routed through the appropriate MPLS network (IPV4 traffic through MPLS IPV4 network and IPV6 through MPLS IPV6network). The NATing equipment are Installed at the ISP-Internet interface. The data traffic coming from IPV4 MPLS network is passing through CG-NAT44 equipment and the data traffic coming from IPV6 MPLS backbone is passing through the CG-NAT64 equipment. As a result, all packets reaching the internet (website-servers) have a public IPV4 associated to them. The network architecture of RailTel is depicted in the diagram above.

2. DDOS Appliance

2.1. Scope

The Scope of the proposed security architecture will be as follows:

2.1.1. Protect the RAILTEL core network from a wide range of DDOS threats both proactively and reactively.
2.1.2. Improved DDoS attack management for Railtel Network and its customers as railtel is planning to offer the DDoS Detection and Mitigation as a service to its esteemed customers as a clear pipe.
2.1.3. Provide an added line of security for subscribers of RAILTEL.
2.1.4. Guarantee the effective use of internet backbone bandwidth
2.1.5. Protect corporate image being tarnished due to possible security attacks.
2.1.6. Avoid legal implications due to improper use of network facilities by RAILTEL subscribers through proactive mitigation process.
2.1.7. Proactively meet regulatory compliance requirements on DDoS protection.
2.1.8. Provide visibility into network for upstream transit & peer network and analysis. The system should be able to have the visibility of the edge routers which are being used to provide connectivity to enterprise customers.
2.1.9. Provide network wide visibility of On-net, Of-net traffic, Backbone traffic.
2.1.10. Provide visibility & traffic analysis of downstream subscriber's traffic, including on-net & off-net traffic.
2.1.11. Provide MPLS VPN traffic visibility
2.1.12. Provide Managed DDoS Services / Clean Pipe Solutions to RAILTEL's subscribers.
2.1.13. To protect the RAILTEL & Subscribers networks from increasingly frequent and sophisticated attacks like application floods and slow attacks in a proactive manner with minimum false-positives or false negatives.
2.1.14. DDoS Detection & DDoS Mitigation system should be from single OEM.

3. Broad Requirements of the solution

3.1. Intelligent DDoS Detection, Classification & Mitigation

Globally the service providers, Enterprises, Financial Institutions and Govt. Organizations are experiencing wide array of complex threats including Internet based attacks like DDoS, Botnets, DNS cache poisoning, BGP route hijacking etc. The size, scale and complexity are ever increasing. Service providers carry the malicious traffic along with the valid traffic and can compromise the network infrastructure of RAILTEL even if it was intended for the end subscribers. Moreover this can cause collateral damage to other clients of Service providers. RAILTEL realizes that it is good position to detect and mitigate such Network based attacks. Hence, a comprehensive solution is required to protect RAILTEL infrastructure and also subscriber's network connectivity. A passive DDoS detection, classification, trace-back using the existing network infrastructure already built in with intelligent detection capabilities and On-demand intelligent filtering solution is the best methodology to protect own network and subscribers network instead of inline devices.

3.2. Managed DDoS Services

An extension of the above DDoS management solution would be to provide differentiated services like Managed DDoS or Clean pipe services. As Service providers are in the best position to offer In-cloud Managed DDoS services, Service provider would like to roll out such services to premium subscribers, financial institutions, Hosting subscribers / IDCs, wholesale subscribers etc.

The solution should include portal redundancies, subscriber's access and control, subscriber's portal etc.

3.3. Traffic analysis & Reporting.

Flow based technologies have proven to be the most authoritative and efficient way of characterizing network traffic. Flow records provide mechanisms for enhanced optimization of the network infrastructure, operational cost reduction, route analysis, improved capacity planning and security. From Service provider's perspective it is important to contain cost of international links and also provide subscribers traffic analysis and differentiated usage based billing for on-net and off-net traffic. The best way to address this requirement is by having a network wide traffic planning strategy and profiling traffic effectively. Therefore Service provider needs to have a system in place to analyze flow based information on international gateway routers, to make informed timely decisions. The system should be capable of providing visibility into Subscribers Traffic, Backbone Traffic, On-net & Off-net traffic and also MPLS RFC2547 VPN traffic reporting.

3.4. Automated Peering Analysis & Traffic Engineering.

The system should be providing detailed analysis into peer and transit traffic. The system should be capable of identifying the most efficient transit providers with detailed what if analysis & reporting. By performing this analysis, Service provider intends to reduce the Transit and infrastructure costs. The system should be able to provide real-time snapshot reports within seconds and support external disk and store and analysis historical raw flows. This analysis is to be used to reduce costs and improve network performance by performing trend analysis, capacity planning and other reporting & analytical tasks.

4. DDOS Solution should support the following features

4.1. To detect and mitigate inbound DDoS attacks from External peering networks and in-house cross bound attacks. The proposed should detect and mitigate all types of inbound DDoS attacks into RAILTEL network from DDoS attacks from External Transit Network & domestic peering network. The objective is to protect RAILTEL network Servers, its Services including DNS,NTP and Data infrastructure and RAILTEL's subscriber's networks from Inbound DDoS attacks.

4.2. To detect Out-bound DDoS attacks emanating from RAILTEL existing subscribers into its Transit network &/ or Domestic Peering networks.

4.3. Hence to cover points above (1 & 2), all transit / peering Edge Routers to be covered. The proposed solution should protect the RAILTEL network & its subscribers from attacks ingressing the RAILTEL network

4.4. To detect cross bound DDoS attacks emanating from RAILTEL existing subscribers into its customers network. Railtel would like to protect critical enterprise customers from cross bound DDOS attacks also; hence solution should include monitoring critical Edge/Customer aggregation routers also.

4.5. However, the system should be scalable and seamless addition of components should be able to cover additional routers & expansion in future.

4.6. As additional Peering Routers or MPLS PE routers monitoring may be needed as the Network expansion or service coverage expansion happens over period of time, the system should be scalable by adding additional components without fork lift upgrades.

4.7. It is mandatory that the solution proposed should be capable of storing alert and traffic data for 1 year time, it should be possible to retrieve and analyze last one year data and alerts. Alerts & Traffic statistic data should be periodically backed up on an external storage system.

4.8. The Total Transit Bandwidth currently is 40 Gigs and is estimated to grow further. The total Intelligent DDoS Mitigation capacity currently required is 20 Gbps, the mitigation

capacity of 20 Gbps should be achieved using 2 Mitigation appliances working in Active /Active mode. The proposed Intelligent DDoS Mitigation appliance should be scalable/ Upgradable from 10 Gig to 40 Gig.

4.9. It should be noted that 10 Gbps mitigation capacity should be available per mitigation appliance from day1. If the deployment architecture proposed requires out-bound traffic also to pass thru the mitigation appliance then 20 Gbps mitigation capacity upgradeable to 80 Gbps per appliance should be proposed. All the countermeasures /filters/signatures available in the mitigation appliance should be supported in the deployment architecture proposed, if few countermeasures/ filters/signatures are supported in symmetric traffic environment then the solution should be proposed with mitigation appliance deployed to see both the side of the traffic.

4.10. Any external router if required for BGP route injection should be proposed. Please refer router specification. 2 routers should be proposed, one each for the mitigation appliance

4.11. The system should have ready built in UI for internal users and also provide scoped view to chosen RAILTEL subscribers so that the system is ready to offer Managed DDoS Mitigation services, if RAILTEL desires to do so.

4.12. It would be the responsibility of RAILTEL to provide the Vendors / System Integrators with essential inputs like IP Flow, Power, space etc. Vendors may assume that the requisite essential inputs for their system like IP Flow (Netflow, cFlowd/jflow or sflow as the case may be), SNMP & BGP information in addition to Rack, Space, Power, Interfaces, IP Addresses etc, is made available by RAILTEL.

4.13. To provide full scale Managed DDoS Services Portal/ UI access to subscribers and additional Mitigation capacity as may required with addition of subscribers.

4.14. To provide MPLS RFC2547 VPN traffic visibility as detailed in the specifications.

4.15. Solution should include internal/external Portal to provide Subscribers access/ DMZ access/ Portal Availability.

5. Technical Specification of DDOS Detector/Flow Collector System

5.1. Scale and Architecture

5.1.1. The system can be deployed in a matter that does not introduce an additional point of failure to the network.

5.1.2. The system scales to monitor interfaces at all speeds supported by the customer's routers

5.1.3. DDOS detection system should be a statistical anomaly detection engine working in an offline, pervasive monitoring mode.

5.1.4. The system scales to monitor interfaces at all speeds supported by the Railtel Data routers.

5.1.5. The solution should cater monitoring aggregated 6 Peering/Gateway Edge routers (scalable to 15) and 25 P/PE aggregation routers (scalable to 75).

5.1.6. The system must be able to accept Netflow data, (a) Jflow, (b)Cflow, (c)Sflow and (d)IPFix.

5.1.7. The system must be able to accept BGP routing table from all monitored routers in the network.

5.1.8. The system should support BGP flow spec or open flow.

5.1.9. The system must be able to poll monitored routers using SNMP v1, v2c or v3.
The system must provide IPv4 and IPv6 dual-stack support allowing for ping, traceroute, ssh, HTTPS, syslog, DNS, NTP, SNMP, and AAA (RADIUS only).

5.1.10. The system must be able to reflect/replicate received Netflow data and export it to other Netflow receivers in the network.

5.1.11. Once the DDoS solution has been procured for a specific number of routers, flexibility should be there to immediately change the routers within the range for which licenses have been procured.

5.1.12. Railtel requirement is 100K flows per second from Day-1 and deployment should support 250K FPS in future through license upgrade. Appliance should support the requirement for 250K FPS from Day-1. There should be option to increase the number of Flows per second through license upgrade. Appropriate appliances or VM licenses should be included in the proposal to support the upgradeability.

5.1.13. DDOS detection system deployment should be license upgradeable to support 15 Gateway routers & 75 P/PE aggregation routers. Appropriate appliances or VM licenses should be included in the proposal to support the upgradeability. .

5.1.14. The system must be able to accept Netflow data from Cisco routers, Cflowd from Juniper and Alcatel routers and Sflow data from Foundry or other Sflow based routers. The system must support Netflow versions 1, 3, 5, 7 or 9, Cflow versions 5, 9 and Sflow version 2, 4, 5 and IPFIX.

5.1.15. The system must be able to accept BGP route data from all monitored routers in the network.

5.1.16. The system must be able to poll monitored routers using SNMP v1,v2c or v3.

5.1.17. The system must provide IPv4 and IPv6 dual-stack support allowing for IPv6 for ping, traceroute, ssh, HTTPS, syslog, DNS, NTP, SNMP, and AAA (RADIUS only)

5.1.18. The system must be able to replicate (“tee”) received Netflow data and export it to other Netflow receivers in the network.

5.1.19. The system must be scalable to be able to monitor up to 2000 routers and 100,000 interfaces by adding additional detector appliances to the deployment.

5.1.20. The system must support explicit configuration of monitored interfaces

5.1.21. The system must support 1000 user-defined managed objects for traffic baselining and should be upgradable to 10000 user defined managed objects.

5.2. <u>System Security</u>

5.2.1. All external communication to the system must be managed through an internal packet filtering firewall that allows only those services that are explicitly enabled.

5.2.2. CLI access must be provided using SSH or optionally telnet.

5.2.3. Version of SSH used by the system must be configurable

5.2.4. The system must supply the full CLI interface via RS-232 serial console port or KVM console for on-site use.

5.2.5. GUI access to the system must be HTTPS. No unsecured GUI protocols must be permitted.

5.2.6. The system must allow for multiple levels of access including administrator and operator levels.

5.2.7. The system must allow for the creation of multiple users with differing group memberships allowing differing permission sets and UI skins.

5.2.8. The system must provide user-level access controls based on tokens assigned to users or groups of users to enforce privilege separation.

5.2.9. The system must provide full AAA to users via a local user table, RADIUS, TACACS, or a configured combination of methods.

5.2.10. The system must support a user configurable radius NAS identifier

5.3. User Interface

5.3.1. The system must have a web based GUI interface compatible with standard web browsers such as Internet Explorer, Firefox / Mozilla, Netscape, Opera etc.

5.3.2. The GUI must provide search functions to aid navigation when large numbers of routers, interfaces and/or managed objects are configured.

5.3.3. The GUI must provide search functions to aid navigation when large numbers of alerts are present in the system.

5.3.4. The system must provide on-line documentation in the GUI to help users understand the functions in each screen.

5.3.5. The system must provide near-real-time graphs and tables for traffic reporting and detected anomalies / alerts.

5.3.6. The system must provide bps and pps values for traffic reporting graphs (where appropriate)

5.3.7. The system must generate real-time or past detected anomaly reports in pdf or XML format.

5.3.8. The system must generate real-time or past traffic reports reports in pdf, XML or CSV format.

5.3.9. The system must provide the ability to customize application; ASN and ToS name number mappings.

5.3.10. The system must allow for customization of UI reports such that screens can be merged, and difference user views can be defined.

5.3.11. The system must provide a commit function to save changes to the configuration. The commit function must give the administrator the ability to add a comment or to view a diff of what is being changed.

5.3.12. The system must allow for configuration rollback to previous versions of the configuration or for a return to the last saved configuration

5.3.13. The system must show an audit trail for configuration changes that shows when changes were made and by whom.

5.3.14. The system must provide an XML/SOAP API for extracting report data and integration with other software/systems.

5.3.15. The system must support GUI for most of configuration

5.4. Status Monitoring and Alerting

5.4.1. The appliances must be SNMP pollable (v1, v2c or v3) for load information.

5.4.2. The system must provide the NetFlow, SNMP and BGP status for each router being monitored.

5.4.3. The system must allow the comparison for Flow and SNMP derived statistics for each interface, to help ensure flow data accuracy.

5.4.4. The system must be able to generate SNMP traps when netflow from a router is interrupted and restored.

5.4.5. The system must be able to generate an alert due to a system error/over-load condition, e.g. process error

5.4.6. The system must be able to provide SMTP based email alerts for severe anomalies, system events, or other traffic/routing issues.

5.4.7. The system must be able to generate SNMP traps and/or syslog messages to external monitoring systems for severe anomalies, system events, or other traffic/routing based issues.

5.4.8. The system must support rule based notification where administrators can define notification criteria based on resource and anomaly severity.

5.4.9. The system must provide access to a syslog file that can be used in troubleshooting issues.

5.4.10. The system must allow for manual or scheduled incremental backup of database information including export of backup data to a remote SCP server.

5.5. Network Threat Detection and Classification: Anomalies, Detection

5.5.1. The system must allow managed objects to be defined as one or more CIDR blocks, a BGP AS regular expression, one or more BGP peer ASNs, one or more BGP confederation sub ASNs or private ASNs, one or more BGP communities, one or more router interfaces, or a boolean combination of the above.

5.5.2. The system must allow managed objects to be defined as one or more IPv6 CIDR blocks.

5.5.3. The system must support a CIDR Group managed object that can specify multiple individual resources for separate baseline and anomaly detection. This managed object allows administrators to provide a common set of detection sensitivity and importance settings for a number of resources at once.

5.5.4. The system must allow Services to be defined on Applications and CIDR blocks.

5.5.5. The system must be able to detect bandwidth, packet and or protocol anomalies towards/from defined managed objects and services in the system, including IPv6 managed objects.

5.5.6. The system must be able to baseline traffic to/from a configured managed object or service and dynamically learn long-term changes in expected traffic as changes occur, including IPv6 managed objects.

5.5.7. The system must determine the importance of anomalies based on impact to network. At least three importance levels must be supported: low/green, medium/yellow and high/red severity, including IPv6 managed objects.

5.5.8. The system must provide flexible ways of setting severity classification thresholds for managed objects and services including: manual configuration by the user; automatic calculation by the system based on applying user specified criteria to normal traffic levels seen for that managed object.

5.5.9. The system must allow users to set detection threshold per managed object or service for bandwidth, protocol and packet detection, including IPv6 managed objects.

5.5.10. The system must support misuse anomaly detection by tracking and alerting when certain traffic patterns towards individual hosts exceed what is considered normal Internet usage. These traffic patterns include TCP SYN, TCP RST, TCP Null, ICMP, IP Null, IP Fragmented, DNS, UDP and IP private address traffic, including traffic to/from IPv6 hosts.

5.5.11. The system clearly identifies the start time and duration of an anomaly, its type, importance, on-going traffic pattern, and the managed object under threat if applicable.

5.5.12. The system must display the overall impact of an anomaly, as well as on a per-interface basis by bit rate and packet rate.

5.5.13. The system must show a basic characterization of the anomaly showing what components were predominant. These must include IPv4/IPv6 address blocks, IP protocols, IP protocol ports or types, and TCP flags, and must include both source and destination components.

5.5.14. The system must identify all monitored routers affected by a network anomaly, and each affected ingress router interface

5.5.15. The system must display anomaly details for the entire anomaly or for any minute of time during that anomaly.

5.5.16. The system must provide IP address identification using WHOIS lookups and/or DNS resolution.

5.5.17. The system must allow users to classify an anomaly, choosing from pre-defined options e.g. Possible Attack, False Positive etc.

5.5.18. The system must allow for automatic download of fingerprints from a central server. These fingerprints will point out specific threats that are active within the monitored network.

5.5.19. The system must give users the ability to create a Fingerprint object based on a user defined FCAP.

5.5.20. The system must give users the ability to set high / low thresholds for alerting on traffic which matches a Fingerprint object at the network border.

5.5.21. The system must generate Fingerprint alerts, when a threshold is violated showing: a summary of traffic matching the Fingerprint, traffic per Peer, traffic per Customer and a list of top hosts responsible for the traffic matching the fingerprint.

5.5.22. Unused address space used by the system for Dark IP detection must be configurable. The system must enable administrators to specify both source and destination CIDRs on which to match Dark IP.

5.5.23. The system must be able to monitor and display data for traffic flows destined for specified unused "Dark IP" addresses. Traffic levels, traffic levels per customer, and top infected hosts must be reported.

5.5.24. Dark IP detection must alert when traffic matching destined for unused address space exceeds configured traffic thresholds.

5.5.25. The system must be capable of providing alerts when an interface exceeds a configurable percentage of utilization.

5.5.26. The system must be capable of providing alerts when an interface goes below a configurable percentage of utilization.

5.5.27. The system must be capable of providing alerts when traffic matching a Managed Object exceeds a configurable utilization threshold.

5.5.28. The system must be capable of providing alerts when traffic matching a Managed Object goes below a configurable utilization threshold.

5.5.29. The system must be capable of providing alerts for routing instability when a configurable number of BGP update/topology changes are seen per five-minute period per router.

5.5.30. The system must be capable of providing an alert if a BGP peer announces a route that is local to the network.

5.6. <u>Traffic/Routing Measurement & Reporting: Generic</u>

5.6.1. The system must be able to track and correlate BGP routing with traffic flows in order to accurately classify router interfaces as network internal, external and backbone.

5.6.2. The system must be able to use regular expression matching on interface descriptions to classify interfaces as network internal, external, and mixed or backbone.

5.6.3. The interface classification must be customizable by the user.

5.6.4. The system must be able to monitor and track traffic and BGP routing information across all monitored routers and their associated interfaces, and accurately report incoming, outgoing, multicast and backbone traffic rates (as appropriate)

5.6.5. The system must provide graphical representations of traffic over time for variable time periods of up to three years.

5.6.6. The system must provide the ability to report on QoS information, including: ToS; ToS DTRM; IP Precedence; DSCP. For the Network as whole, per router, per interface and per Managed Object.

5.6.7. The system must provide the ability to report on Multicast traffic including breakdowns for: Packet Size; Protocol; Managed Objects; Infrastructure; Top Talkers.

5.6.8. The system must provide TCP/UDP Port reports for IPv6 traffic (Netflow v9 IPv6 template data required).

5.6.9. The system must provide IPv6 Top Application reporting.

5.6.10. The system must provide MPLS reports that allow tracking of MPLS vs IPv4 traffic (NetFlow v9 IPv6 template data required).

5.6.11. The system must provide MPLS reports that allow tracking of QoS per MPLS tunnel using the EXP bit for IPv4/IPv6 traffic (NetFlow v9 IPv6 template data required).

5.6.12. The system must provide PE traffic distribution reports for MPLS tunnels in IPv4/IPv6 environments (NetFlow v9 IPv6 template data required).

5.6.13. The system must be able to correlate flow data from each router with the BGP information gathered from the router. The system must be able to provide reports on BGP attributes including: Origin/Peer/All ASN; NextHops. For Managed Objects.

5.6.14. The system must have the ability to provide reporting based upon IPv6 BGP AS_PATH information.

5.6.15. The system must have the ability to provide reporting based upon IPv6 BGP-based managed objects.

5.6.16. The system must be able to report on Applications based on one or more TCP/UDP ports.

5.6.17. The system must support FCAP, where fingerprints can be defined manually

5.6.18. The system must report on traffic matching defined Dark IP address space including: Summary of Traffic; List of Suspicious hosts.

5.6.19. The system must monitor and track BGP updates in the network, by router, and by peer.

5.6.20. The system must provide the reporting capabilities to see BGP updates in a particular moment in the past, or over a defined period of time within the last three months.

5.6.21. The system must provide the reporting capabilities to analyse route instability for given router(s) over a given time period in the last three months, filtered by more/less/exact prefix, asregexp, community.

5.6.22. The system must provide the ability to create customized traffic/routing reports including any data that is available within the system.

5.6.23. The system must provide a mechanism to generate customized reports that run on a recurring basis.

5.6.24. The system must provide actual samples of Netflow for the most recent collection period for routers, interfaces and managed objects.

5.6.25. The system must have the ability to adjust the backend databases and the UI to only track and display the data that is relevant to the user.

5.6.26. The system must provide a mechanism for querying the BGP route tables of other network service providers.

5.7. Traffic/Routing Measurement & Reporting: Peering Evaluation & Traffic Engineering

5.7.1. The system must demonstrate how incoming and outgoing traffic rates / BGP prefixes learned vary by configured Peer object.

5.7.2. The system must show AS distance characteristics for traffic exchanged with each configured Peer object.

5.7.3. The system must report on BGP learned prefixes and instability per configured Peer object

5.7.4. The system must provide the tools necessary to evaluate/compare existing peering relationships and determine viable new peering partners.

5.7.5. The system must provide data that will allow users to predict the effects of changing peering relationships.

5.7.6. The system must report on traffic between peers and other managed objects including customers, profiles and other peers.

5.7.7. The system must have the capability of reporting on traffic between managed objects i.e. customer x customer, profile x profile, etc.

5.7.8. The system must have the capability of reporting on Service and Fingerprint traffic per Customer and Profile Managed Object (and vice versa).

5.7.9. The system must have the capability of tracking both local and remote BGP attributes for Customer, Peer Managed Objects and Interfaces including: Next-Hop, Communities; Origin|All|Peer ASN.

5.7.10. The system must have the ability to perform 4-byte ASN managed object matching.

5.7.11. The system must have the ability to provide 4-byte ASN traffic reports.

5.7.12. The system must have the ability to perform 4-byte ASN route analytics.

5.7.13. The system must have the capability of reporting on As_Path and BGP prefix information for the Network, per router, per interface and per Peer Managed Object.

5.7.14. The system must be capable of tracking the top AS x AS combinations for traffic on the network.

5.8. Traffic/Routing Measurement & Reporting: MPLS VPN Reporting

5.8.1. The system must provide total traffic for each MPLS RFC2547 VPN defined with a set of boundary interfaces and an optional route distinguisher.

5.8.2. The system must provide traffic reports for packet size spread, Protocols, TCP/UDP ports and ICMP type, per VPN and VPN Site.

5.8.3. The system must provide a traffic report for each interface defined as a portion of the MPLS rfc2547 VPN.

5.8.4. The system must provide the ability to report on QoS information, including: ToS; ToS DTRM; IP Precedence; DSCP. For the VPN as whole and per VPN Site.

5.8.5. The system must provide MPLS COS reports for the entire MPLS rfc2547 VPN defined within the system and also for each individual MPLS VPN site.

5.8.6. The system must provide a report for traffic from site to site within any given MPLS rfc2547 VPN defined within the system.

5.9. Portal/User interface Services

5.9.1. The system must provide the capability for a customized web portal login page. Portal Interface should be provisioned with 25 simultaneous login sessions to the DDOS detection and mitigation system from Day 1 and should be scalable.

5.9.2. The system must allow the configuration of Resource Groups which can be assigned to User Account Groups. Resource Groups define the Managed entity(s) which scope a user login.

5.9.3. The system must allow the assignment of customized UI views to User Account Groups.

5.9.4. Portal users must be limited to a scoped view of the traffic monitored by the system. Only traffic / alert information relevant to the assigned Managed entity(s) will be visible.

5.9.5. Portal users must be able to change their own password.

5.9.6. Portal administrator users must be able to create profiles within their scoped view.

5.9.7. Portal users must be able to create detection groups with specific detection settings within their scoped view.

5.9.8. Portal users must be able to view traffic reports for their scoped view and their configured profiles including application, protocol and top talker reports.

5.9.9. Service Portal users must be able to view all on-going and recent anomalies from within their scoped view.

5.9.10. Service Portal users must be able to view all on-going and recent mitigations, relevant to associated Managed entity(s), from within their scoped view.

5.9.11. Service Portal users must be able to view all system alerts, network and infrastructure traffic reports. Managed entity reports should be constrained to the specified Resource Group Monitored entities.

5.9.12. The system must provide a Customer Alert Dashboard summarizing alert activity relevant to the portal user. The Dashboard must be viewable by the system administrator as well as the portal user.

5.9.13. Portal users must be able to delete anomalies from within their scope.

5.9.14. Portal administrator users must be able to create other portal user accounts.

5.9.15. Portal users must be able to save configuration changes made to the system within their scoped view.

5.9.16. The system must provide a Portal or scoped view for each of the defined MPLS rfc2547 VPNs within the system.

5.9.17. Portal users must be able to view details of their MPLS rfc 2547 VPN, including Site x Site traffic, Site comparison reports, Total application traffic and total traffic reports for the VPN.

5.10. MSSP Services

5.10.1. The system must provide the capability for a customized web portal login page.

5.10.2. The system must allow the configuration of Resource Groups which can be assigned to User Account Groups. Resource Groups define the Managed Object(s) which scope a user login.

5.10.3. The system must allow the configuration of both Managed Service and non-Managed Service Resource Groups.

5.10.4. The system must allow the assignment of customized UI skins to User Account Groups.

5.10.5. Portal users must be limited to a scoped view of the traffic monitored by the system. Only traffic / alert information relevant to the assigned Managed Object(s) will be visible.

5.10.6. Portal users must be able to change their own password.

5.10.7. Portal administrator users must be able to create profiles within their scoped view.

5.10.8. Portal users must be able to create detection groups with specific detection settings within their scoped view.

5.10.9. Portal users must be able to view traffic reports for their scoped view and their configured profiles including application, protocol and top talker reports.

5.10.10. Managed Service Portal users must be able to view all on-going and recent anomalies from within their scoped view.

5.10.11. Managed Service Portal users must be able to view all on-going and recent mitigations, relevant to associated Managed Object(s), from within their scoped view.

5.10.12. Non Managed Service Portal users must be able to view all system alerts, network and infrastructure traffic reports. Managed Object reports should be constrained to the specified Resource Group Managed Objects.

5.10.13. Portal administrator users must be able to create other portal user accounts.

5.10.14. The system must provide a Portal or scoped view for each of the defined MPLS rfc2547 VPNs within the system.

5.10.15. Portal users must be able to view details of their MPLS rfc 2547 VPN, including Site x Site traffic, Site comparison reports, Total application traffic and total traffic reports for the VPN.

6. Technical Specification of DDoS Mitigation System

6.1. Scale and Architecture

6.1.1. The system must be deployable without introducing an additional point of failure to the network

6.1.2. External router could be proposed if the mitigation appliance does not support BGP route injection. 2 Routers should be proposed, specification mentioned in Appendix-A. The technical specification for DDOS mitigation appliance hence required as mentioned below should be achievable by the external router proposed

6.1.3. The system must provide two interfaces at speeds of 10Gbps SFP+/XFP based interface. Single mode 1310 nm sfp+/xfp for 10Gbps interface should be provided with interfaces.

6.1.4. The system must allow creation of logical ‘link bundle’ interfaces by grouping multiple physical interfaces together.

6.1.5. The system must allow creation of VLAN sub-interfaces on physical and / or logical interfaces.

6.1.6. The DDOS mitigation appliances should be completely stateless, it should also support asymmetrical traffic flow

6.1.7. The system must be able to directly BGP peer with multiple switches/routers in the network.

6.1.8. The system must support the BGP MD5 option for secure BGP sessions.

6.1.9. The system must be able to send BGP route updates from within the same AS

6.1.10. The system must be able to send BGP route updates to a peer in a remote AS.

6.1.11. The system must be able to re-inject traffic via multiple GRE tunnels based on ultimate destination

6.1.12. The system must support redundant GRE tunnels for re-inject traffic.

6.1.13. The system must support adjustable per-GRE Tunnel MTU size.

6.1.14. The system must support VLANs for mitigation, re-injection, and diversion of traffic.

6.1.15. The system must be able to re-inject traffic in native IP to the next-hop switch/router

6.2. Management

6.2.1. The system must provide on-line documentation in the GUI to help users understand the functions in each screen.

6.2.2. The system GUI must allow for multiple levels of access including administrator and operator levels.

6.2.3. The system must provide a CLI interface that provides system monitoring functions.

6.2.4. The system must provide SYSLOG, SNMP or SMTP notifications for the starting and stopping of mitigations.

6.3. Security

6.3.1. All external communication to the system must be managed through an on-board packet filtering firewall that allows only those services that are explicitly enabled.

6.3.2. CLI access must be provided using SSH or optionally telnet.

6.3.3. GUI access to the system must be HTTP/S. No unsecured GUI protocols must be permitted.

6.3.4. The system must allow for configuration of multiple local user accounts

6.3.5. The system must provide user-level access controls based on tokens assigned to users or groups of users to enforce privilege separation.

6.3.6. The system must provide IP Access Control lists for all remote services that are accessible.

6.3.7. The system must provide full AAA to users via a local user table, RADIUS, TACACS, or a configured combination of methods.

6.4. Performance

6.4.1. The mitigation appliance should support multiple 10 Gig interfaces for traffic diversion and re-injection

6.4.2. Mitigation system available should have a mitigation capacity of 10Gbps per appliance scalable up-to 40Gbps mitigation throughput per appliance. Total of 20 Gbps mitigation capacity needs to be provisioned equally distributed between 2 security centers. Minimum 2 Mitigation appliances should be proposed in the solution.

6.4.3. Mitigation appliance should be proposed in architecture to support all countermeasures/filters/signatures available with the product. If the product supports few countermeasures/filters/signatures in only bi-directional traffic mode where-in the mitigation appliance is required to see the outbound traffic also, then the solution should be proposed in bi-directional traffic mode. In that case, proposed appliance should support 20 Gbps mitigation capacity from day-1 and should be upgradeable to 40 Gbps mitigation capacity.

6.4.4. System should be capable of supporting at least 25 simultaneous on-going mitigations and scalable to 50 simultaneous on-going mitigations.

6.4.5. The system must be able to support up to 10k entries in the global whitelist

6.4.6. The system must be able to support up to 10k entries in the global blacklist

6.4.7. The system must be able to support up to 1000 entries in a black / white list per mitigation

6.4.8. The system must support up to 1000 interfaces configured as physical, logical or sub-interfaces

6.4.9. The appliance must support minimum 20 Million packets per second

6.4.10. The system must be able to support up to 1000 GRE tunnels per device.

6.4.11. The Mitigation system should support MPLS layer 3 VPN.

6.4.12. The Mitigation system should support BGP flow spec or open flow

6.4.13. The Mitigation system should support redirection of traffic through a VRF & rate limit action using BGP flow spec.

6.4.14. The Mitigation system should have a programme capability through dynamic installation of rules to drop the traffic, inject it in different VRF & also have capability to police the traffic at defined rate

6.4.15. The System should Support for 100 GE Interface

6.4.16. The System should Capable of rate limiting in the hardware.

6.4.17. The System should capable to maintain traffic symmetry

6.5. User Interface

6.5.1. The system must support configuration via a secure SSL based GUI interface compatible with standard web browsers.

6.5.2. The system must have a CLI interface accessible via the network using a standard secure protocol such as SSH.

6.5.3. The system must provide a graph showing the amount of mitigation capacity used over the last 24 hours.

6.5.4. The system must provide a dashboard for all mitigations devices on a single page showing running mitigations, traffic received, flow sent, CPU load and memory usage per device.

6.5.5. The system must display near real-time statistics on the amount of dropped and passed traffic during an active mitigation in total.

6.5.6. The system must display real-time statistics on the amount of dropped and passed traffic during a manual or automatically started mitigation, per countermeasure

6.5.7. The system must display real-time statistics on the amount of dropped and passed traffic during a manual or automatically started mitigation, per device if there are multiple devices being used.

6.5.8. The system must annotate mitigations whenever they are started / stopped or a configuration change is made.

6.5.9. The system must allow mitigation parameters to be changed while mitigation is running.

6.5.10. The system must allow mitigation parameters to be changed across multiple mitigation devices from a single UI.

6.5.11. The system must support capturing and viewing sample packets of mitigation traffic per device during mitigation.

6.5.12. The system must support decoding of sample packets and indication of passed / dropped status.

6.5.13. The system must support the downloading of sample packets in PCAP format.

6.5.14. The system must support viewing prior mitigation reports that show the full summary of the mitigation, including configuration changes etc..

6.5.15. The system allows for creation of mitigation templates. Mitigation templates can be associated to specific Managed Objects and facilitate the mitigation workflow.

6.5.16. The system supports the ability to do auto-mitigation. Auto-mitigation can be globally enabled or disabled, as well as on a per Managed Object basis.

6.5.17. The system must support the ability to restrict managed services end-customer users to a read-only view of active mitigations, allowing them to view mitigation statistics but not to configure/alter mitigation settings.

6.5.18. The system must supply the full CLI interface via serial console port.

6.6. Mitigation

6.6.1. Upon user request, the system must be able to inject BGP routes into the network to mitigate an attack by diverting traffic to itself for the prefix being attacked.

6.6.2. BGP route injection must be configurable for one or more routers and users must have the ability to tag the prefix with a specific next-hop or community attribute.

6.6.3. The system must be able to block Invalid Packets (Bad Checksum, Malformed Header, Incomplete Fragment, Duplicate Fragment, and Short Packet) and provide statistics for the packets dropped.

6.6.4. The system must evaluate traffic during mitigation and drop/pass packets based on an operator configurable exception list.

6.6.5. The system must be able to block traffic matching specific Fingerprints describing potentially malicious activities generated by a dedicated research organization.

6.6.6. The system must be able to drop packets of specified TCP ports with payloads matching or not matching a configurable regular expression.

6.6.7. The system must be able to drop packets of specified UDP ports with payloads matching or not matching a configurable regular expression.

6.6.8. The system must be able to drop specific HTTP packets with HTTP headers matching or not matching up to 5 configurable regular expressions.

6.6.9. The system must be able to “AND” or “OR” the HTTP Regular expressions per mitigation.

6.6.10. The system must be able to drop specific DNS packets with DNS requests matching or not matching up to 5 configurable regular expressions.

6.6.11. The system must be able to “AND” or “OR” the DNS Regular expressions per mitigation.

6.6.12. The system must support the dropping of idle TCP sessions with a user-configurable timeout period.

6.6.13. The system must support the dropping of idle TCP sessions if client does not send a user-configurable amount of data within a configurable time period.

6.6.14. DDoS detection and Mitigation system should support remote trigger black holing to inject Null route on RailTel peering routes. This is required for very high volume DDoS attack mitigation at RailTel.

6.6.15. The system must support the ability to blacklist a host after user-configurable number of consecutive TCP idles.

6.6.16. The system must have a TCP SYN authentication countermeasure available.

6.6.17. The TCP SYN Authentication countermeasure must be able to specify Source and/or Destination TCP Ports to be ignored.

6.6.18. The TCP SYN authentication countermeasure must provide a way not to impact on users’ legitimate HTTP sessions via subsequent HTTP re-direction.

6.6.19. The TCP SYN authentication countermeasure must provide an out-of-sequence ACK mechanism for use in protecting TCP-based applications which are sensitive to an RST sent to clients.

6.6.20. The TCP SYN authentication countermeasure must provide a fall back mechanism from the out-of-sequence ACK mechanism to the standard SYN authentication countermeasure in the event of TCP sequence number filtering on client networks.

6.6.21. The system must have a DNS authentication countermeasure available.

6.6.22. The system must have a malformed DNS countermeasure available.

6.6.23. The system must be able to provide DNS authentication through passive authentication timer.

6.6.24. The system must be able to provide DNS Authoritative Server countermeasure through active challenges to client.

6.6.25. The system must be able to limit the number DNS Queries per second by a user-configurable rate.

6.6.26. The system must be able to limit the number of DNS NXDomain failed queries per second by a user-configurable rate.

6.6.27. The system must have the ability to make use of up to five regexp-based expressions to determine domain scoping classification for the DNS Authentication, DNS Query Rate-Limiting, DNS NX Domain Rate-Limiting, and DNS Regular Expression countermeasures.

6.6.28. The system must be able to detect and drop malformed HTTP packets.

6.6.29. The system must be able to block hosts exceeding a configurable threshold for total number of HTTP operations per second, per destination server.

6.6.30. The system must be able to block hosts exceeding a configurable threshold for number of HTTP operations per URL, per second, per destination server.

6.6.31. The system must have the ability to make use of up to five regexp-based expressions to determine domain scoping classification for the HTTP Request Limiting, HTTP Object limiting, and HTTP Header Regular Expression countermeasures.

6.6.32. The system must be able to detect and drop malformed SIP packets.

6.6.33. The system must be able to block hosts exceeding a configurable threshold for total number of SIP operations per second, per destination server.

6.6.34. The system must allow for zombie host detection (compromised hosts involved in an attack) to be enabled/disabled and zombie host thresholds (bps or pps) to be configured per mitigation.

6.6.35. The system must detect zombie hosts and add them to the blacklist. The system must update the zombie army list in real time and provide a report detailing the zombie army detected.

6.6.36. The system must allow for protocol baseline enforcement to be enabled/disabled per mitigation. The system must have the ability to continually and passively learn protocol traffic baselines for the network.

6.6.37. The system must be able to rate limit the traffic matching a configurable FCAP expression to a configurable bps or pps threshold.

6.6.38. The system must have the ability to perform learning mitigations in order to generate appropriate traffic thresholds for managed objects.

6.6.39. The system must have the ability to automatically create and start mitigation for traffic destined to a managed object.

6.6.40. The system must have the ability to create auto-mitigations with multiple prefixes when more than one prefix is cited in an alert.

6.6.41. The system must have the ability to create filter lists based upon IP ranges, FCAP expressions, URLs (for applicable countermeasures), and/or FQDNs (for applicable countermeasures) in order to include/exclude traffic from evaluation and filtering on a per-countermeasure basis.

6.7. Fault Tolerance

6.7.1. The system must generate SNMP traps for GRE tunnel and other re-injection failures.

6.7.2. The system must be configurable to start / not start mitigation if all selected devices (in a group) are not up.

6.7.3. The system must be configurable to start / not start mitigation if all selected device (in a group) do not have all of their BGP peering sessions established.

6.7.4. The system must be configurable to start / not start mitigation if all selected devices (in a group) do not have available bandwidth.

6.7.5. The system must be configurable to stop / not stop a running mitigation if the device involved in the mitigation becomes unreachable from the management system.

6.7.6. The system must be configurable to stop / not stop a running mitigation if the device interface or BGP peering session fails.

6.7.7. The system must be configurable to stop / not stop a running mitigation if a re-inject next-hop or GRE tunnel becomes unavailable.

6.7.8. The system must generate SNMP traps for system faults.

6.7.9. The system must provide access to a syslog file that can be used in troubleshooting issues.

6.7.10. System must provide fault messages in the central UI console.

6.8. Router specification (Required if non-router based mitigation solution is quoted)

6.8.1. Router shall have modular configuration so that different modules can be added to it and shall also have modular Operating system.

6.8.2. Router shall have option checking configuration before committing and option of rolling back to at least five configurations.

6.8.3. Router shall have 60 Gbps backplane capacity and shall have 4x10G ports and 20 x1G SFP based ports .

6.8.4. 10 GE Interfaces shall support both WAN PHY and LAN PHY.

6.8.5. Shall support DC redundant power supply.

6.8.6. The proposed router should support synchronization protocols like SyncE & 1588v2 PTP on Ethernet interfaces

6.8.7. For each Type-D Router, bidder has to quote Ten SFPs each of GE single mode 1550 nm/10 kms and Two SFPs each of 10GE single mode 1550 nm/10 kms.

6.8.8. FIB capacity of 1 Million and RIB capacity of upto 4 Million for IPv4 routes

6.8.9. The router shall support 512K IPv6 FIB

6.8.10. 2K L3VPN VRF and 4K VPLS routing-instances and MAC scaling of 512K MAC

6.8.11. All 1 Gige and 10 Gige interfaces shall support services like L2VPN, L3VPN ,VPLS and multicast VPN for both IPv4 and IPv6 with line rate throughput.

6.8.12. The 1 Gige/10 Gige interfaces shall be WAN type interfaces meaning that VLANs can be reused on different 1gige interfaces.

6.8.13. The router shall have minimum 2GB RAM and compact flash with at least 4GB HD

6.8.14. The router should have redundant DC power supplies with the operating range of -40 to -72 VDC

6.8.15. Shall support both IPv4 and IPv6 from day one.

6.8.16. Shall support QoS, option of traffic shaping per Interface based.

6.8.17. Shall support at least 8 Queues per Interface

6.8.18. Shall support ingress policing, marking and shaping on all the interface and Router Hardware should support 128 k hardware queues.

6.8.19. Shall support following class of service features:

6.8.19.1. Policing
6.8.19.2. Rewrite
6.8.19.3. Two-rate tri-color marking
6.8.19.4. Classification
6.8.19.5. Filtering
6.8.19.6. It shall be possible to configure multiple forwarding classes for transmitting packets.
6.8.19.7. Manage congestion using a random early detection (RED) algorithm
6.8.19.8. RFC 2474, Definition of the Differentiated Services Field in the IPv4 and IPv6 Headers
6.8.19.9. RFC 2597, Assured Forwarding PHB Group
6.8.19.10. RFC 2598, An Expedited Forwarding PHB.
6.8.19.11. RFC 2698, A Two Rate Three Color Marker
6.8.19.12. Router should be able to classify based on 802.1ad, 802.1p, EXP, TOS and DSCP bits.

6.9. Software Feature support for Type A,B,C and D

6.9.1. The router shall support aggregated Ethernet and it shall be possible to bundle upto 16 links.

6.9.2. Shall support following MPLS features

a) LDP and RSVP signaling
b) RFC 3036, LDP Specification
c) RFC 3212, Constraint-Based LSP Setup using LDP (Optional)
d) RFC 3215, LDP State Machine (Optional)
e) RFC 3478, Graceful Restart Mechanism for LDP

6.9.3. MPLS-TE and FRR

a) RFC 2858, Multiprotocol Extensions for BGP-4 (Optional)
b) RFC 3063, MPLS Loop Prevention Mechanism (Optional)
c) RFC 3031, Multiprotocol Label Switching Architecture (provides a good overview of MPLS)
d) RFC 3032, MPLS Label Stack Encoding (Optional)
e) RFC 3140, Per Hop Behavior Identification Codes (Optional)
f) Pseudo wire support
g) L3VPN , L2VPN and VPLS

6.9.4. Support for P and PE router functionality for MPLS on the same router simultaneously and on all the interfaces

(i) The router should be able to do load-balancing over multiple equal cost MPLS LSP
(ii) The router should support traffic engineering extensions to setup constraint path for LSP
(iii) The Router shall support MPLS Fast Reroute both link protection and Node protection.
(iv) The MPLS LSP should support features like Diffserv-TE and Auto bandwidth LSP (Optional)
(v) MPLS Ping, MPLS Trace Route
(vi) ICMP Extensions for Multi-protocol Label Switching (Optional)
(vii) Fast Reroute Extensions to RSVP-TE for LSP Tunnels
(viii) MPLS Label Stack Encoding
(ix) The router shall Support of Sync-E technology
(x) Shall support MPLS based VPN services

a) L3VPN,L2VPN (Kompella BGP/ Martini LDP),

b) VPLS (BGP/LDP)

c) Internet draft, draft-ietf-l2vpn-vpls-bgp-08.txt, *Virtual Private LAN Service (VPLS) Using BGP for Auto-discovery and Signaling* (Optional)

d) RFC 4762 (FEC 128, control bit 0, and Ethernet pseudo wire type hexadecimal 0x0005), *Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling* (Optional).

e) Next Generation mVPN (P2MP) based on (Draft-ietf-13vpn-2547bis-mcast-01.txt) & mVPN (draft-rosen-vpn-mcast).

(xi) The router shall support the following routing features

a. BGPv4, BGP confederations and route reflector
b. Dynamic Host Configuration Protocol (DHCP)
c. RFC 1587, The OSPF NSSA Option
d. RFC 2328, OSPF Version 2
e. RFC 2370, The OSPF Opaque LSA Option (support provided by the RSVP update-threshold configuration option)
f. RFC 2740, OSPF for IPv6
g. RFC 3101, The OSPF Not-So-Stubby Area (NSSA) Option
h. RFC 3137, OSPF Stub Router Advertisement
i. RFC 3623, OSPF Graceful Restart
j. RFC 3630, Traffic Engineering (TE) Extensions to OSPF Version 2
k. RFC 1195, Use of OSI IS-IS for Routing in TCP/IP and Dual Environments
l. RFC 2104, HMAC: Keyed-Hashing for Message Authentication
m. RFC 2763, Dynamic Hostname Exchange Mechanism for IS-IS.
n. RFC 2966, Domain-wide Prefix Distribution with Two-Level IS-IS.
o. RFC 2973, IS-IS Mesh Groups
p. RFC 3277, IS-IS Transient Black hole Avoidance
q. RFC 3358, Optional Checksums in IS-IS.
r. RFC 3359, Reserved Type, Length and Value (TLV) Code points in IS-IS.
s. RFC 3373, Three-Way Handshake for IS-IS Point-to-Point Adjacencies
t. RFC 3784, IS-IS Extensions for Traffic Engineering
u. RFC 3787, Recommendations for Interoperable IP Networks Using IS-IS
v. RFC 3847, Restart Signaling for IS-IS
w. RFC 3212, Constraint-Based LSP Setup using LDP
x. RFC 2327, SDP: Session Description Protocol
y. RFC 3590, Source Address Selection for Multicast Listener Discovery Protocol
z. RFC 2974, Session Announcement Protocol
aa. RFC 3208, PGM Reliable Transport Protocol Specification

(xii) IGMP v2 and v3 as described in RFC 2236 and RFC 3376 (optional) with IGMP Routing Policies to filter IGMP requests.

(xiii) The router shall support Virtual Router Redundancy Protocol (VRRP) as per IETF RFC 3768

(xiv) Router shall support SNMP v2/v3 and NTP

(xv) It shall be possible to have role based privileges for the system access and radius authentication for the System admin.

(xvi) The router should have a Console or Out-of –band Management

(xvii) Shall support BFD

(xviii) Shall support the following OAM features

a) 802.3ah
b) 802.1ag
c) Y.1731

(xix) Shall support Multi-chassis LAG

(xx) Shall support GRE, IP-IP and IP multicast PIM SM, SSM

(xxi) **Shall support NATTING SYSTEM for Type- B and C:**-The router should be capable of large scale NAT features like NAT44 and NAT64 all configured at the same time with at least 5 Million concurrent sessions. The NAT scale should be 8Gbps per System. Any license and hardware required shall be quoted in the tender response as optional (SOR-D). RailTel may implement the same within one or two year of commissioning of the Network.

(xxii) IPv6 Features

a. IPv6 ping
b. IPv6 trace route
c. Stateless Auto configuration
d. RIPng
e. OSPF v3
f. IPv6 L3 forwarding in HW
g. IS-IS
h. VRRPv6
i. IPv6 CoS (BA, MF classification & rewrite, scheduling based on TC).
j. IPv6 ACL
k. 6PE and 6VPE

(xxiii) Multicast Feature: It shall support following:

a. It shall support IGMP snooping v2 and field upgradeable to v3 as and when desired by RAILTEL as described in RFC 1112, RFC 2236, and RFC 3376 with IGMP Routing Policies to filter IGMP requests.
b. The router shall support Mode, RFC 4601
c. Rendezvous Point (RP) - ability to be configured as an RP
d. RFC 3569, Source Specific Multicast (SSM) to ensure that no user initiates a source within the multicast domain and limit users only to the range of multicast address in SSM.
e. Dynamic broadcast Source Failover using Anycast routing
f. RFC 2365, Administratively Scoped IP Multicast
g. RFC 3446, Anycast Rendezvous Point (RP) Mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP).
h. RFC 3618, Multicast Source Discovery Protocol (MSDP).
i. Following features shall be supported as per IETF draft. Support for the standardized version of the draft shall be provided within six months of standardization:
j. Multicast in MPLS VPN
k. Bootstrap Router (BNG) Mechanism for PIM Sparse Mode
l. Source Specific Multicast for IP
m. "If some of the multicast features are not supported at day one, same shall be made available free of cost within 6 months from the date of Purchase Order."

(xxiv) Modular Operating System: the routers shall have a modular operating system. It shall support the following features.

a. The modular operating system shall be able to restart different modules (routing, SNMP, class of service) individually. This shall help provide better availability of system since a failure or restart of one module shall not affect the whole system.
b. Modular OS should also allow to upgrade an OS module without rebooting the system, and allow RAILTEL to make upgrades to the software
c. Individual restart of most modules and processes without affecting other processes or rebooting the entire operating system
d. The modular OS should support the routing protocols, interface management, chassis management, and SNMP management each execute as independent processes.

(xxv) Regulatory Compliance

(i) NEBS GR-63-Core:NEBS, Physical Protection, GR-1089-Core:EMC and Electrical Safety for Network Telecommunications Equipment
(ii) ETS-300386 Telecommunication Network Equipment Electromagnetic Compatibility Requirements
(iii) The operating system of the router series or the router shall have Common criteria EAL2 or higher certification from authorized agencies.
(iv) EMC
   a. AS/NZS 3548 Class A (Australia/New Zealand)
   b. EN 55022 Class A Emissions (Europe)
   c. FCC Class A (USA)

7. TENDERER's Responsibility

The tenderer will be responsible for supply & Installation and Commissioning of complete work for this tender including the System design of network and integration with the existing network, wherever required. It shall be the responsibility of Supplier to transport the equipment to site for the Installation & Commissioning.

7.1. OUTSIDE PLANT ACCEPTANCE

The tenderer should check and ascertain that the 230V AC power supply and earthing arrangement (value less than one ohm) existing at the respective nodes meet the requirement of equipment proposed to be installed. Augmentation required if any may be clearly brought out by tenderer.

7.2. INSTALLATION, INTEGRATION, TESTING, TRIAL RUN AND COMMISSIONING OF EQUPEMENTS NETWORK

The Tenderer shall be fully responsible for Quality Assurance of equipment & other network elements and supervision of following:-

7.2.1. Installation and integration of the above said equipment/ items as per System design
7.2.2. Integration with existing network
7.2.3. Testing of the Solution as specified in the document
7.2.4. Trial run of the Solution.
7.2.5. Commissioning of Solution.

7.3. TRAINING OF PURCHASER'S PERSONNEL

Training on the equipment and network operation shall be provided by the Tenderer During execution of the supplies covered in the SOR in the field, the tenderer shall undertake to train RailTel engineers and other Railway staff nominated by the RailTel in different aspects of equipment designs, functioning, field installation, testing, commissioning, operation, maintenance and repair, covering both hardware and software. The training should be comprehensive for transfer of complete know-how so as to impart full knowledge and competence to independently and successfully execute the installation, operation, user related software changes, maintenance and repair of all equipment.

The tenderer shall arrange formal class room training as per approved course structure for 10 men weeks at each RailTel regions and shall also include hands on practical experience at the manufacturer's/bidder premises. Set of Documents related to training to each of the trainees shall be provided. All expenses of Training shall be bear by the

tenderer however expenses for travel to and from the place of training, boarding and lodging of the trainees shall be borne by the RailTel.

7.4. GENERAL SYSTEM GUIDELINES

7.4.1. Tenderer shall be responsible for the successful completion of the project.

7.4.2. Purchaser/Engineer reserves the right to modify, revise, and alter the specifications of equipment system prior to acceptance of any offer.

7.4.3. If during the course of execution of the work any discrepancy or inconsistency, error or omission in any of the provisions of the contract is discovered, the same shall be referred to the Purchaser/Engineer who shall give his decision in the matter and issue instructions directing the manner in which the work is to be carried out. The decision of the Purchaser/Engineer shall be final and conclusive and the Tenderer shall carry out the work in accordance thereof.

7.4.4. Any item of Tenderer's goods/services not specifically mentioned, but considered essential for completion/commissioning of the work in all respects shall be deemed to be included in the scope of work. The tenderer may bring out any additional requirement and quote the price for the same as per the relevant SOR item, otherwise, it shall be required to be supplied by the tenderer free of cost.

7.5. TECHNICAL RESPONSE

The technical response shall be fully comprehensive and detailed and will include detailed guaranteed specifications of the equipment and systems to be supplied. Marginal performance shall not be accepted.

7.6. FEATURES AND CAPABILITIES OF EQUIPMENT

The succeeding specifications contain the necessary requirements of RailTel with regard to the features and capabilities of the equipment to be offered by the Tenderers. These will be carefully studied and commented upon by the Tenderer. These should not be treated as maximum specifications.

7.7. COMPLIANCE TO TECHNICAL REQUIREMENTS

7.7.1. CLAUSE BY CLAUSE COMPLIANCE

In the offer, the Tenderer shall include statement of clause by clause compliance of the tender document and sufficient documentation such that RailTel can validate the compliance statements. In the statement of compliance, the Tenderer shall state:

7.7.2. "FULLY COMPLIANT," if systems and functions offered fully meet the tender requirement.

7.7.3. "PARTIALLY COMPLIANT," if systems and functions offered meet the tender requirement partially. The Tenderer shall state the reason why the offer is partially compliant. However, if the Tenderer is able to fulfill the specified requirement later, the time schedule for this shall be stated. In such cases, the Tenderer shall clearly mention the extent to which other requirements or specifications are affected.

7.7.4. "NON COMPLIANT," if systems and functions cannot meet the requirements. The Tenderer shall also state the reasons for it.

7.7.5. In addition to the above mentioned compliance statements, wherever statement is given for some numerical parameter specified in tender, then Tenderer shall state the actual numerical value of specification as met by the offered systems/equipment.

7.8. NIL OR UNCLEAR RESPONSE STATEMENTS

In case of nil or unclear statements of compliance for any specified requirement, RailTel will interpret that particular requirement as being "NON COMPLIANT."

7.9. VARIANCE FROM SPECIFIED REQUIREMENTS

In case of variance of the offered equipment from the specified Technical requirements, the decision of RailTel on whether the equipment offered is responsive to the bid requirements shall be final and binding upon the Tenderer.

****

B. INSPECTION AND INSTALLATION, TESTING & COMMISSIONING

1. TESTS AND MEASUREMENTS

All equipments shall be subjected to tests as per technical specification and requirement specified in Chapter-3, Part-A, at manufacturer facility/premises and a test report for each equipment duly signed by the testing authority and accepted by suitable authority shall be submitted along with the equipment.

1.1 TEST CATEGORIES

1.1.1 The following tests shall be conducted for acceptance of the equipment and the system before final acceptance of the system.

i) Factory Acceptance Testing (FAT)
ii) Pre-commissioning test (after installation) for total integrated system.
iii) Site Acceptance Testing (SAT)
i) Trial Run / Field Trials.

Under exceptional circumstance, if it is not feasible to conduct Factory Acceptance Testing (FAT) at manufacturing facility, the equipment shall be accepted on the basis of certified manufacturer test report. In that case preliminary inspection of the equipment shall be arranged by the vendor at a suitable facility within India and detail inspection at site as per mutually agreed testing procedure. Exemption of inspection at factory premises (FAT) will be at the sole discretion of RailTel.

1.1.2 These tests shall be carried out on all equipment supplied by tenderer including those supplied by sub-vendors, if any. Tenderer shall arrange all necessary test instruments, manpower, test-gear, accessories etc.

1.1.3 All technical personnel assigned by Tenderer shall be fully conversant with the system specifications and requirements. They shall have the specific capability to make the system operative quickly and efficiently and shall not interfere or be interfered by other concurrent testing, construction and commissioning activities in progress. They shall also have the capability to incorporate any minor modifications/suggestions put forward by Purchaser/Engineer.

1.1.4 Test Plan: The Contractor shall submit to Purchaser 'Test Plans' well in advance of commencement of actual testing in each of the above mentioned test categories.
The plans shall include:
1.1.4.1 System/Equipment functional and performance description (in short) and Tests to be conducted and purpose of test.
1.1.4.2 Test procedures (including time schedule for the tests) and identification of test inputs details and desired/expected test results

1.1.5 Test Report: The observations and test results obtained during various tests conducted shall be compiled and documented to produce Test Reports by Tenderer. The Test Reports shall be given for each equipment/item and system as a whole. The report shall contain the following information to a minimum:
1.1.5.1 Test results
1.1.5.2 Comparison of test results and anticipated/expected (as per specifications) test result as given in test plans and reasons for deviations, if any.
1.1.5.3 The data furnished shall prove convincingly that:

a. The system meets the Guaranteed Performance objectives

b. Mechanical and Electrical limits were not exceeded.
c. Failure profile of the equipment during the tests are well within the specified limits.

1.1.6 Failure of Cards/Components:

Till the system is accepted by the Purchaser, a log of each and every failure of cards/components shall be maintained. It shall give the date and time of failure, description of failed component/ card with serial no., lot no. etc, circuit, module, component designation, effect of failure of component on the system/ equipment, cause of failure, date and time of repair, mean time to repair etc. Repair/modification done at any point of time at one site shall be carried out by Tenderer at all the sites. Detailed documentation for the same shall be submitted to Purchaser for future reference.

If the malfunction and/or failures of a unit/module/sub-system/equipment repeat during the test, the test shall be terminated and Tenderer shall replace the necessary component or module to correct the deficiency. Thereafter, the tests shall commence all over again from the start.

If after the replacement the equipment still fails to meet the specification, Tenderer shall replace the equipment with a new one and tests shall begin all over again. If a unit/ subsystem/module have failed during the test, the test shall be suspended and restarted all over again only after the Tenderer has placed the Equipment back into acceptable operation. Purchaser's approval shall be obtained for any allowable logical time required to replace the failed component/unit/module/sub-system.

1.1.7 Re-adjustments

No adjustments shall be made to any equipment/cards during the acceptance tests. If satisfactory test results cannot be obtained unless readjustments are made, Tenderer shall carry out only those readjustment needed to ready the equipment/system for continuance of tests. A log of all such adjustments shall be kept giving date and time, equipment, module, circuit, adjustments, reasons, test result before and after adjustment etc. Fresh acceptance tests shall be conducted after the readjustments have been completed.

1.2 FACTORY ACCEPTANCE TESTING (FAT)

Factory acceptance tests shall be carried out after review and approval of FAT procedure/documents as per bid requirements and review of Pre-Factory acceptance results & shall be conducted at the manufacturing facilities from where the respective equipment/subsystems are offered. The factory acceptance testing shall be conducted in the presence of the Purchaser/Engineer. The tests shall be carried out on all equipment/items including those supplied by Sub-vendors and factory acceptance certificates shall be issued. The factory tests shall include but not be limited to:

1.2.1 Equipment Testing:

1.2.1.1 Mechanical checks to the equipment for dimensions, inner and outer supports, finishing, welds, hinges, terminal boards, connectors, cables, painting etc.
1.2.1.2 Electrical checks including internal wiring, external connections to other equipment etc.
1.2.1.3 Check for assuring compliance with standards mentioned in the specifications.
1.2.1.4 Individual check on each/module/sub-assembly in accordance with the modes and diagnostics programs of the Tenderer
1.2.1.5 Checks on power consumption and heat dissipation characteristics of various equipment.

1.2.1.6 Environment testing and other laid down tests in Type Tests plan of the specification of the equipment.

1.2.1.7 Functional testing

1.2.1.8 Any other test not included in FAT document but relevant to the project as desired by the Purchaser/Engineer at the time of factory acceptance testing.

All equipments materials fittings and components will be subject to inspection by the purchaser or his representative at the manufacturer's factory/tenderer works before dispatch and no materials shall be dispatched until these are inspected and/or approved.

Under exceptional circumstance, if it is not feasible to conduct Factory Acceptance Testing (FAT) at manufacturing facility, the equipment shall be accepted on the basis of certified manufacturer test report. In that case preliminary inspection of the equipment shall be arranged by the vendor at a suitable facility within India and detail inspection at site as per mutually agreed testing procedure. Exemption of inspection at factory premises (FAT) will be at the sole discretion of RailTel.

1.2.2 System Integration Testing

Functional and performance test should be conducted for the complete system/ all major equipment constituting the system (including the equipment supplied by sub-vendors, as applicable) simulating the complete network with appropriate network elements. All equipment shall be connected using the same cables (interfaces/components) as will be used during final installation so that the system can be tested in its final configuration. This testing shall be conducted at the manufacturing facility of the main equipment.

1.3 INSTALLATION

After successful completion of Factory Acceptance Test or acceptance report of equipment on the basis of certified manufacturer test report, equipment shall be sent to site for installation.

All equipment shall be checked for completeness as per the specifications of equipment required for a particular station. Installation shall be carried out in accordance with the installation manuals and approved installation drawings in the best workmanship.

The contractor shall be responsible for ensuring that the work throughout are executed in the most substantial, proper and workmanlike manner with the quality of material and workmanship in strict accordance with the specifications and as per sound industrial practices and to the entire satisfaction of the RailTel.

If during installation and commissioning any repairs are undertaken, the maintenance spares supplied with equipment shall not be used for the repair. Tenderer shall arrange his own spare parts for such activities till such time the system has been finally accepted by the Purchaser. A detailed report & log of all such repairs shall be made available by the Tenderer to Purchaser/Engineer and shall include cause of faults and repair details, within two weeks of fault occurrence.

Tenderer shall supply all installation materials required for proper installation of the equipment. These shall include but not be limited to, all connectors, inter-bay and inter-equipment cables, power/earthing cables, connectors, anchoring bolts, nuts, screws, washers etc. as needed.

The bidder has to ensure that installation of equipment shall be done as to present neat and clean appearance in accordance with approved installation document drawings. All inter bay, power supply and other cables shall be routed through wall mounted cable trays. No cable shall be visible. Equipment installed at one of the site shall be made as model site and Tenderer shall take approval from Purchaser/engineer on various aspects etc.

1.4 PRE-COMMISSIONING

On completion of installation of equipment, the correctness and completeness of the installation as per Manufacturer's manual and approved installation documents shall be checked by the Tenderer on his own.

A list of Pre-Commissioning tests (same as approved by the Purchaser/Engineer for Site Acceptance Testing) and activities shall be prepared by Tenderer and the test shall be carried out by the Tenderer on his own. After the tests have been conducted to the Tenderer own satisfaction, the Tenderer shall provide the test results for review by Purchaser/Engineer and then offer the system for Site Acceptance Testing.

During pre-commissioning, if any fault occurs to any equipment or system, Tenderer shall identify the same and provide report/history of all faults to the Purchaser.

Tenderer shall ensure that the spares meant for operation and maintenance are not used during installation and commissioning.

1.5 SITE ACCEPTANCE TESTING (SAT)

On completion of Pre-commissioning, site acceptance testing shall be conducted on the system as per approved SAT procedures and its constituents by the Tenderer under the presence of Purchaser/Engineer.

The tests shall include, but not be limited to the following:

1.5.1 Checks for proper installation as per the approved installation drawings for each equipment/item and system as a whole.
1.5.2 Guaranteed performance specifications of individual equipment/item.
1.5.3 Self diagnostics test on individual equipment
1.5.4 Tests on metering and alarm panels
1.5.5 Tests on remote alarm transmission and reception
1.5.6 System tests on per hop basis and END TO END for the ring/link, all complete.

1.6 PROVISIONAL ACCEPTANCE CERTIFICATE (PAC)

On installation of the equipment, the contractor shall certify and advise Railtel Supervisor where equipment has been installed, in writing that the installation is (i) completed (ii) ready for satisfactory commercial service and (iii) ready to be handed over. After successful completion of Site Acceptance Testing, a report (SAT) shall be forwarded to GGM/DNM. Provisional Acceptance Certificate (PAC) will be issued by GGM/DNM. PAC will not be held back for want of minor deficiencies not affecting the functioning of the equipment. Deficiencies, if any, pointed at the time of issuance of PAC, will be rectified by the contractor within one month.

1.7 TRIAL RUN/FIELD TRIALS

Upon conclusion of the site acceptance testing, the Tenderer shall keep the facilities commissioned for one month for 'TRIAL RUN/FIELD TRIALS'. During this period Tenderer shall provide all specialist Engineers & Technicians including experts at the NMS to maintain the total log, incidents, failures & for assisting site engineer & for total co-ordination. However, the normal operation and maintenance of the system shall be performed by the personnel of the Purchaser trained for the purpose.

If during 'TRIAL RUN/FIELD TRIALS' any defect is noted in the system, the Tenderer shall rectify, replace the same to the satisfaction of Purchaser/Engineer. The decision to

repeat the final test or restart the 'Trial / Field Trials' shall be of Purchaser/Engineer depending upon the severity of the defect.

During trial run / field trial, if any fault occurs to any equipment of system, Tenderer shall identity and rectify the same and provide report, history of all faults to the Purchaser.

Ideally, during the 'TRIAL RUN / FIELD TRIALS', no shutdown of the system due to failure of equipment, power supply etc. should happen. A record of all failures shall be kept for each manned/unmanned station and the availability of the system on per hop and end to End basis shall be calculated, accordingly and results submitted to Purchaser/engineer. If the system fails to come up to the guaranteed performance, the Tenderer, within a period of thirty (30) days shall take any and all corrective measures and resubmit the system for another 'Trial Run' of trial period. All modifications, changes, corrective measures, labour etc. shall be at the cost of the Tenderer. In case the date of completion for the second trial run exceeds the time schedule for the project, he shall be liable to pay liquidated damages. If the system fails to reach the guaranteed performance even after the second trial run, the Purchaser shall be free to take any action as he deems fit against the Tenderer and to bring the system to the guaranteed performance with the help of third party at the expense of the Tenderer.

1.8 FINAL ACCEPTANCE

The final acceptance of the works completed shall take effect from the date of successful completion of 12 months after issue of PAC provided in any case that the contractor has complied fully with his obligations in respect of each item under the contract. The Final Acceptance Certificate of all regions against the contract shall be issued by GGM/DNM. Notwithstanding the issue of Final Acceptance Certificate the contractor and the purchaser shall remain liable for fulfillment of any obligation incurred under the provision of the contract prior to the issue of Final Acceptance Certificate which remains unperformed at the time such certificate is issued and for determining the nature and extent of such obligation the contract shall be deemed to remain in force between the parties hereto.

1.9 QUALITY ASSURANCE

1.9.1 Tenderer shall submit the details of Quality Assurance program followed by them beginning with raw materials, active, passive and fabricated components, units, sub-assemblies, assemblies, wiring, interconnections, structures etc. to finished product. Tenderer shall obtain and forward the Quality Assurance Program for equipment supplied by Sub-vendor, if any.

1.9.2 The Purchaser/engineer reserves the right to inspect and test each equipment at all stages of production and commissioning of the system. The inspection and testing shall include but not be limited to raw materials. Components, sub-assemblies, prototypes, production units, guaranteed performance specifications etc.

1.9.3 For inspection and testing, Tenderer shall arrange all that is required e.g. quality assurance personnel, space, test instruments etc. for successful carrying out of the testing by the Purchaser/Engineer, at Tenderer cost, at the Manufacturer's works/tenderer premises/site.

1.9.4 Purchaser/Engineer shall have free entry and access to any and all parts of the Manufacturer's facilities associated with manufacturing and testing of the system at any given time.

1.9.5 It shall be explicitly understood that under no circumstances shall any approval of the Purchaser/Engineer relieve the Tenderer of his responsibility for material, design, quality assurance and the guaranteed performance of the system and its constituents.

1.9.6 Tenderer shall invite the Purchaser/Engineer, at least 7 days in advance, of the date at which system shall be ready for Inspection and Testing. All relevant documents and manuals approved Engineering drawings etc. shall be available with the Purchaser/Engineer well in advance of the start of Inspection and Testing.

1.9.7 Purchaser or his representative shall, after completion of inspection and testing to their satisfaction, issue factory acceptance certificates to release the equipment for shipment.

No equipment shall be shipped under any circumstances unless a factory acceptance certificate has been issued for it, unless agreed otherwise by Purchaser/Engineer.

****

C. TRAINING, VENDOR DATA REQUIREMENT, DOCUMENTATION, AND DESIGN GUIDELINES

1. TRAINING

Tenderer shall train personnel of Purchaser/engineer in all aspects of offered system.

The training course shall be conducted at the manufacturing facilities from where the respective equipment/subsystems are manufactured/ offered or in India if the firm can arrange full fledged training facilities in case their manufacturing facilities are located outside India.

It shall be explicitly understood, that Purchaser's/Engineer's personnel shall be fully associated during Engineering, Installation, Testing and Commissioning activities and this opportunity shall be taken by Tenderer to impart on the job training in addition to the above training course.

Tenderer offer excludes costs of transportation, lodging and boarding of the trainees which shall be arranged by the Purchaser.

The training course to be conducted at the manufacturing facilities shall be designed to train the trainees in all aspects of System engineering, equipment operation, installation and functional details, theory of operation of equipment, trouble shooting and familiarization with the equipment at card and component level. All equipment used for training shall be identical to those quoted and supplied for site installation in hardware and software versions.

Tenderer shall provide comprehensive documentation, course material, manuals, literature etc. as required for proper training of personnel at his own cost. Consolidated and comprehensive documentation shall be available to each participant. After the completion of course, all such materials shall become the property of the PURCHASER. Tenderer shall update the course material of manuals in case there are any changes owing to revision/modifications in equipment/system specifications.

Tenderer shall, prior to start of training, send complete training program including details of each course, duration, subject matter etc. The Purchaser/Engineer reserves their right to suggest any additions/deletions in the program, which shall be incorporated by the Tenderer at no additional cost.

Resident Engineer (Qualification and Experience required)

- Graduate from a recognized university.
- 3-6 years of experience in information security (SOC operations preferred)
- Good knowledge of OSI layers and TCP/IP suite, security concepts, firewall, encryption etc.
- Good knowledge of network and security anomalies exhibited by IT network environment
- Good knowledge of TCP/IP stack and network protocols
- Hands on experience in vulnerability assessment and penetration testing using specialized tools
- Good knowledge of malware analysis (static and behavioural)
- Good knowledge of different network attacks and countermeasures
- Good knowledge of web servers, database servers (Windows/SQL/Linux/Oracle/Apache)
- Knowledge/experience in log analysis and event correlation
- Experience in event log monitoring of security devices
- Must have knowledge on security and network components from multiple vendors
- Good knowledge of industry best practices on information security standards such as ISO 27001
- One or more of the following certifications(Preferable):-CISSP or CEH or ISO 27001

2. VENDOR DATA REQUIREMENT AND DOCUMENTATION

One set of Documentation shall be supplied with each system. In addition, 2 more sets of full documents shall be supplied. All documents and manuals shall be in English language only.

The following documents for the complete system shall be supplied and approved by Purchaser/Engineer in order to start inspection:

a. System description, System configuration diagram & Connectivity diagram

b. Detail technical manual of each type of equipment

c. Equipment interconnection diagram including details of various interfaces, signaling protocols used at each stage.

d. Layout of equipment and space requirement.

e. Installation manual including installation procedure and commissioning.

f. Supervisory configuration, alarm list, operator interface etc.

g. Maintenance manual of each type of equipment containing:

   i. Preventive maintenance procedures.

   ii. Trouble shooting/repairs procedures including failure analysis shall provide exhaustive information about repairs including but not limited to removal, reinsertion of components and cards, repairs, adjustments, tuning, calibration, tools required for a particular operation, test points, including turnaround time for repair and the details of the maintenance support service centre to be furnished in the bid and all other maintenance related details.

   iii. Expansion possibilities of the system without causing deterioration in the system performance.

   iv. Any other data, document not specifically mentioned, but required for the satisfactory testing, installation and commissioning, operation and maintenance of the system shall be provided.

   v. Documents to be supplied after trial runs but before System commissioning (Acceptance of the System by Purchaser/Engineer).

3. DESIGN GUIDELINES

i) Equipment shall conform to the similar housing standards and shall preferably be integrated in one 19" rack.

ii) All equipment shall have sufficient number of alarms and supervisory indications and shall be provided with self-diagnostic facilities. All alarms and monitoring & diagnostic facilities shall be built-in & shall be displayed on the front panel of the equipment for ease of maintenance. It shall be possible to transmit these indications, parameters to the control station /NMS on real time basis.

iii) The healthy/unhealthy condition of the units shall be displayed by different color LEDs/Lamps.

iv) For important switches, the maintenance personnel shall provide controls on the front panel with suitable safeguard to avoid accidental operation. Manual changeover should be performed by more than one sequential operating procedure to avoid accidental operation.

v) All equipment shall be immune to EMI; RFI interference generated by any nearby source & shall meet the latest international standards in this regard.

vi) The equipment shall be capable of functioning with minimum maintenance and shall be preferred to have no requirement of any preventive maintenance.

vii) All patch cords shall be provided with connectors matching to the cable used and shall have identification markings.

viii) All sub-assemblies or modules, switches and controls and the circuit components shall be so mounted as to permit their replacement without appreciable disturbance to other components.

ix) If the vendor is not using distributed power supply system on individual module basis then the Power supply cards shall be duplicated (1+1). However one standalone power supply card shall be able to run the system for its entire lifetime.

x) All equipment sub racks, housings shall be provided with antistatic wristbands, if required for safe handling of Cards.

xi) The equipment should have modular design and should be configurable in number of operational modes to perform complex and different network functions without need of any additional software.

****

CHAPTER 4

COMMERCIAL TERMS & CONDITIONS

1. Offer letter and Validity of offer

1.1. The bidder shall complete the offer letter (Chapter 1) and the Price Schedule (Chapter 2) furnished in the tender documents, indicating the goods to be supplied, description of the goods, associated technical literature, quantity and prices etc.

1.2. The offer should remain valid for a minimum period from the date of opening of tender including the date of opening as indicated in Bid Data Sheet (BDS) Chapter 5.

2. Warranty

2.1. The warranty would be valid for a period as indicated in Bid Data Sheet (BDS) Chapter 5. The supplier shall warrant that stores to be supplied shall be new and free from all defects and faults in material, workmanship and manufacture and shall be of the highest grade and consistent with the established and generally accepted standards of materials of the type ordered and shall perform in full conformity with the specifications and drawings. The supplier shall be responsible for any defects that may develop under the conditions provided by the contract and under proper use, arising from faulty materials, design or workmanship such as corrosion, inadequate quantity of material to meet equipment requirements, inadequate contact protection, deficiencies in design and/ or otherwise and shall remedy such defects at his own cost when called upon to do so by the Purchaser who shall state in writing in what respect the stores are faulty.

2.2. If it becomes necessary for the contractor to replace or renew any defective portion/portions of the supplies under this clause, the provisions of the clause shall apply to the portion/portions of the equipment so replaced or renewed or until the end of the above mentioned period or twelve months, whichever may be later. If any defect is not remedied within a reasonable time of 30 days, the Purchaser may proceed to do the work at the contractor's cost, but without prejudice to any other rights which the Purchaser may have against the contractor in respect of such defects

2.3. Replacement under warranty clause shall be made by the contractor free of all charges at site including freight, insurance and other incidental charges.

2.4. Warranty Support

2.4.1. Material for repair during Warranty Period shall be handed over /taken over to contractors engineer at regional NOC's or mutually agreed RailTel PoP location.

2.4.2. During the warranty period, the contractor shall be responsible to the extent expressed in this clause for any defects that may develop under the conditions provided for by the contract and under proper use, arising from faulty materials, design or workmanship in the plant, or from faulty execution of the plant by the contractor but not otherwise and shall remedy such defects at his own cost when called upon to do so by the Purchaser Engineer who shall state in writing in what respect the portion is faulty.

2.4.3. During the free warranty maintenance period contractor should stabilize the working of the system. Purchaser has the right to extend the period of supervision of the maintenance free of cost till the system stabilizes and works satisfactorily for a reasonable period of time. If during the time any equipment etc. is to be added or deficiencies are to be rectified to make the system work trouble free the same also will have to be done by the contractor at no cost to RailTel as to make good all the deficiencies.

2.4.4. Bidder should provide the one Qualified (L2 Level) Engineer (working 6 days a week for 8 Hrs) and DDoS detection & Mitigation Solution up time should be 99.99 % for redundant system and 99.95% for non redundant System excluding the

dependencies on account of RailTel and unforeseen circumstances. If the Bidder fail to achieve uptime as mentioned, the following penalties will be imposed. It will be calculated on quarterly (3 month) basis and maximum penalties will be 10 % of the cost of Equipment per year.

Service type Parameter	Service Level	Penalties
For redundant system	>= 99.99%	NIL
	Between 99.99% and 99.95%	0.2% of the cost of Equipment
	Between 99.95% and 98.95%	2% of the cost of Equipment
	Between 98.95% and 96.96%	4% of the cost of Equipment
	Between 96.95% to 95%	6% of the cost of Equipment
	< 95%	10% of the cost of Equipment

2.4.5.Replacement Services

During warranty and AMC period, if the Bidder fails to replace card/Part/Equipment within Next Business Day Working days, the following penalties will be imposed.

Equipment	Duration of repair	Deduction/Penalties
All Modules and accessories	Next Business Day	Nil
All Modules and accessories	Beyond Next Business Day	10% of the cost of affected part/module
All Modules and accessories	More than 10 days and up to 30 days	25% of the cost of affected part/module
All Modules and accessories	More than 45 days	100% of the cost of affected part/module

Note:

a. In event of that bidder fails on both service SLA and replacement services the maximum aggregate penalties would be limited to equipment cost.

b. OEM should provide facility to RailTel for direct fault case open on TAC Support in case emergency.

2.5. Maintenance Supervision

2.5.1.After the proposed network is commissioned and placed in service and after Provisional Acceptance Certificate (PAC) is issued, the contractor shall be responsible for proper maintenance supervision of the network free of cost for a period of twelve months from the Successful commissioning of the solution.

2.5.2.To summarize, the total period of warranty as per BDS in Chapter-5, will comprise of first 12 months of Maintenance Supervision (after issue of PAC) extendable by RailTel for reasons as explained, as per para 2.5 above, post which FAC will stand issued.

3. Long Term Maintenance Support

➢ The Bidder will submit a certificate from OEM of switch towards maintenance support after successful completion of the warranty obligations for a minimum period of 5 years. The long term maintenance support shall be comprehensive and include all hardware and software of equipment etc. (on repair and return basis) supplied against this contract. RailTel should be extended the benefits of software up-grades made by OEM on the

system from time to time to improve performance. During this period the following terms and conditions shall be applicable.

- Material for repair shall be handed over /taken over to contractors engineer at the RailTel's NOC or mutually agreed RailTel PoP location. The cost of repairs etc. shall be included in the quoted bid price during warranty period. During this period, the contractor shall remain responsible to arrange replacement within 10 days and for setting right at his own cost any device which is of defective manufacture or design or becomes unworkable due to any cause whatsoever. The decision of the RailTel's representative in this regard to direct the contractor to attend to any damage or defect in work shall be final and binding on the Contractor.

- During the year contractor shall be responsible to the extent expressed in this clause for any defects that may develop under the conditions provided for by the contract and under proper use, arising from faulty materials, design or workmanship in the plant, or from faulty execution of the plant by the contractor but not otherwise and shall remedy such defects at his own cost when called upon to do so by the Purchaser Engineer who shall state in writing in what respect the portion is faulty.

- If it become necessary for the contractor to replace or renew any defective portions of the system under this clause the provisions of this clause shall apply to the portions of the plant to be replaced or renewed until the expiration of three months from the date of such replacement or renewal or until the end of the support period whichever may be later. If any defect is not remedied within reasonable time, the purchaser may proceed to do the work at contractor's risk and expense, but without prejudice to any other rights which the purchaser may have against the contractor in respect of such defects.

- Tender/OEM, shall be paid @ 3.5% of supply cost per annum towards Long Term Maintenance Support after completion of warranty period, to undertake repairs/ replacements of all type of module/ card/assembly/ subassembly and update/upgrade of software released during this period and /or which may fail in the network after the warranty. Only incremental cost in % over and above this, if perceived by the OEM and Tenderer, may be indicated in Schedule of Requirement and shall be added towards evaluation of tender. If however the tenderer feels that his AMC Cost is less than 3.5% per annum, he should give suitable discount in equipment pricing. For AMC he will be paid @ 3.5% per annum only. If the Tenderer quotes a higher base rate for AMC, he will be paid at his quoted rate per annum and five year differential cost shall be added to offered cost for evaluation. AMC would have to be valid for minimum period of 4 years after the warranty.

  In case a tenderer quotes AMC rates lower than 3.5%, no advantage will be given to him for evaluation purposes. In case the tenderer wins the contract his cost will be reduced by differential (w.r.t. 3.5%) AMC rates & he will be paid accordingly. AMC charges to him, however be paid only @ 3.5% per annum.

- Separate LOA/agreement for AMC after warranty period shall be entered with OEM/ Bidder by RailTel. A fresh Bank Guarantee valid for five years for 10% of the Long Term Maintenance Support cost of five years quoted by the tenderer, shall be required to be submitted by OEM/ Tenderer for due fulfillment of long term maintenance support obligation.

- Quarterly payment for AMC Charges would be made by RailTel after successful completion of AMC Services of that quarter and on the certificate furnished by concerned RailTel representative of the Executive Director of the Region.

Note: The acceptance of the above clause is mandatory and specific acceptance from OEM is required to be enclosed as per Annexure-1. Any deviation / non acceptance will lead to rejection of the bid summarily.

4. Delivery Period

The materials as per SOR are required to be delivered within period as indicated in Bid Data Sheet (BDS, Chapter 5) to the site /transported to different locations which will be provided by RailTel to the successful bidder.

Road permit will be facilitated by RailTel and shall issue necessary request letter etc. Tenderer are required to obtain the road permit. However, it has no bearing on delivery period.

5. Payment Terms

5.1. Payment shall be made in Indian Currency (Rs) 75% payment of the value of the supply items would be made on receipt of material by the consignee(at site / the stores) duly inspected and on submission of the following documents subject to any deductions or recovery which RailTel may be entitled to make under the contract:

- Invoice
- Delivery Challan
- Excise Gate pass/Excise/Custom Invoice
- Packing list.
- Factory Test Report/Certified manufacturer Test Report
- Purchaser's Inspection certificate
- Consignee receipt
- Warranty certificate of OEM
- Insurance certificate
- Certificates duly signed by the firm certifying that equipment/ materials being delivered are new and conform to technical specification.

5.2. 15% payment of the value of Supply items of the PO shall be made by RailTel on successfully Installation & Commissioning at site, 5% payment of value of Supply items of the PO on issue of Provisional Acceptance Certificate (PAC) and the last 5% payment of the value of Supply items of the PO shall be made by RailTel on issue of Final Acceptance Certificate (FAC) which will be issued by GGM/DNM.

5.3. 15% payment of value of supply items of the PO which could not be installed within 90 days due to site readiness or other reason on account of RailTel will be made with approval of GGM/DNM and remaining (5% + 5%) on issue of PAC and FAC.

5.4. RailTel shall make payments after the submission of invoice with required documents as per contract. Accounting/Bill passing unit for SOR for supplies is Corporate Office. All Bills shall be submitted to the GGM/DNM for certifying and verification and onwards submission to Finance of RailTel Corporate Office for releasing the payment.

5.5. Form "C" shall be issued for respective stations, if required, by respective Executive Director of the Region only.

5.6. The breakup of taxes has to be furnished and same should be reflected in the bills so that any CENVAT/input credit can be availed by RailTel.

5.7. Payment of Services Items

5.7.1. Payment of service items shall be made in Indian Currency (Rs.) only. 90% payment of SOR item towards "Installation, Testing & Commissioning" shall be made by Corporate Office on successful Installation, testing & commissioning, 5% on issue of PAC and final 5% on issue of Final Acceptance Certificate.

5.7.2. Payments for Resident Engineer will be paid on quarterly basis after satisfactory go ahead from competent authority.

5.7.3. Payment of SOR item towards "AMC " would be paid quarterly by the Corporate Office after satisfactory completion of AMC Services of that quarter and on certificate furnished by CNOC.

6. Performance Bank Guarantee (Security Deposit)

6.1. The successful bidder shall have to submit a performance Bank Guarantee (PBG) within 30 days of the issue of Purchase order @ 10% of the value of the PO for the satisfactory performance of materials covered in SOR given in Chapter 2 valid for a period of 4 months beyond warranty period. Extension of time for submission of PG beyond 30(thirty) days and up to 60 days from the date of issue of Letter of acceptance may be given by the Authority who is competent to sign the contract agreement. However, a penal interest of 15% per annum shall be charged for delay beyond 30(thirty) days. i.e from 31st day after issue of LOA. In case the contractor fails to submit the requisite PG even after 60dyas from the date of issue of LOA, the contract shall be terminated duly forfeiting EMD and other dues, if any, payable against that contract. The failed contractor shall be debarred from participating in re-tender for that work.

6.2. The earnest money shall be released on submission of PBG. The Performa for PBG is given in Chapter 6 Form No. 1. If the delivery period gets extended, the PBG should also be extended appropriately

6.3. The Performance Bank Guarantee (security deposit) will bear no interest.

6.4. This PBG would be released after satisfactory completion of contract including warranty period and only after submission of 10 % PBG towards AMC.

7. **Taxes & Duties**

7.1. The price quoted in the offer should be firm, fixed indicating the breakup and inclusive of all taxes & duties like import, custom, C.V.D., Anti-Dumping duty(if any), ED & sales tax, VAT etc. The offer should be inclusive of packing, forwarding, freight upto destination, insurance charges.

7.2. The Octroi / entry tax shall be paid extra as per actual on production of proof of payment / document.

7.3. Anti-Dumping duty if applicable on the equipment proposed to be supplied by OEM/Tenderer as per extant instructions of Ministry of Commerce/Finance Government of India, has to be borne by the tenderer and shall be deducted from the amount payable to the contractor at the time of making payment to the firm, if this duty amount is paid to Custom Authority by RailTel.

7.4. Any changes in the statutory taxes & duties during the contract period shall be on RailTel account with in the original DOC. Beyond DOC, changes in statutory taxes & duties shall be on RailTel's account only when the delay is an account of RailTel.

8. **Insurance**

8.1. The Contractor shall take out and keep in force a policy or policies of insurance from the date, the delivery of material starts (including the transit portion) against all liabilities of the Contractor or the Purchaser. The contractor shall take out and keep in force a Policy or policies of Insurance for all materials covered in schedule of requirement irrespective of whether used up in the portion of work already done or kept for the use in the balance portion of the work until such material are provisionally handed over to RailTel. The goods will be issued by purchaser to supplier and risk of goods shall remain with supplier until the issue of PAC by RailTel. Insurance policy has to be kept valid by the contractor till issue of PAC by RailTel.

8.2. The Contractor should insure the stores brought to site, against risks as required under the Emergency Risk (Goods) Insurance Act in force from time to time up to contract value.

8.3. It may be noted that the beneficiary of the insurance policy should be RailTel or the policies should be pledged in favor of RailTel. The contractor shall keep the policy/policies current till the equipment are handed over to the purchaser. It may also be noted that in the event of contractor's failure to keep the policy current and alive, renewal of policy will be done by purchaser for which the cost of the premium plus 20% of premium shall be recovered from the contractor.

9. **Liquidated Damages**

The timely delivery is the essence of this tender. Liquidated damages will be applicable at the rate of half percent 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.

10. **Transportation**

The rates quoted should be CIP destination. The destination shall be defined POP / nominated office of RailTel in the proposed sections which shall be indicated by RailTel's representative.

11. **Statutory Deduction**

These will be made at source as per the rules prevalent in the area of work.

12. **Qualification Criteria**

Qualifying criteria under this clause lays down minimum acceptable qualifications in various areas to ensure that qualified tenderer has necessary experience, technical expertise, equipment and financial and human resources to successfully complete the project. Bids from bidder not meeting these qualification criteria shall be summarily rejected.

12.1. **Technical Capability**

12.1.1. The Tenderer/bidder should be an Original Equipment Manufacturer (OEM) or Authorized partner of OEM specifically authorized by OEM for bidding in this tender (as indicated in Bid Data Sheet (BDS) Chapter 5). The OEM should have proven facilities for Engineering, manufacture, assembly, integration and testing of offered system and basic facilities with respect to space, Engineering, Personnel, Test equipment, Manufacture, Training, Logistic Supports for at least past three years in the country from where the proposed equipment are planned to be supplied.

12.1.2. The Tenderer/bidder should have supplied and provision of similar offered equipments of security solution commercially with satisfactory working as indicated in Bid Data Sheet (BDS) Chapter 5 to Government/PSUs/Telecom Service Providers/Public Listed Company during the last three years from the date of opening of tender.

12.1.3. The Bidder should have registered office in India for a minimum period of 3 years as on originally scheduled date of bid opening.

12.1.4. The Bidder should have authorization from respective OEMs and should submit the vetted BOM from their respective OEMs.

12.1.5. The Bidder should have minimum of 3 Technically Certified Engineers on their own rolls trained in OEM technology whose Products are being offered. The Bidder should submit the copy of certificates along with the bid.

12.1.6. Each OEM can authorize up to a maximum of three (3) authorized partners to bid the tender.

12.1.7. The Bidder or their promoters having equity stake or operating partnership in bidder, should not be holding valid License for Telecom service provider/ISP/NLD, Services License of Government of India for Telecom Operation.

12.1.8. RailTel reserves the right:-

a) To verify, if so desired, the correctness of documentary evidence furnished by the tenderer.

b) To verify the successful operation and performance of qualifying projects and tenderer shall arrange permission for the same.

c) To carry out capability assessment of the bidder(s) including referral to in-house information.

d) RailTel shall not be responsible for any delay in the receipt of tenders and reserves the right to accept/reject any or all tenders without assigning any reason.

12.1.9. The bidder shall furnish documentary proof of backend support including software upgrades and availability of spares for a period of 5 years from the respective OEMs of the products offered.

12.1.10. The tenderer must provide technical presentation on solution and methodology approach.

12.1.11. The tenderer/OEM should submit the details of supply of offered equipment executed as indicated in Bid Data Sheet (BDS) Chapter 5, along with certificates from the original user for whom the project was undertaken certifying the date of award of contract, date of completion, and the present working state of the system which should clearly bring out performance of the equipment. The certificates are to be submitted in original or their true copies duly signed by the tenderer.

12.2. Financial Criteria

12.2.1. The bidder should be a company registered under the Companies Act, 1956 or a partnership firm registered under Indian Partnership Act 1932 or Limited Liability Partnership Act 2008 with registered office in India and in operation for at least 3 years as on 31.03.2016 and should have their registered offices in India.

Valid documentary proof of:

- Certificate of incorporation
- Certificate of Commencement
- Certificate consequent to change of name, if applicable
- Copy of Memorandum of Association

12.2.2. The company must be registered with appropriate authorities for all applicable statutory duties/taxes.

Valid documentary proof of:

- Central Sales Tax/VAT number.
- Service Tax registration number.
- Income Tax registration/PAN number
- Income Tax returns for the last three years

12.2.3. The tenderer should present at least four (4) projects each worth at least INR 50 lakhs showcasing supply, design, installation, testing, commissioning, implementation and operations projects for security solutions commercially in India in the last 2 years.

Copy of work orders supported with relevant documentary evidences for the design parameters as mentioned in criteria 4 and the completion certificates by the client. Documentary evidence should clearly indicate the nature of systems implemented for each project

12.2.4. The sum total of the turnover of contractual payment received during the last preceding 3 financial years (i.e. current year and three previous financial years) from the date of opening of tender should be a minimum of the value as indicated in Bid Data Sheet (BDS) Chapter 5.

12.2.5. Tenderer should produce Audited Balance Sheet and Income statement of all the preceding three financial years.

12.2.6. The tenderer shall furnish such documents as to establish the financial soundness of their company. The latest balance sheet audited or certified by a neutral agency shall be furnished.

12.2.7. In the event of foreign Original Equipment Manufacturer (OEM), Indian Subsidiary is allowed to participate with the experience and financial credential of parent company with specific authorization for doing so from the OEM. The specific authorization addressed to RailTel should be submitted by the tenderer.

13. System Performance Guarantee

13.1. The tenderer shall give unqualified and unconditional guarantee that when the equipment / material supplied by him is installed and commissioned at site, it shall achieve the desired objective and that in the event of performance of the system when installed not complying with the end objective or with the specifications, he shall provide further inputs to enable the RailTel to realize the end objectives with full compliance of the specifications contained in these documents. No additional payment will be made to the contractor for supply of any additional goods and service required in this regard.

13.2. This certificate in the Proforma given in Chapter 6 Form No. 2, shall accompany the final offer. Absence of this certificate which will form part of the agreement shall disqualify the tenderer automatically.

14. Evaluation of Offer

14.1. For the purpose of relative ranking of offers, all inclusive value for entire supply, supervision of installation, testing & commissioning and warranty period support, training, AMC shall be taken into account.

14.2. Additional features offered by the bidder, over and above the ones asked for in the tender documents, shall not be considered for evaluation of bids.

14.3. The tenderer should make available the offered products, if desired during technical evaluation of offered equipment for testing and benchmarking at any testing facility approved by RailTel.

14.4. The bidders should quote for all items & the offer will be evaluated in totality. The bidders should indicate brand name, type/model number of the products offered. Optional items will be considered for evaluation of offers. The equipment should be supplied as per Technical Specifications given in Chapter-3.

15. Security Considerations & Security Agreement

15.1. While evaluating the tender, regards would be paid to National Defence and Security considerations.

15.2. The directives issued from time to time by the Department of Telecommunications (DoT), Ministry of Communications and IT or any other Ministry of Govt. of India on security considerations shall be applicable to the present tender. Accordingly, as per the extent amendment of the National Long Distance (NLD) Service License Agreement for Security related concerns for expansion of Telecom Services in various zones of the country issued vide Department of Telecommunication, Ministry of Communication and IT, Govt. of India's letter no. 10-54/2010-CS-III (NLD) dated: 31.05.2011, the successful tenderer/OEM shall comply with the provisions stated in the above mentioned directive of DoT and shall have to enter into an agreement with RailTel as per the template agreement between Telecom Service Provider and the vendor of equipment, product and services (available on DoT website). The tenderer must submit a declaration along with their bid.

15.3. The Network is being provided primarily to meet the requirement of Indian Railways. Accordingly, the network shall take into consideration the National Security requirement and National Security aspects indicated by the Indian Railways.

16. Purchaser's Right to Vary Quantities

16.1. The purchaser shall be at liberty to enhance or reduce the quantity mentioned in the purchase order as indicated in Bid Data Sheet (BDS) Chapter 5 without assigning any reasons. The bidder shall comply with such modifications unconditionally provided these are made before completion of the deliveries under the purchase order. Any such change in quantity shall have no impact on the rates mentioned in the purchase order for any such item.

17. Purchaser's Right to accept any offer / Bid and to reject any or all offer/ Bid

17.1. The Purchaser reserves the right to accept or reject any offer / bid, and to annul the bidding process and reject all offers / bids, at any time prior to award of order without assigning any reason whatsoever and without thereby incurring any liability to the affected bidder or bidders on the grounds for the Purchaser's action.

18. Execution of Purchase Order

18.1. The successful bidder has to submit the copy of the Purchase order duly signed on each page including Annexures & will submit the Performance Bank Guarantee as per Clause no. 6 for due fulfillment of the PO.

18.2. If the successful bidder fails to submit the accepted copy of PO and required PBG within 30 days from the date of issue, it shall constitute a breach of the agreement affected by the acceptance of the tender in which case the full value of the earnest money accompanying the tender shall stand forfeited without prejudice to any other rights or remedies. The Tenderer shall also submit the inspection plan, Implementation plan etc, within this 30 days period.

18.3. In the event of any tenderer, whose tender is accepted, refuses to execute the PO as herein before provided, RailTel may determine that such tenderer has abandoned the Purchase Order and thereupon his tender and acceptance thereof shall be treated as cancelled and RailTel shall be entitled to forfeit the full amount of the Earnest Money and to recover the damages for such default.

19. Annulment of Award

19.1. Failure of the successful bidder to comply with the requirement of various clauses of tender document shall constitute sufficient ground for the annulment of the award and forfeiture of EMD in which event the Purchaser may make the award to any other bidder at the discretion of the Purchaser or call for new offers/ bids.

20. Earnest Money Deposit (EMD)/ Bid Security

20.1. The tenderer shall furnish a sum as given in Bid Data Sheet (BDS) Chapter 5 as Earnest Money in the form of Demand Draft from any scheduled bank in India in favour of "RailTel Corporation of India Limited" payable at New Delhi.

20.2. 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.

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

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

20.5. 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 6.

20.6. Earnest Money will bear no interest.

21. Preference to Domestic Manufacturers for Telecom Equipment

21.1. "Preference to domestically manufactured electronic goods in procurement due to security considerations" shall be applicable as per Government of India policy as on the date of opening of price bid. The manufacturer claiming to qualify under the scope of such rules for PMA (Preferential Market Access) must submit the declaration of VA (Value Addition) as required under the issued notification for the specified period ((2012-13,2013-14 & 2014-15).)

22. Offer/ Bid Prices

22.1. The bidder shall give the prices indicating all levies and taxes, packing forwarding, freight and insurance etc. The basic unit price and all other components of the price need to be individually indicated against the goods it proposes to supply under the tender document as per schedule given in Chapter 2. The price shall be quoted in Indian Rupees or in any major foreign currency for the imported items (FOR/CIP destination). Octroi will be payable at actual on production of proof of payment but delivery within Octroi limits must be done only with prior approval of Executive Director of the Region.

22.2. The breakup of price of each item of SOR in terms of basic Unit price, Excise duty, Sales Tax, Freight, Custom Duty, Forwarding, Packing, Insurance and any other Levies/charges already paid or payable by the tenderer shall be quoted in the SOR Chapter 2. Any changes in statutory duties/taxes after opening of technical bid will be to RailTel's account within the contracted delivery period.

22.3. All prices and other information like discounts etc. having a bearing on the price shall be written both in figures and in words in the prescribed offer form (SOR). In case of difference in words and figures, the amount written in words will be taken into consideration. In the event of any discrepancy between total unit cost and total cost, the value shown in total unit cost will be taken for evaluation purpose.

22.4. Fall Clause:- The tenderer shall undertake that in case the tenderer offers same type of material at a lower price to any other purchaser including Central/State/ Government Organization or Public Sector Undertaking, during the validity of purchase order, the equal benefit of lower prices will be passed on to RailTel. The tenderer will submit an undertaking to this effect while claiming the payment.

23. Clause wise Compliance

23.1. Clause wise compliance statement of the Technical Specifications (Chapter 3) and Commercial Terms & Conditions (Chapter 4) shall be enclosed with the offer along with the technical literature of the material and other documents in support of relevant clauses.

24. Inspection

24.1. Pre-shipment / pre-dispatch inspection shall be carried out at manufacturer's / tenderer's works/site by RailTel's authorized representative. At least part of the material should be offered for inspection within 60 days of issue of confirmed Purchase Order. Traveling, lodging & boarding expenses of RailTel's representative and charges for 3rd party inspection if any shall be borne by RailTel but necessary facilities to carry out tests/witness inspection shall be provided by the manufacturer/ tenderer, free of cost. Under exceptional circumstance, if it is not possible to carry out pre-dispatch inspection at manufacturer's premises, Exemption for the same shall be obtained from competent authority.

24.2. Along with inspection call, the tenderer/manufacturer shall submit details of test procedures, test programme, test parameters together with permitted values, etc., and their Quality Assurance Plan.

24.3. In case material fails during inspection, the fresh lot of material shall be offered without any extra cost, by the manufacturer/tenderer. In such a case, total cost of re-inspection including travel, lodging & boarding of the inspecting officials shall be to manufacturer's/ tenderer's account.

25. Force Majeure

25.1. If during the Agreement, the performance in whole or in part, by either 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

EVENTS), provided notice of happenings of any such EVENT is given by the affected party to the other, within twenty one (21) days from 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 Agreement shall be resumed as soon as practicable, after such EVENT comes to an end or ceases to exist.

25.2. 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 Agreement. Neither party shall be liable for any breach, claims, damages against the other, in respect of non-performance or delay in performance as a result of Force Majeure leading to such termination.

26. Settlement of Disputes

26.1. Any dispute or difference whatsoever arising between the parties out of or relating to the construction, meaning , scope, operation or effect of this contract or the validity or the breach thereof shall be settled by arbitration in accordance with the Arbitration and Conciliation Act, 1996 as amended and the award made in pursuance thereof shall be binding on the parties. The venue of such arbitration or proceedings thereof shall be New Delhi.

26.2. All arbitration proceedings shall be conducted in English. Recourse against any Arbitral award so rendered may be entered into court having jurisdiction or application may be made to such court for the order of enforcement as the case may be.

26.3. The Arbitral Tribunal shall consist of the sole Arbitrator appointed by mutual agreement of the parties.

26.4. Each of the parties agree that notwithstanding that the matter may be referred to Arbitrator as provided herein, the parties shall nevertheless pending the resolution of the controversy or disagreement continue to fulfill their obligation under this Agreement so far as they are reasonably able to do so.

27. Governing Laws

27.1. The Purchase Order 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.

28. Termination for Default

The purchaser may, without prejudice to any other remedy for breach of contract, by written notice of default, sent to the Tenderer, terminate this contract in whole or in part.

28.1. If the tenderer fails to deliver any or all of the goods within the time period(s) specified in the contract.

28.2. If the tenderer fails to perform any other obligation(s) under the contract; and

28.3. If the tenderer, in either of the above circumstance(s) does not remedy his failure within a period of 30 days (or such longer period as the Purchaser may authorize in writing) after receipt of the default notice from the Purchaser.

28.4. In case of any of the above circumstances the RailTel shall pay the supplier for all products and services delivered till point of termination as per terms and conditions of the contract. However any recovery and losses occurred to RailTel will be recovered from Contractor up to the value of contract.

29. Risk & Cost

29.1. If the contractor fails to deliver the equipment or honor the contractual commitment within the period fixed for such delivery in the contract, the Purchaser may terminate the Purchase contract in whole or in part, the Purchaser may proceed to purchase, upon such terms and in such manner as it deems appropriate, goods similar to those undelivered at no risk and cost to contractor. However, the security deposit of tenderer shall be forfeited/ Performance Bank Guarantee shall be encashed. The failed tenderer shall not be permitted to take part in the tender for balance work.

30. Termination for Insolvency

30.1. The purchaser may at any time terminate the Purchase order by giving written notice to the tenderer, without compensation to the tenderer, if the tenderer becomes bankrupt or otherwise insolvent as declared by the competent court provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the Purchaser.

31. **Rates during Negotiation**

The tenderer/s shall not increase his/their quoted rates including payment terms in case the RailTel Administration negotiates for reduction of rates. Such negotiations shall not amount to cancellation or withdrawal of the original offer and the rates originally quoted will be binding on the tenderer/s.

32. **Pre- Bid Conference & Clarification Requests**

Pre- bid conference for this tender will be held on date, time & venue as given in Bid Data Sheet (BDS) Chapter 5.

It is solicited that the written queries/ clarifications may be sent to the RailTel's office latest by the date as indicated in the Bid Data sheet (BDS) through e-mail to pawan@railtelindia.com with copy to asablania@railtelindia.com (in word format) & hard copy by post. All relevant clarifications sought will be addressed during the pre-bid meeting.

33. **Submission of Offers**

33.1. All offers in the prescribed forms should be submitted before the time and date fixed for the receipt of the offers.

33.2. In case the schedule of requirement quoted by tenderer is incomplete with reference to tender document, the offer is liable to be rejected.

33.3. ATTESTATION OF ALTERATION: No scribbling is permissible in the tender documents. Tender containing erasures and alterations in the tender documents are liable to be rejected. Any correction made by the tenderer/ tenderers in his/their entries must be signed (not initialed) by him/them.

33.4. The tenderer shall submit his tender in two copies in sealed cover on specified date & time as mentioned in BDS Chapter 5. Each copy of the tender shall be complete in all respects. The copies should be marked "Original" & "Duplicate". The original tender paper purchased from this office or down loaded from the RailTel web site shall be returned duly signed on each page along with the original offer.

33.5. The offer shall be submitted in two parts, Part-I - Credential Bid (Techno-Commercial Bid) & Part-II – Price Bid. Both bids shall be sealed in separate envelopes and both envelopes put in one large envelope. Both envelopes should bear the Tender No., its description and date of closing/opening.

33.5.1. Part-I "CREDENTIAL BID"; -The bid shall consist of the following:-

33.5.2. Offer Letter complete.

33.5.3. Schedule of Requirements with quantities but with prices blanked out (this will be a replica of price bid with prices blanked out).

33.5.4. Earnest Money in prescribed form.

33.5.5. Audited balance sheet duly attested by Notary Public.
33.5.6. Constitution of Firm and Power of Attorney.
33.5.7. Clause wise compliance to tender conditions.
33.5.8. Copies of purchase orders and other documents in support of meeting qualifying criteria.
33.5.9. Complete technical data and particulars of the equipment offered, as specified in the Tender papers together with descriptive literature, leaflets, Drawings, if any, complete with list etc.
33.5.10. Documentary proof of equipment being proven and working for more than 6 months in India or outside India along with user certificate and Contact Details of user/firm.
33.5.11. Technical proposal of tenderer in conformity with system design or alternative proposal of the tenderer, if any.
33.5.12. System Performance Guarantee as per Chapter 6 Form no. 2
33.5.13. The manufacturer claiming to qualify under the scope of rules for PMA (Preferential Market Access) must submit the declaration of VA (Value Addition) as required under the issued notification for the specified period (2012-13,2013-14 & 2014-15).
33.5.14. Any other information desired to be submitted by the tenderer.
33.5.15. NIL Deviation certificate

Note:The Credential Bid Part-I under no circumstances should contain any rates offered. Otherwise the tender offer shall be summarily rejected. This envelope shall be clearly superscribed with "CREDENTIAL BID (Part-I)" along with the Tender No. and its description in bold letters and seal`ed.

33.6. Part –II "Price Bid" must be submitted online mode only

34. Constitution of Firm and power of Attorney

34.1. Any individual(s) signing the tender or other documents connected therewith should specify whether he is signing:-
34.1.1. As sole proprietor of the concern or as attorney of the sole Proprietor.
34.1.2. As a partner or partners of the firm.
34.1.3. As a Director, Manager or Secretary in the case of Limited Company duly authorized by a resolution passed by the Board of Directors or in pursuance of the authority conferred by Memorandum of Association.

34.2. In the case of a firm not registered under the Indian Partnership Act, all the partners or the attorney duly authorized by all of them should sign the tender and all other connected documents. The original Power of Attorney or other documents empowering the individual or individuals to sign should be furnished to the Purchaser for verification, if required.

34.3. The RailTel will not be bound by Power of Attorney granted by the tenderer or by the changes in the composition of the firm made subsequent to the execution of the contract agreement.

34.4. In case where the Power of Attorney partnership deed has not been executed in English, the true and authenticated copies of the translation of the same by Advocate, authorized translators of Courts and Licensed Petition Writers should be supplied by the Contractor(s) while tendering for the work.

34.5. The duly notorised Power of Attorney shall be submitted in original or duly signed.

35. Opening of Tender

35.1. Tenderer's Credential Bid (Part-I) will be opened on specified date & time as mentioned in BDS Chapter 5 of the tender in presence of such Tenderers/ Representatives who choose to be present.

35.2. After scrutinizing Credential Bid, "Price Bid (Part- II)" will be opened on a time and date to be informed separately in presence of those Tenderers who qualify in "Credential

Bid (Part-I)" as per qualifying criteria laid down in Clause 12 of this Chapter and who choose to be present.

35.3. Price Bid (part-II) envelops of those Tenderers who are not found to meet tender conditions will not be opened.

36. Non-Transferability & Non-Refund ability

36.1. The tender documents are not transferable. The cost of tender paper is not refundable.

37. Errors, Omissions & Discrepancies

37.1. The Contractor(s) shall not take any advantage of any mis-interpretation of the conditions due to typing or any other error and if in doubt, shall bring it to the notice of the purchaser without delay. In case of any contradiction only the printed rules, and books should be followed and no claim for the mis-interpretation shall be entertained.

38. Wrong Information by Tenderer

If the tenderer/s deliberately gives/give wrong information in his/their tender which creates/create circumstances for the acceptance of his/their tender the RailTel reserves the right to reject such tender at any stage.

39. The envelope shall be addressed to the Purchaser at the following address:

Group General Manager/DNM
RailTel Corporation of India Ltd.
Plot No. 143, Institutional Area,
Opposite-Gold Souk,
Sector-44, Gurgaon-122003

40. The envelope shall bear name of the tender, the tender no. and the words “DO NOT OPEN BEFORE” (due date).

41. Offer / Bid should be delivered to the above address so as to reach up to 15:00 Hrs of due date. The offers / bids shall be opened at 15:00 Hrs on the same day in the above office in the presence of those representatives of the bidders who choose to be present. Offers / Bids received after due date and time shall be dealt as per extant rules.
In case the date of opening happens to be a holiday, the tender will be received and opened at the same time on the next working day.

42. **Limitation of Liability**

Provided the following does not exclude or limit any liabilities of either party in ways not permitted by applicable law:

42.1. The Supplier shall not be liable to the Purchaser, whether in contract, tort, or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the Supplier to pay liquidated damages to the Purchaser; and

42.2. The aggregate liability of the Supplier to the Purchaser, whether under the Contract, in tort or otherwise, shall not exceed the total Contract Price, provided that this limitation shall not apply to any obligation of the Supplier to indemnify the Purchaser with respect to intellectual property rights infringement.

****

CHAPTER- 5

BID DATA SHEET (BDS)

The section consists of provisions that are specific to various Clauses of the tender document COMMERCIAL TERMS & CONDITIONS Chapter 4.

Clause	Description
Clause 1.2	Validity of offer 120 days.
Clause 2	Warranty 12 months after Installation of Equipment and issue of the PAC.
Clause 4	Delivery Period Delivery and supervision of installation and commissioning within 180 days of issue of Purchase Order
Clause 12.1.1	Technical Capability The Tenderer/bidder should be an Original Equipment Manufacturer (OEM) or Authorized partner of OEM specifically authorized by OEM for bidding in this tender. The OEM should have proven facilities for Engineering, manufacture, assembly, integration and testing of offered system and basic facilities with respect to space, Engineering, Personnel, Test equipment, Manufacture, Training, Logistic Supports for at least past three years in the country from where the proposed equipment are planned to be supplied
Clause 12.1.2	The Tenderer/bidder should have supplied and provision of similar offered security solution with satisfactory working as to Government/PSUs/Telecom Service Providers/Public Listed Company during the last three years from the date of opening of tender.
Clause 12.2.1	**Financial Criteria** i) The tenderer should present at least four (4) projects each worth at least INR 50 lakhs showcasing supply, design, installation,testing, commissioning, implementation and operations projects for security solutions commercially in India in the last 2 years. Copy of work orders supported with relevant documentary evidences for the design parameters as mentioned in criteria 4 and the completion certificates by the client. Documentary evidence should clearly indicate the nature of systems implemented for each project ii) The sum total of the turnover of contractual payment received during the last preceding 3 financial years from the date of opening of tender should be Minimum of Rs. 200 Cr.
Clause 18.1	Purchaser's Right to Vary Quantities Up to a maximum extent of +/- 30% of SOR quantity.

Clause	Description
Clause 22.1	Earnest Money Deposit (EMD)/ Bid Security Rs. 5,00,000/- (Rs. Five lacs)
Clause 34	Pre- Bid Conference & Clarification Requests Last date of Submission of Clarification Date: 02.06.2016 Pre- bid Conference date Date: 03.06.2016 Time: 15:00 hours Venue: Corporate Office RailTel
Clause 35.4	Last Date of Submission of Offer Date: 21.06.2016 1500 hrs Time: 15:00 hours Venue: same as above
Clause 37.1	Date of Opening of Tender Date: 21.06.2016 Time: 15:30 hours Venue: same as above

****

E-TENDER NO.RAILTEL/TENDER/OT/CO/DNM/2016-17/DDOS/330

CHAPTER- 6

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 6th Floor, IIIrd Block, Delhi Technology Park, Shastri Park,Delhi-110053 (Herein after called RailTel) 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.

Dated the day of 2015

for ……..

(indicate the name of the Bank)

Witness

1. Signature
   Name

2. Signature
   Name

Form No. 2

PROFORMA FOR THE SYSTEM PERFORMANCE GUARANTEE

(On Stamp Paper of Rs. One hundred)

The Director,
RailTel Corporation of India Limited

I / We ……. hereby guarantee that the design on the basis of which we have submitted our tender no. …… has been carefully made to conform to the end objectives in the tender documents and to technical specification therein. We further guarantee that in the event of the performance of the system, when installed, not complying with the end objectives or with the specifications contained in the tender documents, we shall provide further inputs to enable the RailTel to realize the end objectives contained in these documents without any additional payment for any additional equipment which may be required in this regard. We further guarantee that all the expenses for providing the additional inputs under the System Guarantee will be borne by us. We further guarantee that these additional inputs will be provided by us to make the system workable within 1 month from the date on which this guarantee is invoked by the Purchaser. The guarantee is valid for a period of one year from the date of commissioning of the system.

(Signature of Firm's Authorized Officer)

Seal

Signature of witness:

1. …….

2. …….

Annexure-1

Form No. 3

PROFORMA FOR THE LONG TERM MAINTENANCE SUPPORT
(To be signed by the O.E.M.)

To

The Director,
RailTel Corporation of India Limited

I / We ……. hereby confirm and accept that against RailTel Tender No. …….. , there is a requirement of Long Term Maintenance Support as per Clause 3. We confirm that Long Term Maintenance Support shall be met by us directly or through Authorized partner, as the case may be based on contracts. I / We have gone through the requirement mentioned in the Tender document and shall provide services for the offered supply items.

(Signature of Firm's Authorized Officer)
Seal

Signature of witness:

1. ……

2. …….

.

END of Tender Document
****