Corrigendum - II

"Supply, Installation, Testing & Commissioning of DDoS Solution for MPLS Network of RailTel and Licenses"

RailTel Corporation of India Ltd.

6th Floor, Plate-A, Office Block-2, NBCC Building, East Kidwai Nagar

New Delhi -110023, Ph: 011-22900600, Fax: 011-22900699

Website: www.railtelindia.com

In reference to Tender for **Supply, Installation, Testing & Commissioning of DDoS Solution for MPLS Network of RailTel and Licenses, etc. of RailTel** against **Tender No. RAILTEL/TENDER/OT/CO/ITP/2022-23/ DDoS & DC-DR Licenses/003 dated 10.02.2023,** all are advised to note following changes in the tender document:

SN	Pg. No.	RFP Clause No	RFP Clause	Revised Clause
1	23	General Requirements Clause 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.	Deleted
2	38	SOR- B-1 – DDoS for Application Layer, SN.8	The solution should support Brute Force attack mitigation and BOT mitigation using Source Verification with CAPTCHA	The solution should support Brute Force attack mitigation and BOT mitigation using either Source Verification with CAPTCHA or any other technique.
3	39	SOR- B-1 – DDoS for Application Layer, SN-26	The appliance should be high performance purpose built next generation multi tenant hardware with Network function virtualization. The Appliance should support multiple network functions virtualization with dedicated hardware resources for each virtual instance. It should also run 3rd party and open source network functions on same appliance like Linux- CenOS/Ubuntu based applications.	Deleted
4	39	SOR- B-1 – DDoS for Application Layer, SN-29	Support for endpoint security and VPN with 2FA including HDD ID, CPU ID, OS ID.	Deleted
5	39	SOR- B-1 – DDoS for Application Layer, SN-30	The Proposed solution should have Endpoint Security Check and baselining of Endpoint to ensure only verified systems can access through the device. E.g.: Antivirus, Patching, etc	Deleted
6	39	SOR- B-1 – DDoS for Application Layer, SN-51	Offered solution must be natively integrated at various customer deployments with Splunk, Sev1, ArcSight, Extra hop, ELK, Grafana and others	Offered solution must be natively integrated at various customer deployments with SIEM Solutions like Splunk, ArcSight, Qradar etc.
7	40	Technical Specification for SOR-C1, C2, C3 and C4:	RHEL for Virtual Data Centre with 3 years of **standard support** for Unlimited VMs- 40 Nos.	RHEL for Virtual Data centre-Unlimited Guest with **Premium support**- 40 Nos.

SN	Pg. No.	RFP Clause No	RFP Clause	Revised Clause
8		Point no. 3 of Clause 12.1.1 of Chapter-4, **(Eligibility Criteria for Bidder)**	**Definition of Similar work under Technical Capability:** # Similar Work: Projects of Supply, installation and commissioning of Data Center Hardware/Software Solution items in Government / PSUs / Telecom Service Providers network/ISP Network/ Public listed company^.	**Definition of Similar work under Technical Capability:** # Similar Work: Projects of Supply, installation and commissioning of Data Center Hardware/Software Solution items/ Security Solution (Firewall/ IPS/ WAF/ DDoS) in Government / PSUs / Telecom Service Providers network/ISP Network/ Public listed company^.
9	52	Clause 5.4 of Chapter-4 3.3 (Payment terms)	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 Contract Management Authority i.e. GM/ITP/CO for certifying and verification and onwards submission to Finance of RailTel Corporate Office for releasing the payment	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 DGM level officer for certifying and verification and onwards submission to Finance of RailTel Corporate Office for releasing the payment.
10	57	Point no. 1 of Clause 12.2 of Chapter-4, (Eligibility Criteria Requirements for OEM's)	**Eligibility Criteria Requirements:** The Equipment offered by the OEM or equipment/software of the same series/family from the same OEM should have been satisfactorily working in 3 Government/PSUs/Telecom Service Providers/ Public Listed Company for at least more than 12 months as on date of opening of tender, in India or Abroad. Work experience certificate issued by Public listed company having average annual turnover of Rs 500 Cr and above in last 3 financial years excluding the current financial year, listed on National Stock Exchange or Bombay Stock Exchange or any global stock exchange, incorporated/registered at least 5 years prior to the date of opening of tender, shall also be considered provided the work experience	**Eligibility Criteria Requirements:** The Equipment offered by the OEM or equipment/software of the same series/family from the same OEM should have been satisfactorily working in Government/PSUs/Telecom Service Providers/ Public Listed Company for at least more than 12 months as on date of opening of tender, in India or Abroad. Work experience certificate issued by Public listed company having average annual turnover of Rs 500 Cr and above in last 3 financial years excluding the current financial year, listed on National Stock Exchange or Bombay Stock Exchange or any global stock exchange, incorporated/registered at least 5 years prior to the date of opening of tender, shall also be considered provided the work experience

SN	Pg. No.	RFP Clause No	RFP Clause	Revised Clause
			certificate has been issued by a person authorized by the Public listed company to issue such certificates	certificate has been issued by a person authorized by the Public listed company to issue such certificates
11	57 & 58	SN. 1 of Clause 12.2 of Chapter-4, (Eligibility Criteria Requirements for OEM's)	**Supporting Document Required** Satisfactory Working certificate from **End User** clearly mentioning the make & model number of the offered Hardware. An undertaking by the OEM has to be submitted in support, in case issued satisfactory working certificate is the immediate predecessor of same series/family of the offered Hardware.	**Supporting Document Required** Satisfactory Working certificate from **End User** clearly mentioning the make & model number of the offered Hardware. Or OEM should submit self-certificate for Satisfactory Working with proper contact detail of End User where hardware / software deployed (PO No., Issued Date, Purchaser Organization Details - Firm Name, Firm Address, Name of Contact person, Designation, Telephone Number, Fax, Official mail id etc.) An undertaking by the OEM has to be submitted in support, in case issued satisfactory working certificate is the immediate predecessor of same series/family of the offered Hardware.
12	71	Under Clause 41 (a) of Chapter-4 (**Integrity Pact Program**)	**Name & contact details of Nodal Officer (IP) in RailTel:** General Manager/NTP RailTel Corporation of India Ltd 6th Floor, Office Block Tower-2, NBCC Complex, East Kidwai Nagar, New Delhi-110023 E-Mail: pawaria@railtelindia.com	**Name & contact details of Nodal Officer (IP) in RailTel:** General Manager/ITP RailTel Corporation of India Ltd 6th Floor, Office Block Tower-2, NBCC Complex, East Kidwai Nagar, New Delhi-110023 E-Mail: hjp@railtelindia.com
13	94	Clause 7.6.2 of Chapter-7 3.3 (Performance Bank Guarantee)	The contractor is required to submit a Performance Bank Guarantee (PBG) within 30 days from the date of issue of LOA for AMC @ 10% of the annual value of AMC (or as per Government of India guidelines applicable at the time of issue of LOA/PO for AMC) valid for a period of 4 months beyond the	The contractor is required to submit a Performance Bank Guarantee (PBG) within 30 days from the date of issue of LOA for AMC @ 3% of the value of issued LOA for AMC (or as per Government of India guidelines applicable at the time of issue of LOA/PO for AMC) valid for a period of 4 months beyond the

SN	Pg. No.	RFP Clause No	RFP Clause	Revised Clause
			AMC period of 5 years from the date of issue of LOA. The Proforma for PBG is given in Form No. 1 of tender document. If the AMC period got extended, the PBG will also be extended accordingly.	completion of AMC from the date of LOA for due fulfillment of long term maintenance. The Proforma for PBG is given in Form No. 1 of tender document. If the AMC period got extended, the PBG will also be extended accordingly.

The last date of submission of bids is also extended from 17.03.2023 to 22.03.2023. The tender will be opened at 15:30 Hrs. on 22.03.2023.

The response of queries is attached as Annexure-I. All other term & conditions of tender documents will remain same.

Rajeev Kumar
11/03/2023

(Rajeev Kumar)
Dy. General Manager/ITP

Annexure-I

SN	Clause no. & Chapter no.	Page No.	Content of the tender Clause	Change asked by firm	Justification by Firm	RailTels Response / Clarification
1	SOR-A: A-1	6	DDOS Detection Device Collector / Traffic Routing & Analytics platform with 04 Nos. of SFP-1G per appliance for the Detection/ Collector device and 3 Years of Warranty, Maintenance & Support for all supplied items as per Technical Specification given in Chapter-3A	Does Railtel require 4 Collectors? Are the Leader / Backup Leader or Controller with HA part of the 4 units requested. Or they need to be proposed separately.	This would help us in better estimation and propose a techno-commercially feasible solution	As per tender.
2	SOR-A: A-4	6	OEM Professional services for installation, Implementation and deployment of supplied hardware/ software etc. as per Technical Specification given in chapter-3A	The Professional Services will be required to be onsite to do the deployment or remote support is acceptable?	This would help us in better estimation and propose a techno-commercially feasible solution	**Clarification- Bidder to facilitate onsite resources and OEM professional services can be remote to deliver the scope as per SOR-A 4**
3	SOR-B: B-1	6	Application Layer DDoS with HA at both DC and DR (2 box at DC and 2 Box at DR) with 3 Years of Warranty as per Technical Specification given in chapter-3A	The Clause mentions 4 units whereas the quantity Column mentions 2 units. Pls calrify how many units are required.	This would help us in better estimation and propose a techno-commercially feasible solution	**Clarification- In the tender DDoS Solution has been asked with HA, hence quantity is mention 2. However to provide the solution in HA, bidder has to provision total 4 units ie. 2 units at DC and 2 units at DR.**
4	XII	9	The tenderer shall make available the offered products during technical evaluation for testing and benchmarking to RailTel at any testing facility approved by RailTel. Tenderer shall provide all the required equipment and accessories for above testing at testing facility. Tenderer shall bear all the cost of above testing. RailTel shall provide only rack space and power supply. Decision of RailTel shall be final and binding in this regard.	Railtel did not explain anywhere in the RFP regarding What kind of Testing and Benchmarking is required? Pls help clarify.	This would help us in better estimation and propose a techno-commercially feasible solution	As per tender.
5	Clause 4.8: S. No. i	21	RailTel has existing DDoS deployment and would continue to use the existing Licenses & Mitigation capacity in the deployment as per Annexure-1	This part of RFP mentions Railtel would continue to use existing licenses and mitigation capacities, whereas in earlier clause the ask is for 3 mitigation units. If the vendor intends to proposed a new solution which is not compatible with existing deployment, then the vendor has to propose everything from scratch ?	This would help us in better estimation and propose a techno-commercially feasible solution	As per tender.
6	Clause 4.8: S. No. ii	21	The DDOS mitigation system, DDOS detection system, Traffic Analytics, Forensics System & CDN/OTT Visibility solution proposed to RailTel must be from single vendor and a common User Interface.	Request you to kindly make it open, so that multiple OEMs in industry providing similar functionality, even though there would be different User Interfaces for Detection, Mitigation, Analytics and MSSP Portal may qualify	This would help us to propose a techno-commercially feasible solution	As per tender.
7	Clause 4.8: S. No. iii	21	The refresh involves following components: a. 2 Platforms with Collector role. b. 2 Platforms with User Interface role. c. 2 Platforms with Mitigation / Scrubbing role (The existing deployment will be used)	As per SOR-A: A2, The number of mitigation units required are 3 Qty. However the clause in question mentions 2 mitigation units. This arises confusion. Pls suggest whether 2 mitigation units are required or 3 ?	This would help us in better estimation and propose a techno-commercially feasible solution	As per tender.

8	SOR-A2: SN 7	29	The system shall be able to directly BGP peer with multiple switches/routers in the network.	Both Detection and Mitigation systems peering with routers is not required. Detection system alone do bgp peering and provide same results.	The system shall be able to do BGP peering with multiple switches/routers in the network from either the Detection system or the mitigation system.	As per tender.
9	SOR-A2: SN 14	29	The system shall support BGP flow spec diversion mechanism for diverting traffic to scrubbing center.	BGP Flowspec diversion can be done from Detection system as well, so this function is not required on mitigation system.	The system shall support BGP flow spec diversion mechanism for diverting traffic to scrubbing center from either Detection or mitigation system.	As per tender.
10	SOR-A2: SN 20	30	Mitigation reporting must be available from common User Interface which is also a centralised configuration, management, reporting of detection and mitigation system.	There are basic mitigation reports and then detailed mitigation reports. The reports are important and how they are fetched should not be limited.	Basic mitigation reports are usually available from common User Interface, whereas detailed mitigation reports are available from the dedicate UI of mitigation portal.	As per tender.
11	SOR-A2: SN 27	30	The Proposed Solution shall use Learning Mitigation mechanism to provide correct baselines for mitigation countermeasures without dropping the traffic.	Every solution vendor has different nomenclature. Learning Mitigation is vendor specific, Behaviour Analysis is another terminology.	The Proposed Solution shall use Learning Mitigation mechanism or behaviour analysis to provide correct baselines for mitigation countermeasures without dropping the traffic.	As per tender.
12	Reporting for Mitigation System: Pt 9	31	The system shall allow mitigation parameters to be changed while mitigation is running.	Changing mitigation parameters during ongoing mitigation require dedicated interface for mitigation devices. This cannot be achieved from a single User Interface.	The system shall allow mitigation parameters to be changed while mitigation is running from either single User Interface or via dedicated management portal for mitigation units.	As per tender.
13	SOR-A3: Data Ingestion: SN 27	35	System should enrich flows with CDN and OTT provider names without relying on integration with DNS ingestor.	it is not possible to prvoide CDN OTT vsibility without dns ingestor. Manually configuring CDN Names and prefixes / ASN is not the right approach.	DNS Ingestor must be made mandatory for CDN OTT Visibility.	As per tender.
14	SOR- A-3 - Analytics & Forensics: [Reports & Queries: xxi]	36	The solution must be able to classify OTT sites and services in categories such as Streaming video, Collaboration, Private Cloud, Public Cloud, Social media, Messaging, Gaming etc.	OTT categorisation is not possible with flow based solution and that too without DNS Ingestor.	Request to delete this clause.	As per tender.
15	SOR- A-3 - Analytics & Forensics: [CDN and OTT Visibility: xiii]	36	System support future integration of DNS Ingestor for DNS data ingestion in real-time to enrich flows with CDN Data.	it is not possible to prvoide CDN OTT vsibility without dns ingestor. Manually configuring CDN Names and prefixes / ASN is not the right approach.	DNS Ingestor must be made mandatory for CDN OTT Visibility from Day1.	As per tender.
16	Scope 2.1 DDOS SOR- A-3 - Analytics & Forensics:	21	DDoS Detection & DDoS Mitigation system should be from single OEM.	As you have requested for Analytics functionality as well is that also required from same OEM	DDoS Detection , DDoS Mitigation & Analytics system should be from single OEM.	As per tender.
17	3. Long Term Maintenance Support Clause 3.1	50	Bidder shall provide maintenance support for a minimum period of 5 years after successful completion of warranty obligations. The long term maintenance support shall be comprehensive and include all hardware and software equipment supplied against this contract. RailTel should be extended the benefits of software update/up-grades made by OEM on the system from time to time to improve performance. During this period the scope of work as mentioned in clause 2 above & its sub clauses will be applicable.	The warranty support requested in this RFP is 3 yrs upfront do you mean 3 yrs + 5 yrs AMC total support commitment for 8 yrs ?	Bidder shall provide maintenance support for a minimum period of 5 years after successful completion of installation obligations. The long term maintenance support shall be comprehensive and include all hardware and software equipment supplied against this contract. RailTel should be extended the benefits of software update/up-grades made by OEM on the system from time to time to improve performance. During this period the scope of work as mentioned in clause 2 above & its sub clauses will be applicable. Total support commitment for 3yrs upfront and 2 yrs AMC	As per tender.

18	12.2. Eligibility Criteria Requirements for OEM's: Serial no 2	58	OEM should have supplied the equipment offered or equipment/software of the same series/family at least of Rs. 7.39 Cr. during last preceding 5 financial years (i.e. current year and five previous financial years) as on opening date of bid to Government/PSUs /Telecom Service Providers / Public Listed Company in India or Abroad or 35% of their offered equipment cost by respective OEM against SOR.	If OEM is submitting the letter from the customer & user having all the details is that acceptable ? As OEM's don't have access to the commercial value of end customer to SI's If OEM gives self certification for the PO booked in last 5 yrs consolidated will that be acceptable		For required amount, multiple POs in favour of OEM's System Integrators are also acceptable
19	Form No. 7 OEM Undertaking on Letter Head (To be signed by the OEM) C. We Certify that, iii	86	Security breach or damages to system, if any, so caused by any embedded malicious code or otherwise, due to the act of either OEM or bidder or both, the OEM as well as the bidder would be considered liable jointly or severally and shall be banned for conducting any business with RailTel. Also the present contract, may liable to be terminated by the purchaser.	OEM / bidder can ensure the same once the system is delivered , installed and commissioned in Railtelnetwork and handed over to Railtel. Security of devices & SW post that will be responsibility of Railtel ?		As per tender.
20	SOR- B-1 – DDoS for Application Layer, SN - 3	38	Legitimate/clean throughput handling: 20 Gbps from day one and scalable up to 40 Gbps SSL CPS (2K Key): 100,000 and (ECC p256): 75K Ports: 8 x 10G SFP+ and 4 x 1G SFP from day-1 and additional 4 x 10G/1G SFP for future use, 4 TB HDD and 512 GB RAM	Now a days, 95 percent of the traffic are SSL and L4 CPS, L7 RPS based these parameters are very critical, however there is no SSL TPS and L4 CPS, L7 parameter mentioned in the specifications. It is suggested to amend the clause as "**Legitimate/clean throughput handling: 20 Gbps from day one and scalable up to 40 Gbps SSL CPS (2K Key): 100,000 and (ECC p256): 75K with minimum 8M L7 requests per second Ports: 8 x 10G SFP+ and 4 x 1G SFP from day-1 and additional 4 x 10G/1G SFP for future use, 4 TB HDD and 512 GB RAM"**	Layer 7 requests per second is not mentioned in this clause. So, we would like to request the honorable tendering committee to amend this.	As per tender.
21	44	39	The OEM should be Make in India Class 1 Vendor.	In Case of Make in India Class 1 Vendor, OEM should have OEM TAC based in India. **So it is suggested to amend the clause "The OEM should be Make in India Class 1 Vendor and should have OEM TAC based in India."**	We would like to request the honorable tendering committee to amend this clause to get better OEM support.	As per tender.
22	4.8. General Requirement, SN: ii	21	The DDOS mitigation system, DDOS detection system, Traffic Analytics, Forensics System & CDN/OTT Visibility solution proposed to RailTel must be from single vendor and a common User Interface.	As asked in the RFP clause, This feature is only supported by a single OEM/vendor and hence is proprietary in nature. **It is suggested to delete the clause. Also, clarify that asked clasue is for SOR-A and SOR-B. Or Two different OEM can participate in SOR-A and SOR-B.**	We would like to request the honorable tendering committee to amend this clause for wider participation and to get the best technocommercial solution available in the market.	As per tender.
23	2.1.13	20	DDoS Detection & DDoS Mitigation system should be from single OEM.	As asked in the RFP clause, DDoS Detection & DDoS Mitigation system should be from single OEM. **So please clarify that asked clasue is for SOR-A and SOR-B. Or Two different OEM can participate in SOR-A and SOR-B.**	We would like to request the honorable tendering committee to amend this clause for wider participation and to get the best technocommercial solution available in the market.	**Clarification- SOR-A and SOR-B are individual items, hence two different OEM may also participate.**

24	25.Force Majeure	69	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.	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. However, RailTel shall pay all the outstanding amount due which have been incurred by the Bidder during the performance of the Contract.	In event of termination of Contract due to occurrence of FM event, Supplier should be entitled to receive all the outstanding payments keeping the Financial interest of the organization in mind.	As per tender.
25	41. Limitation of Liability	74	Provided the following does not exclude or limit any liabilities of either party in ways not permitted by applicable law: 41.1. 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 41.2. 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.	Provided the following does not exclude or limit any liabilities of either party in ways not permitted by applicable law: 41.1. 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 41.2. The aggregate liability of the Supplier to the Purchaser, whether under the Contract, in tort or otherwise, shall not exceed the applicable affceted portion of purchase order giving rise to such liability. ~~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.	In order to capture the liabilities of the parties we have modified the said clause and mitigated our liability capping as the same is critical from financial as well as legal perspective.	As per tender.
26	7.6.10 Determination of Contract	102	Right of RailTel to determine the contract: The RailTel shall be entitled to determine and terminate the contract at any time, should in the RailTel's opinion, the cessation of the work becomes necessary owing to paucity of funds or from any other cause whatever, in which case the value of approved materials at site and of work done to date by the Contractor will be paid for in full at the rate specified in the contract. Notice in writing from the RailTel of such determination and the reasons thereof shall be conclusive evidence thereof.	Right of RailTel to determine the contract: The RailTel shall be entitled to determine and terminate the contract at any time by giving 30 (thirty) days prior written notice, should in the RailTel's opinion, the cessation of the work becomes necessary owing to paucity of funds or from any other cause whatever, in which case the value of approved materials at site and of work done to date by the Contractor will be paid for in full at the rate specified in the contract. Notice in writing from the RailTel of such determination and the reasons thereof shall be conclusive evidence thereof.	There should be a reasonable timeline before terminating the contract,so that the Tenderer should have sufficent time to conclude their transactions with subcontractors/vendors/OEMs etc.	As per tender.

27	clause 3.3 of long term support	50	Separate LOA for AMC shall be issued by RailTel before completion of warranty period and separate Agreement shall be signed with the Bidder. A fresh Bank Guarantee valid for a period of 4 months beyond the completion of AMC from the date of LOA shall be required to be submitted by OEM/ Tenderer for due fulfillment of long term maintenance support obligation. Value of PBG will be 3% of the value of issued LOA for AMC or as per Government of India guidelines applicable at the time of issue of LOA for AMC. This PBG of AMC shall be submitted by the bidder within 30 days from the date of issue of LOA for the AMC. In case bidder does not submit the PBG in the stipulated time period, RailTel may encash the PBG given with the original LOA.	Plese explain PBG is either of 3% or 10% for the AMC period as the same is mentioned differently in both clause	This will help us in better estimation	Please see corrigendum
	clause 7.6.2	94	Performance Bank Guarantee: The contractor is required to submit a Performance Bank Guarantee (PBG) within 30 days from the date of issue of LOA for AMC @ 10% of the annual value of AMC (or as per Government of India guidelines applicable at the time of issue of LOA/PO for AMC) valid for a period of 4 months beyond the AMC period of 5 years from the date of issue of LOA. The Proforma for PBG is given in Form No. 1 of tender document. If the AMC period got extended, the PBG will also be extended accordingly.			**Corrigendum**
28	Technical Specification for SOR-C1, C2, C3 and C4:	40	RHEL for Virtual Data Centre with 3 years of standard support for Unlimited VMs- 40 Nos.	As we understand from RFP, this is a requirment for the Production environment. Please clarify , do you need 24*7*365 support?		**Corrigendum**
29	SOR- A-4 - OEM Professional services:	37	Low Level Design Document – LLD	Please confirm if any OEM Professional services required from RHEL component perspective.		As per tender.
30	SOR- A-4 - OEM Professional services:	37	Onsite Knowledge Transfers and Support Handover-	Please confirm if any OEM training is required for RHEL (Red Hat Enterprise Linux)?		As per tender.
31	Technical Specification for SOR-C1, C2, C3 and C4:	40	Bidder is required to supply latest versions of the following software at Data Centre (GGN-DC, SC-DC,) as per below mentioned qty.- Red Hat Enterprise Linux Server Physical or Virtual Nodes, Up to 2 Physical CPU Sockets (2 Guest VMs) with Premium Subscription and support for 3 Years, - 47	Is the quantity mentioned for each component like example RHEL Server qty mentioned is 47, includes /caters to both Data Centre (GGN-DC and SC-DC)? Or Is it for one Data Centre and same to be counted for another DC as well?		**Clarification- Quantity mentioned i.e. 47, here is total required quantity, RailTel may further disctribute the same in DC and DR.**

32	Technical Specification for SOR-C1, C2, C3 and C4:	40	Bidder is required to supply latest versions of the following software at Data Centre (GGN-DC, SC-DC,) as per below mentioned qty.-	Will both the Data Center in Active-Active mode?		**Clarification- Quantity mentioned i.e. 47, here is total required quantity, RailTel may further disctribute the same in DC and DR**
33	Technical Specification for SOR-C1, C2, C3 and C4:	38	SOR- B-1 – DDoS for Application Layer:	We observe that RFP talks and ask about the Network ACL's, Detect Malicious IP, Patching, Policy enforcement, Compliance monitoring but it doesn't mention or define any specification for Automation platform/tool to do such activities. A tool/platform like Ansible possess all such functionality and widely been used in the Industry. Any thoughts on the same line?		As per tender.
34	General Requirements Clause 4.10	23	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.	Router specifications is not mentioned in the RFP. Request you to please provide the same.		**Corrigendum**
35	3.C. 12.1.1.3 Eligibility Criteria for Bidder	55	The tenderer must have successfully completed any of the following during last 07 (seven) years, ending last day of month previous to the one in which tender is invited: One similar work# costing not less than the amount Rs. 12.67 Cr. or Two similar works# each costing not less than the amount Rs. 8.44 Cr., or Three similar works# each costing not less than the amount Rs. 6.33 Cr., # Similar Work: Projects of Supply, installation and commissioning of Data Center Hardware/Software Solution items in Government / PSUs / Telecom Service Providers network/ISP Network/ Public listed company^.	Request you to please amend the clause as following : The tenderer must have successfully completed any of the following during last 07 (seven) years, ending last day of month previous to the one in which tender is invited: One similar work# costing not less than the amount Rs. 12.67 Cr. or Two similar works# each costing not less than the amount Rs. 8.44 Cr., or Three similar works# each costing not less than the amount Rs. 6.33 Cr., # Similar Work: Projects of Supply, installation and commissioning of Data Center Hardware/ Software Solution/Security product/ Networking product items in Government / PSUs / Telecom Service Providers network/ISP Network/ Public listed company/ Large Corporate. Note: ^ - Work experience certificate issued by Public listed company/ Large Corporate having average annual turnover of Rs 500 Cr and above in last 3 financial years excluding the current financial year, listed on National Stock Exchange or Bombay Stock Exchange, incorporated/registered at least 5 years prior to the date of opening of tender, shall also be considered provided the work experience certificate has been issued by a person authorized by the Public listed company to issue such certificates.	Request you to please consider our requests to have larger participation in the tender so that department can avail benefit for calling the open tender	As per tender.

36			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: i) Tax Invoice (GST) ii) Delivery Challan/e-way bill. iii) Packing list. iv) Factory Test Report/Certified manufacturer Test Report v) Purchaser's Inspection certificate vi) Consignee receipt vii) Warranty certificate of OEM viii) Insurance certificate ix) Certificates duly signed by the firm certifying that equipment/ materials being delivered are new and conform to technical specification.	Request you to please amend the clause as following : 5.1. Payment shall be made in Indian Currency (Rs) 85% 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: i) Tax Invoice (GST) ii) Delivery Challan/e-way bill. iii) Packing list. iv) Factory Test Report/Certified manufacturer Test Report v) Purchaser's Inspection certificate vi) Consignee receipt vii) Warranty certificate of OEM viii) Insurance certificate ix) Certificates duly signed by the firm certifying that equipment/ materials being delivered are new and conform to technical specification.	Request you to please consider our requests since this project is mainly of CAPEX and department can avail benefit for calling the open tender.	As per tender.
37			5.2. 15% payment of the value of Supply items of the PO shall be made by RailTel on successfully Installation & Commissioning at site based on SAT Report issued by RailTel DC Team, 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 Contract Management Authority i.e. GM/ITP/CO. 5.3. 15% payment of value of supply items of the PO which could not be installed and commissioned within 180 days due to site readiness or other reason on account of RailTel will be made with approval of Contract Management Authority i.e. GM/ITP/CO and remaining (5% + 5%) on issue of PAC and FAC as per clause 5.2.	5.2. 10% payment of the value of Supply items of the PO shall be made by RailTel on successfully Installation & Commissioning at site based on SAT Report issued by RailTel DC Team 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 Contract Management Authority i.e. GM/ITP/CO. 5.3. 10% payment of value of supply items of the PO which could not be installed and commissioned within 180 days due to site readiness or other reason on account of RailTel will be made with approval of Contract Management Authority i.e. GM/ITP/CO and remaining (5%) on issue of FAC as per clause 5.2.		As per tender.
38	SOR-A: A-1	6	DDOS Detection Device Collector / Traffic Routing & Analytics platform with 04 Nos. of SFP-1G per appliance for the Detection/Collector device and 3 Years of Warranty, Maintenance & Support for all supplied items as per Technical Specification given in Chapter-3A	Does Railtel require 4 Collectors? Are the Leader / Backup Leader or Controller with HA part of the 4 units requested. Or they need to be proposed separately.		As per tender.

39	SOR-A: A-4	6	OEM Professional services for installation, Implementation and deployment of supplied hardware/ software etc. as per Technical Specification given in chapter-3A	The Professional Services will be required to be onsite to do the deployment or remote support is acceptable?		**Clarification- Bidder to facilitate onsite resources and OEM professional services can be remote to deliver the scope as per SOR-A 4**
40	SOR-B: B-1	6	Application Layer DDoS with HA at both DC and DR (2 box at DC and 2 Box at DR) with 3 Years of Warranty as per Technical Specification given in chapter-3A	The Clause mentions 4 units whereas the quantity Column mentions 2 units. Pls calrify how many units are required.		**Clarification- In the tender DDoS Solution has been asked with HA, hence quantity is mention 2. However to provide the solution in HA, bidder has to provision total 4 units ie. 2 units at DC and 2 units at DR.**
41	XII	9	The tenderer shall make available the offered products during technical evaluation for testing and benchmarking to RailTel at any testing facility approved by RailTel. Tenderer shall provide all the required equipment and accessories for above testing at testing facility. Tenderer shall bear all the cost of above testing. RailTel shall provide only rack space and power supply. Decision of RailTel shall be final and binding in this regard.	Railtel did not explain anywhere in the RFP regarding What kind of Testing and Benchmarking is required? Pls help clarify.		As per tender.
42	Clause 4.8: S. No. i	21	RailTel has existing DDoS deployment and would continue to use the existing Licenses & Mitigation capacity in the deployment as per Annexure-1	This part of RFP mentions Railtel would continue to use existing licenses and mitigation capacities, whereas in earlier clause the ask is for 3 mitigation units. If the vendor intends to proposed a new solution which is not compatible with existing deployment, then the vendor has to propose everything from scratch ?		As per tender.
43	Clause 4.8: S. No. ii	21	The DDOS mitigation system, DDOS detection system, Traffic Analytics, Forensics System & CDN/OTT Visibility solution proposed to RailTel must be from single vendor and a common User Interface.	This clause seems to favour a specific vendor. Railtel must be open to consider other solutions in the industry providing similar functionality, even though there would be different User Interfaces for Detection, Mitigation, Analytics and MSSP Portal.		As per tender.
44	Clause 4.8: S. No. iii	21	The refresh involves following components: a. 2 Platforms with Collector role. b. 2 Platforms with User Interface role. c. 2 Platforms with Mitigation / Scrubbing role (The existing deployment will be used)	As per SOR-A: A2, The number of mitigation units required are 3 Qty. However the clause in question mentions 2 mitigation units. This arises confusion. Pls suggest whether 2 mitigation units are required or 3 ?		As per tender.
45	SOR-A2: SN 7	29	The system shall be able to directly BGP peer with multiple switches/routers in the network.	Both Detection and Mitigation systems peering with routers is not required. Detection system alone do bgp peering and provide same results.	The system shall be able to do BGP peering with multiple switches/routers in the network from either the Detection system or the mitigation system.	As per tender.
46	SOR-A2: SN 14	29	The system shall support BGP flow spec diversion mechanism for diverting traffic to scrubbing center.	BGP Flowspec diversion can be done from Detection system as well, so this function is not required on mitigation system.	The system shall support BGP flow spec diversion mechanism for diverting traffic to scrubbing center from either Detection or mitigation system.	As per tender.

47	SOR-A2: SN 20	30	Mitigation reporting must be available from common User Interface which is also a centralised configuration, management, reporting of detection and mitigation system.	There are basic mitigation reports and then detailed mitigation reports. The reports are important and how they are fetched should not be limited.	Basic mitigation reports are usually available from common User Interface, whereas detailed mitigation reports are available from the dedicate UI of mitigation portal.	As per tender.
48	SOR-A2: SN 27	30	The Proposed Solution shall use Learning Mitigation mechanism to provide correct baselines for mitigation countermeasures without dropping the traffic.	Every solution vendor has different nomenclature. Learning Mitigation is vendor specific, Behaviour Analysis is another terminology.	The Proposed Solution shall use Learning Mitigation mechanism or behaviour analysis to provide correct baselines for mitigation countermeasures without dropping the traffic.	As per tender.
49	Reporting for Mitigation System: Pt 9	31	The system shall allow mitigation parameters to be changed while mitigation is running.	Changing mitigation parameters during ongoing mitigation require dedicated interface for mitigation devices. This cannot be achieved from a single User Interface.	The system shall allow mitigation parameters to be changed while mitigation is running from either single User Interface or via dedicated management portal for mitigation units.	As per tender.
50	SOR-A3: Data Ingestion: SN 27	35	System should enrich flows with CDN and OTT provider names without relying on integration with DNS ingestor.	it is not possible to prvoide CDN OTT vsibility without dns ingestor. Manually configuring CDN Names and prefixes / ASN is not the right approach.	DNS Ingestor must be made mandatory for CDN OTT Visibility.	As per tender.
51	SOR- A-3 - Analytics & Forensics: [Reports & Queries: xxi]	36	The solution must be able to classify OTT sites and services in categories such as Streaming video, Collaboration, Private Cloud, Public Cloud, Social media, Messaging, Gaming etc.	OTT categorisation is not possible with flow based solution and that too without DNS Ingestor.	Request to delete this clause.	As per tender.
52	SOR- A-3 - Analytics & Forensics: [CDN and OTT Visibility: xiii]	36	System support future integration of DNS Ingestor for DNS data ingestion in real-time to enrich flows with CDN Data.	it is not possible to prvoide CDN OTT vsibility without dns ingestor. Manually configuring CDN Names and prefixes / ASN is not the right approach.	DNS Ingestor must be made mandatory for CDN OTT Visibility from Day1.	As per tender.
53	Scope 2.1 DDOS SOR- A-3 - Analytics & Forensics:	21	DDoS Detection & DDoS Mitigation system should be from single OEM.	As you have requested for Analytics functionality as well is that also required from same OEM	DDoS Detection , DDoS Mitigation & Analytics system should be from single OEM.	As per tender.
54	3. Long Term Maintenance Support Clause 3.1	50	Bidder shall provide maintenance support for a minimum period of 5 years after successful completion of warranty obligations. The long term maintenance support shall be comprehensive and include all hardware and software equipment supplied against this contract. RailTel should be extended the benefits of software update/up-grades made by OEM on the system from time to time to improve performance. During this period the scope of work as mentioned in clause 2 above & its sub clauses will be applicable.	The warranty support requested in this RFP is 3 yrs upfront do you mean 3 yrs + 5 yrs AMC total support commitment for 8 yrs ?	Bidder shall provide maintenance support for a minimum period of 5 years after successful completion of installation obligations. The long term maintenance support shall be comprehensive and include all hardware and software equipment supplied against this contract. RailTel should be extended the benefits of software update/up-grades made by OEM on the system from time to time to improve performance. During this period the scope of work as mentioned in clause 2 above & its sub clauses will be applicable. Total support commitment for 3yrs upfront and 2 yrs AMC	As per tender.

55	12.2. Eligibility Criteria Requirements for OEM's: Serial no 2	58	OEM should have supplied the equipment offered or equipment/ software of the same series/family at least of Rs. 7.39 Cr. during last preceding 5 financial years (i.e. current year and five previous financial years) as on opening date of bid to Government/PSUs /Telecom Service Providers / Public Listed Company in India or Abroad or 35% of their offered equipment cost by respective OEM against SOR.	If OEM is submitting the letter from the customer & user having all the details is that acceptable ? As OEM's don't have access to the commercial value of end customer to SI's If OEM gives self certification for the PO booked in last 5 yrs consolidated will that be acceptable		For required amount, multiple POs in favour of OEM's System Integrators are also acceptable
56	Form No. 7 OEM Undertaking on Letter Head (To be signed by the OEM) C. We Certify that, iii	86	Security breach or damages to system, if any, so caused by any embedded malicious code or otherwise, due to the act of either OEM or bidder or both, the OEM as well as the bidder would be considered liable jointly or severally and shall be banned for conducting any business with RailTel. Also the present contract, may liable to be terminated by the purchaser.	OEM / bidder can ensure the same once the system is delivered , installed and commissioned in Railtelnetwork and handed over to Railtel. Security of devices & SW post that will be responsibility of Railtel ?		As per tender.
57	5. Technical Specification:	40	Technical Specification for SOR-C1, C2, C3 and C4: RHEL for Virtual Data Centre with 3 years of standard support for Unlimited VMs- 40 Nos.	As we understand from RFP, this is a requirment for the Production environment. Please clarify , do you need 24*7*365 support for RHEL for Virtual Data Centre?		**Corrigendum**
58	5. Technical Specification:	37	SOR- A-4 - OEM Professional services: Low Level Design Document – LLD	Please confirm if any OEM Professional services required from RHEL component perspective.		As per tender.
59	5. Technical Specification:	37	SOR- A-4 - OEM Professional services: Onsite Knowledge Transfers and Support Handover-	Please confirm if any OEM training is required for RHEL (Red Hat Enterprise Linux)?		As per tender.
60	5. Technical Specification:	40	Technical Specification for SOR-C1, C2, C3 and C4: Bidder is required to supply latest versions of the following software at Data Centre (GGN-DC, SC-DC,) as per below mentioned qty.- Red Hat Enterprise Linux Server Physical or Virtual Nodes, Up to 2 Physical CPU Sockets (2 Guest VMs) with Premium Subscription and support for 3 Years, - 47	Is the quantity mentioned for each component like example RHEL Server qty mentioned is 47, includes /caters to both Data Centre (GGN-DC and SC-DC)? Or Is it for one Data Centre and same to be counted for another DC as well?		**Clarification- Quantity mentioned i.e. 47, here is total required quantity, RailTel may further disctribute the same in DC and DR.**
61	5. Technical Specification:	40	Technical Specification for SOR-C1, C2, C3 and C4: Bidder is required to supply latest versions of the following software at Data Centre **(GGN-DC, SC-DC,)** as per below mentioned qty.-	Will both the Data Center in Active-Active mode?		**Clarification- Quantity mentioned i.e. 47, here is total required quantity, RailTel may further disctribute the same in DC and DR.**

62	5. Technical Specification:	38	Technical Specification for SOR-C1, C2, C3 and C4: SOR- B-1 – DDoS for Application Layer:	We observe that RFP talks and ask about the Network ACL's, Detect Malicious IP, Patching, Policy enforcement, Compliance monitoring but it doesn't mention or define any specification for **Automation platform/tool** to do such activities. A tool/platform like Ansible possess all such functionality and widely been used in the Industry. Any thoughts on the same line?		As per tender.
63	SOR-A: A-1	6	DDOS Detection Device Collector / Traffic Routing & Analytics platform with 04 Nos. of SFP-1G per appliance for the Detection/Collector device and 3 Years of Warranty, Maintenance & Support for all supplied items as per Technical Specification given in Chapter-3A	Does Railtel require 4 Collectors? Are the Leader / Backup Leader or Controller with HA part of the 4 units requested. Or they need to be proposed separately.		As per tender.
64	SOR-A: A-4	6	OEM Professional services for installation, Implementation and deployment of supplied hardware/ software etc. as per Technical Specification given in chapter-3A	The Professional Services will be required to be onsite to do the deployment or remote support is acceptable?		**Clarification-** **Bidder to facilitate onsite resources and OEM professional services can be remote to deliver the scope as per SOR-A 4**
65	SOR-B: B-1	6	Application Layer DDoS with HA at both DC and DR (2 box at DC and 2 Box at DR) with 3 Years of Warranty as per Technical Specification given in chapter-3A	The Clause mentions 4 units whereas the quantity Column mentions 2 units. Pls calrify how many units are required.		**Clarification- In the tender DDoS Solution has been asked with HA, hence quantity is mention 2. However to provide the solution in HA, bidder has to provision total 4 units ie. 2 units at DC and 2 units at DR.**
66	XII	9	The tenderer shall make available the offered products during technical evaluation for testing and benchmarking to RailTel at any testing facility approved by RailTel. Tenderer shall provide all the required equipment and accessories for above testing at testing facility. Tenderer shall bear all the cost of above testing. RailTel shall provide only rack space and power supply. Decision of RailTel shall be final and binding in this regard.	Railtel did not explain anywhere in the RFP regarding What kind of Testing and Benchmarking is required? Pls help clarify.		As per tender.
67	Clause 4.8: S. No. i	21	RailTel has existing DDoS deployment and would continue to use the existing Licenses & Mitigation capacity in the deployment as per Annexure-1	This part of RFP mentions Railtel would continue to use existing licenses and mitigation capacities, whereas in earlier clause the ask is for 3 mitigation units. If the vendor intends to proposed a new solution which is not compatible with existing deployment, then the vendor has to propose everything from scratch ?		As per tender.
68	Clause 4.8: S. No. ii	21	The DDOS mitigation system, DDOS detection system, Traffic Analytics, Forensics System & CDN/OTT Visibility solution proposed to RailTel must be from single vendor and a common User Interface.	This clause seems to favour a specific vendor. Railtel must be open to consider other solutions in the industry providing similar functionality, even though there would be different User Interfaces for Detection, Mitigation, Analytics and MSSP Portal.		As per tender.

69	Clause 4.8: S. No. iii	21	The refresh involves following components: a. 2 Platforms with Collector role. b. 2 Platforms with User Interface role. c. 2 Platforms with Mitigation / Scrubbing role (The existing deployment will be used)	As per SOR-A: A2, The number of mitigation units required are 3 Qty. However the clause in question mentions 2 mitigation units. This arises confusion. Pls suggest whether 2 mitigation units are required or 3 ?		As per tender.
70	SOR-A2: SN 7	29	The system shall be able to directly BGP peer with multiple switches/routers in the network.	Both Detection and Mitigation systems peering with routers is not required. Detection system alone do bgp peering and provide same results.	The system shall be able to do BGP peering with multiple switches/routers in the network from either the Detection system or the mitigation system.	As per tender.
71	SOR-A2: SN 14	29	The system shall support BGP flow spec diversion mechanism for diverting traffic to scrubbing center.	BGP Flowspec diversion can be done from Detection system as well, so this function is not required on mitigation system.	The system shall support BGP flow spec diversion mechanism for diverting traffic to scrubbing center from either Detection or mitigation system.	As per tender.
72	SOR-A2: SN 20	30	Mitigation reporting must be available from common User Interface which is also a centralised configuration, management, reporting of detection and mitigation system.	There are basic mitigation reports and then detailed mitigation reports. The reports are important and how they are fetched should not be limited.	Basic mitigation reports are usually available from common User Interface, whereas detailed mitigation reports are available from the dedicate UI of mitigation portal.	As per tender.
73	SOR-A2: SN 27	30	The Proposed Solution shall use Learning Mitigation mechanism to provide correct baselines for mitigation countermeasures without dropping the traffic.	Every solution vendor has different nomenclature. Learning Mitigation is vendor specific, Behaviour Analysis is another terminology.	The Proposed Solution shall use Learning Mitigation mechanism or behaviour analysis to provide correct baselines for mitigation countermeasures without dropping the traffic.	As per tender.
74	Reporting for Mitigation System: Pt 9	31	The system shall allow mitigation parameters to be changed while mitigation is running.	Changing mitigation parameters during ongoing mitigation require dedicated interface for mitigation devices. This cannot be achieved from a single User Interface.	The system shall allow mitigation parameters to be changed while mitigation is running from either single User Interface or via dedicated management portal for mitigation units.	As per tender.
75	SOR-A3: Data Ingestion: SN 27	35	System should enrich flows with CDN and OTT provider names without relying on integration with DNS ingestor.	it is not possible to prvoide CDN OTT vsibility without dns ingestor. Manually configuring CDN Names and prefixes / ASN is not the right approach.	DNS Ingestor must be made mandatory for CDN OTT Visibility.	As per tender.
76	SOR- A-3 - Analytics & Forensics: [Reports & Queries: xxi]	36	The solution must be able to classify OTT sites and services in categories such as Streaming video, Collaboration, Private Cloud, Public Cloud, Social media, Messaging, Gaming etc.	OTT categorisation is not possible with flow based solution and that too without DNS Ingestor.	Request to delete this clause.	As per tender.
77	SOR- A-3 - Analytics & Forensics: [CDN and OTT Visibility: xiii]	36	System support future integration of DNS Ingestor for DNS data ingestion in real-time to enrich flows with CDN Data.	it is not possible to prvoide CDN OTT vsibility without dns ingestor. Manually configuring CDN Names and prefixes / ASN is not the right approach.	DNS Ingestor must be made mandatory for CDN OTT Visibility from Day1.	As per tender.
78	Scope 2.1 DDOS SOR- A-3 - Analytics & Forensics:	21	DDoS Detection & DDoS Mitigation system should be from single OEM.	As you have requested for Analytics functionality as well is that also required from same OEM	DDoS Detection , DDoS Mitigation & Analytics system should be from single OEM.	As per tender.

79	3. Long Term Maintenance Support Clause 3.1	50	Bidder shall provide maintenance support for a minimum period of 5 years after successful completion of warranty obligations. The long term maintenance support shall be comprehensive and include all hardware and software equipment supplied against this contract. RailTel should be extended the benefits of software update/up-grades made by OEM on the system from time to time to improve performance. During this period the scope of work as mentioned in clause 2 above & its sub clauses will be applicable.	The warranty support requested in this RFP is 3 yrs upfront do you mean 3 yrs + 5 yrs AMC total support commitment for 8 yrs ?	Bidder shall provide maintenance support for a minimum period of 5 years after successful completion of installation obligations. The long term maintenance support shall be comprehensive and include all hardware and software equipment supplied against this contract. RailTel should be extended the benefits of software update/up-grades made by OEM on the system from time to time to improve performance. During this period the scope of work as mentioned in clause 2 above & its sub clauses will be applicable. Total support commitment for 3yrs upfront and 2 yrs AMC	As per tender.
80	12.2. Eligibility Criteria Requirements for OEM's: Serial no 2	58	OEM should have supplied the equipment offered or equipment/software of the same series/family at least of Rs. 7.39 Cr. during last preceding 5 financial years (i.e. current year and five previous financial years) as on opening date of bid to Government/PSUs /Telecom Service Providers / Public Listed Company in India or Abroad or 35% of their offered equipment cost by respective OEM against SOR.	If OEM is submitting the letter from the customer & user having all the details is that acceptable ? As OEM's don't have access to the commercial value of end customer to SI's If OEM gives self certification for the PO booked in last 5 yrs consolidated will that be acceptable		As per tender.
81	Form No. 7 OEM Undertaking on Letter Head (To be signed by the OEM) C. We Certify that, iii	86	Security breach or damages to system, if any, so caused by any embedded malicious code or otherwise, due to the act of either OEM or bidder or both, the OEM as well as the bidder would be considered liable jointly or severally and shall be banned for conducting any business with RailTel. Also the present contract, may liable to be terminated by the purchaser.	OEM / bidder can ensure the same once the system is delivered , installed and commissioned in Railtelnetwork and handed over to Railtel. Security of devices & SW post that will be responsibility of Railtel ?		As per tender.
82	40	Technical Specification for SOR-C1, C2, C3 and C4:	RHEL for Virtual Data Centre with 3 years of standard support for Unlimited VMs- 40 Nos.	As we understand from RFP, this is a requirment for the Production environment. Please clarify , do you need 24*7*365 support?		**Corrigendum**
83	37	SOR- A-4 - OEM Professional services:	Low Level Design Document – LLD	Please confirm if any OEM Professional services required from RHEL component perspective.		As per tender.
84	37	SOR- A-4 - OEM Professional services:	Onsite Knowledge Transfers and Support Handover-	Please confirm if any OEM training is required for RHEL (Red Hat Enterprise Linux)?		As per tender.

85	40	Technical Specification for SOR-C1, C2, C3 and C4:	Bidder is required to supply latest versions of the following software at Data Centre (GGN-DC, SC-DC,) as per below mentioned qty.- Red Hat Enterprise Linux Server Physical or Virtual Nodes, Up to 2 Physical CPU Sockets (2 Guest VMs) with Premium Subscription and support for 3 Years, - 47	Is the quantity mentioned for each component like example RHEL Server qty mentioned is 47, includes /caters to both Data Centre (GGN-DC and SC-DC)? Or Is it for one Data Centre and same to be counted for another DC as well?		**Clarification- Quantity mentioned i.e. 47, here is total required quantity, RailTel may further disctribute the same in DC and DR.**
86	40	Technical Specification for SOR-C1, C2, C3 and C4:	Bidder is required to supply latest versions of the following software at Data Centre (GGN-DC, SC-DC,) as per below mentioned qty.-	Will both the Data Center in Active-Active mode?		**Clarification- Quantity mentioned i.e. 47, here is total required quantity, RailTel may further disctribute the same in DC and DR**
87	38	Technical Specification for SOR-C1, C2, C3 and C4:	SOR- B-1 – DDoS for Application Layer:	We observe that RFP talks and ask about the Network ACL's, Detect Malicious IP, Patching, Policy enforcement, Compliance monitoring but it doesn't mention or define any specification for Automation platform/tool to do such activities. A tool/platform like Ansible possess all such functionality and widely been used in the Industry. Any thoughts on the same line?		As per tender.
88	3. Broad Requirements of the solution:	20	Broad Requirements of the solution:	Request to relax the clause specific to single OEM.	There are solution like Detection, Mitigation, Traffic analysis & Reporting, Traffic Engineering has been asked in the specification and all the solution should be from same OEM. There are clauses specific to single OEM. As RADWARE being a LEADER in DDoS Soluion, We mainly focus on inline as well as out-of-path protection. Every OEM has its own method for detection and mitigation, We integrate with 3rd paty OEM for analysis & telemetry. There are many customer in INDIA including Telco using this technology. Despite being LEADER in latest Forrester/IDC report as well as MII Class-I supplier, we are not able to participate. Hence, request to relax the clause specific to single OEM and allow LEADER OEM to participate in this prestigious opportunity.	As per tender.
89	SN 1	38	DDoS mitigation solution should be a dedicated appliance (not a part of Router, UTM and IPS)	DDoS mitigation solution should be a dedicated appliance (not a part of Router, UTM, ADC and any statefull appliance) with Unlimited attack concurrent session handling	DDoS Appliance should be stateless and transparent in nature so that attacker should not be able to track. There should not be any limitation in handling attack session as it can't be predicted in number.	As per tender.
90	SN 3	38	Legitimate/clean throughput handling: 20 Gbps from day one and scalable up to 40 Gbps	Legitimate/clean throughput handling: 20 Gbps from day one and scalable up to 40 Gbps. Mitigation throughput handling: 40 Gbps from day one and scalable up to 80 Gbps. Attack Prevention Rate: 25MPPS (Data should be publically available)	Mitigation throughput should also be considered while sizing the solution. Solution should cater inbound as well as outbound mitigation. PPS should also be considered.	As per tender.
91	SN 3	38	SSL CPS (2K Key): 100,000 and (ECC p256): 75K	SSL CPS (2K Key): 90,000 and TLS1.3 Support	Request to generalize the clause for broader participation	As per tender.

92	SN 3	38	Ports: 8 x 10G SFP+ and 4 x 1G SFP from day-1 and additional 4 x 10G/1G SFP for future use, 4 TB HDD and 512 GB RAM	Ports: 8 x 10G SFP+ and 4 x 1G SFP from day-1 and additional 4 x 10G/1G SFP for future use. MNG Port: 2x1G RJ45 Console: RJ45 (Data should be publically available)	Asked clause is specific to single OEM who is not even present in any of the global report for DDOS. DDoS is a security appliance and it is always recommended to consider separate centralized management for reporting. It will ensure smooth functioning in case of large attacks. As DDoS is transparent in nature, it has only management port for device management. MNG port should always be redundant.	As per tender.
93	SN 5	38	The proposed solution should have the capability to be deployed in Inline Proxy or Bridge Mode and SPAN/TAP mode (out of path).	The proposed solution should have the capability to be deployed in Inline Transparent Mode and SPAN/TAP mode (out of path).	DDoS will be deployed as transparent in nature hence, proxy mode is not relevant	As per tender.
94	SN 6	38	The proposed solution should support dynamic routing protocols such as BGP, OSPF, RIP, etc.	Delete the clause	DDoS will be deployed as transparent in nature hence, routing protocol is not relevant	As per tender.
95	SN 8	38	The solution should support Brute Force attack mitigation and BOT mitigation using Source Verification with CAPTCHA	The solution should support Brute Force attack mitigation and BOT mitigation	Every OEM has its own method for mitigation like BOT. There should not be any limitation to handle mitigation	**Corrigendum**
96	SN 26	39	The appliance should be high performance purpose built next generation multi tenant hardware with Network function virtualization. The Appliance should support multiple network functions virtualization with dedicated hardware resources for each virtual instance. It should also run 3rd party and open source network functions on same appliance like Linux-CenOS/Ubuntu based applications.	Delete the clause	DDoS will be deployed as transparent in nature hence, virtualization is not relevant. Virtualization is relevant for statefull appliance. Installing 3rd party OS on dedicated appliance for DDoS will create a security hole which will further create concern on security compliance.	**Corrigendum**
97	SN 29	39	Support for endpoint security and VPN with 2FA including HDD ID, CPU ID, OS ID.	Delete the clause	As DDoS appliance is used to protect infra from network and application attacks, end-point security and VPN should not be added on top of it. There should be separate dedicated solution to be considered for End-Point and VPN.	**Corrigendum**
98	SN 30	39	The Proposed solution should have Endpoint Security Check and baselining of Endpoint to ensure only verified systems can access through the device. E.g.: Antivirus, Patching, etc	Delete the clause	As DDoS appliance is used to protect infra from network and application attacks, end-point security should not be added on top of it. There should be separate dedicated solution to be considered for End-Point.	**Corrigendum**
99	SN 31	39	The solution should have support for Rate Shaping at application level as well as network traffic level.	Delete the clause	Rate Shaping should be done on statefull appliance like firewall. It should not be added on top of dedicated DDoS solution.	As per tender.
100	SN 50	39	The proposed solution should have the capability to define multiple log destinations for each application	The proposed solution should have the capability to define log destinations	Logging should only be considered for broader participation	As per tender.
101	SN 51	39	Offered solution must be natively integrated at various customer deployments with Splunk, Sev1, ArcSight, Extra hop, ELK, Grafana and others	Offered solution must support integration with SIEM	Solution should have functionality to integrate with SIEM for broader participation	**Corrigendum**