Consolidated Queries for “Appointment of an Agency for supply, installation, configuration, operations and maintenance of ICT infrastructure at RailTel Data Centre(s)”

E-Tender No. RailTel/Tender/OT/CO/DNM/2017-18/ DC Procurement/383

Sr. No.	Section No.	Clause No.	Reference/Subject	Clarification Sought/Suggestion	RailTel Remarks
1	II	26.5 Eligibility Criteria 3(b)	Eligibility Criteria for Turnover : Existing Clause says "The bidder’s cumulative annual turnover from sale of Security systems, Storage Systems, Tape Library, Networking systems and integration Services etc. should be more than (INR)100 crores in each of the last three financial years viz; 2014-15, 2015-16 and 2016-17"	As per our understanding the turnover required for eligibility is 100 Cr cumulative for last 3 financial years. Kindly advise if this is correct. If yes, please delete 'each of' from the existing clause and amend the clause as: The bidder’s cumulative annual turnover from sale of Security systems, Storage Systems, Tape Library, Networking systems and integration Services etc. should be more than (INR)100 crores in the last three financial years viz; 2014-15, 2015-16 and 2016-17	may kindly refer corrigendum-II
2	II	26.5 Eligibility Criteria 5(b)	The bidder’s organization must on its roll have at least three (3) ITIL/ISO 20000 Lead Auditor (LA) or Lead Implementer (LI) resources and three (3) BS7799 / ISO 27001 lead Auditor / Lead Implementer certified resources as 31st March 2017.	We do not see any requirement of so many ITIL/ISO/BS7799 Lead Implementors and Lead Auditors. Only one certified resource on ISO9001, ISO20000 or ISO9001 is enough, or even if the bidder is ISO certified, it is sufficient. Kindly amend the clause as: The bidder’s organization must be ISO certified or on its roll have at least one (1) ITIL /ISO20000/BS7799/ISO270001 Lead Auditor (LA) or Lead Implementer (LI) resource.	may kindly refer corrigendum-II
3	II	32.1 Bank Guarantee for Contract Performance	Existing Clause says "Within 15 days after the receipt of notification of award of the Contract from the Purchaser, the successful Tenderer shall furnish Contract Performance Guarantee to the Purchaser, which shall be equal to 20% of the value of the Contract and shall be in the form of a Bank Guarantee Bond from a Nationalized Bank in the Proforma given at Section VI – Additional Requirements/ Pro forma.	As per standard followed by the Govt. of India, the Performance Bank Guarantee asked in most Govt. tenders is 10% of the contract value. 20% of the value of this contract will be very high. You are requested to amend this Performance Bank Guarantee required to 10% of the contract value and amend the clause as: Within 15 days after the receipt of notification of award of the Contract from the Purchaser, the successful Tenderer shall furnish Contract Performance Guarantee to the Purchaser, which shall be equal to 10% of the value of the Contract and shall be in the form of a Bank Guarantee Bond from a Nationalized Bank in the Proforma given at Section VI – Additional Requirements/ Pro forma.	may kindly refer the corrigendum- II
4	3		(a) The bidder should have positive net worth as on 31st March 2017 and should be profitable for each of the last three years viz; 2014-15, 2015-16 and 2016-17. (b) The bidder’s cumulative annual turnover from sale of Security systems, Storage Systems, Tape Library, Networking systems and integration Services etc. should be more than (INR)100 crores in each of the last three financial years viz; 2014-15, 2015-16 and 2016-17 Note: The turnover refers to the bidder and not the composite turnover of its subsidiaries/sister concerns etc.	1. Audited Financial Reports for 2016-17 will be available only after August/September 2017. Request you to consider 2013-14, 2014-15 and 2016-17 as last 3 Fys	may kindly refer corrigendum-II

5	5		(a) As on 31st March,2017 The bidder must have on its roll at least 50 technically qualified professionals in the ICT domains like security, networking, system software, systems integration, storage who have prior experience in providing the Data Center Infrastructure maintenance services. (b) The bidder's organization must on its roll have at least three (3) ITIL/ISO 20000 Lead Auditor (LA) or Lead Implementer (LI) resources and three (3) BS7799 / ISO 27001 lead Auditor /Lead Implementer certified resources as 31st March 2017. (c) The service operations manager deployed for the project," Appointment of an agency for Supply, Installation, Configuration, Maintenance and Operations of ICT Infrastructure for the establishment of a Data Centre at Delhi" must have an IT experience of 10-15 years with minimum 5 years of relevant experience in Data Center and should have a Post Graduate Degree in Computer Science/graduate degree in computer/IT engineering and should be PMP certified. The designated service operations manager should also be on rolls of the organization for a minimum of 2 years.	5a) HR Declaration OK, but compiling 50 CVs can be tedious and perhaps, not necessary at PQ stage. Request you to delete this requirement. We can submit the HR declaration with resource names, qualifications etc. CVs can be submitted later on award of contracts at the time of actual deployment. (We can however submit 8-10 sample CVs for key rolls if RAILTEL insists on CVs in PQ)	may kindly refer corrigendum-II
6	10		The bidder must have ISO 9001:2000 certification for system integration or sale, design and development, testing and implementation of Data Center products and solutions	Request you to change to: "The bidder must have ISO 9001:2008 certification for sales and support of ICT solutions & services"	may kindly refer corrigendum-II
7	11		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, ServicesLicense of Government of India for Telecom Operation.	ICT Projects need a lot of technical expertise and know-how and SIFY has the required experience in successfully delivering similar projects in key Government/PSUs. We request you to delete this clause. This will also facilitate additional competitive and responsive bidder in your current and future RFPs.	No change to the tender condition
8	16.1		Delivery of goods at the proposed Data Centre/Regional Office Site. 8 calendar weeks from the date of release of Work order	Request you to increase the delivery timelines by 4 weeks and change the clause from 8 calender weeks to 12 calender weeks	No change to the tender condition
9	D(Security infrastructure)		Antivirus (Client Server) on all servers and computing infra (Desktop - 1200 users Server -50)	Please provide list of locations along with number of antivirus to be installed in each location	The list will be provided at the point of issue of PO
10	32		Failure of the successful Tenderer to comply with the requirement of Clause 31 or Clause Error! Reference source not found. shall constitute sufficient grounds for the annulment of the award and forfeiture of the EMD. In case of exigency, if the Purchaser gets the work done from elsewhere, the difference in the cost of getting the work done will be borne by the successful Tenderer.	Please elaborate on "or Clause Error! Reference source not found"	may kindly refer corrigendum-II
11	32		Within 15 days after the receipt of notification of award of the Contract from the Purchaser, the successful Tenderer shall furnish Contract Performance Guarantee to the Purchaser, which shall be equal to 20% of the value of the Contract and shall be in the form of a Bank Guarantee Bond from a Nationalized Bank in the Proforma given at Section VI – Additional Requirements/ Proforma.	20% bank guarantee is too high. Most of the tenders that we see in Government/PSUs ask for 10% bank guarantee. Request you to reduce the same to 10%	may kindly refer corrigendum-II
12	36		Payment Terms	While Payment terms for Hardware are ok, request you to please change payment terms of software as 75% on Delivery, 15% against installation, 5% against PAC, 5% against FAC	may kindly refer corrigendum-II

13	36.5		Payment of service items shall be made in Indian Currency (Rs.) only. 30% payment of item towards “Installation, Testing & Commissioning" shall be made by Corporate Office on successful Installation, testing & commissioning, 60% on issue of PAC and final 10% on issue of Final Acceptance Certificate	Request to change the payment terms to "Payment of service items shall be made in Indian Currency (Rs.) only. 70% payment of item towards “Installation, Testing & Commissioning" shall be made by Corporate Office on successful Installation, testing & commissioning, 20% on issue of PAC and final 10% on issue of Final Acceptance Certificate"	may kindly refer corrigendum-II
14	36.5		Payment for Long Term Maintenance / Annual Maintenance Contract (AMC): Payment would be made bi-annually by RailTel after satisfactory completion of AMC Services of that period and on certificate furnished by concerned RailTel’s representative.	Request to change this to " Payment would be made Quarterly by RailTel after satisfactory completion of AMC Services of that period and on certificate furnished by concerned RailTel’s representative."	may kindly refer corrigendum-II
15	13.9		High level Steering Committee involving representatives of the Purchaser and senior officials of the Agency (including the Managing Director, Country Head and Operational Head) shall be formed for the purpose of this contract. This committee shall meet at intervals, as decided by the Purchaser later, to oversee the progress of the project.	Request to change to "High level Steering Committee involving representatives of the Purchaser and senior officials of the Agency (including the Managing Director or CEO or COO or Regional Operations Head or Country Head or Operational Head, can be any two) shall be formed for the purpose of this contract. This committee shall meet at intervals, as decided by the Purchaser later, to oversee the progress of the project."	No change to the tender condition
16	16.3		If the agency fails to execute and complete the work within the stipulated time the agency shall accept reduction in the total amount payable to him by the purchaser at the rate of 0.5% per week or part thereof (rounded off to the nearest whole number) of the total value of the contract for the actual delay occasioned beyond the appointed time by which the work shall have been completed under the contract.	Request to change to "If the agency fails to execute and complete the work within the stipulated time the agency shall accept reduction in the total amount payable to him by the purchaser at the rate of 0.5% per week or part thereof (rounded off to the nearest whole number) of the undelivered component for the actual delay occasioned beyond the appointed time by which the work shall have been completed under the contract."	may kindly refer corrigendum-II
17	31		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.	Request you to change to "Taxes as applicable" as there is a likelihood of GST getting activated soon.	may kindly refer the tender document
18	II	18.1	Consortium	In order to bring synergy of various organizations for a better delivery /implementation of the project, we request you to kindly allow consortium	No change to the tender condition

19	II	26.5.3 eligibility criteria no.4	During the last three financial years, viz; 2014-15, 2015-16 and 2016-17 the bidder must have implemented at least one data center project(s) in government/PSU for India, which include activities like Supply, Installation, Configuration, Maintenance and Operations of the ICT Infrastructure like Security Equipment, Storage and Backup Equipment, for the Data Centre, where the value of each project should be more than (INR) Three crores and Eighty five lakhs (Rs 3.85 crores). Out of the above project(s), at least one of the projects should meet the following parameters: Data Centre of Tier II / III Should have deployed security systems like firewall, End point protection, storage and backup systems, EMS, etc. Note: Bidder's in house data centers shall not be considered. Bidders who have built their own Data Centre (IDC), for commercial use will be considered	Data centers also have a sizable network and server infrastructure as a part of it and not just limited to security tools and storage / backup. Hence we request that the clause may be amended as :- "During the last three financial years, viz; 2014-15, 2015-16 and 2016-17 the bidder must haveimplemented at least one data center project(s) in government/PSU for India, which include activities like Supply, Installation, Configuration, Maintenance and Operations of the ICT Infrastructure like DC Build, Network, Server, Security Equipment, Storage and Backup Equipment, for the Data Centre, where the value of each project should be more than (INR) Three crores and Eighty five lakhs (Rs 3.85 crores). Out of the above project(s), at least one of the projects should meet the following parameters: Data Centre of Tier II / III Should have deployed security systems like firewall, End point protection, storage and backup systems, EMS, etc. Note: Bidder's in house data centers shall not be considered. Bidders who have built their own Data Centre (IDC), for commercial use will be considered"	may kindly refer the corrigendum-II
20	II	26.5.3 eligibility criteria no.5	a) As on 31st March,2017 The bidder must have on its roll at least 50 technically qualified professionals in the ICT domains like security, networking, system software, systems integration, storage who have prior experience in providing the Data Center Infrastructure maintenance services. (b) The bidder's organization must on its roll have at least three (3) ITIL/ISO 20000 Lead Auditor (LA) or Lead Implementer (LI) resources and three (3) BS7799 / ISO 27001 lead Auditor / Lead Implementer certified resources as 31st March 2017. (c) The service operations manager deployed for the project," Appointment of an agency for Supply, Installation, Configuration, Maintenance and Operations of ICT Infrastructure for the establishment of a Data Centre at Delhi" must have an IT experience of 10-15 years with minimum 5 years of relevant experience in Data Center and should have a Post Graduate Degree in Computer Science/graduate degree in computer/IT engineering and should be PMP certified. The designated service operations manager should also be on rolls of the organization for a minimum of 2 years.	The emphasis of the clause is on quality process and compliance. Organizations have different approach to meet the same. Hence the certification of the organization should be asked of instead of auditors on the rolls. The current clause is restrictive in nature and the same kindly be amended as :- "The bidder should be certified for ISO 20000 and 27000 and the bidder will commit to provide the necessary resource alongwith necessary qualifications." However the condition for employment for last 2 years should be relaxed .	may kindly refer the corrigendum - II
21	II	26.5.3 eligibility criteria no. 10	The bidder must have ISO 9001:2000 certification for system integration or sale, design and development, testing and implementation of Data Center products and solutions	In addition to the ISO 9001, the bidder should have ISO 20000 and ISO 27001, to ensure that proper implementation of the project is done	may kindly refer the corrigendum-II

22		3B, PAGE NO. 26	The bidder’s cumulative annual turnover from sale of Security systems,Storage Systems, Tape Library, Networking systems and integration Services etc. should be more than Services etc. should be more than Services etc. should be more than (INR)100 crores in each of the last three financial years viz; 2014-15, 2015-16 and 2016-17. NOTE- The turnover refers to the bidder and not the composite turnover of its subsidiaries/sister concerns etc.	The bidder’s cumulative annual turnover should be more than (INR)100 crores of the last three financial years viz; 2014-15, 2015-16 and 2016-17	may kindly refer the corrigendum-II
23		4, PAGE NO. 27	During the last three financial years, viz; 2014-15, 2015-16 and 2016-17 the bidder must have implemented at least one datacenter project(s) in government/PSU for India, which include activities like Supply,Installation, Configuration, Maintenance and Operations of the ICT Infrastructure like Security Equipment, Storage and Backup Equipment, for the Data Centre, where the value of each project should be more than (INR) Three crores and Eighty five lakhs (Rs3.85 crores). Note- Out of the above project(s), at least one of the projects should meet the following parameters: Data Centre of Tier II / III Should have deployed security systems like firewall, End point protection, storage and backup systems, EMS, etc.	The bidder must have implemented at least one datacenter project(s) in government/PSU for India, which include activities like Supply,Installation, Configuration, Maintenance and Operations of the ICT Infrastructure like Security Equipment, Storage and Backup Equipment, for the Data Centre, where the value of project should be more than (INR) Three crores and Eighty five lakhs Rs3.40 crores	may kindly refer the corrigendum-II
24		ANNEXURE 4.5, PAGE 82	For the position of 'Project-in-charge', it is mandatory to provide name of proposed resource along with details desired as per format given below. It is mandatory that the resource proposed for this position should not change till the commissioning and acceptance of the complete solution. Note : The resources will be deployed at RailTel Data Centre at Gurugram and remotely manage/operate on the devices at Secunderabad Data Centre.	Should be , provided resource name as on date of award of tender.	may kindly refer the corrigendum-II
25		5. A, PAGE NO. 28	As on 31st March,2017 The bidder must have on its roll at least 50 technically qualified professionals inthe ICT domains like security, networking, system software, systems integration, storage who have prior experience in providing the Data Center Infrastructure maintenance	As on 31st March,2017 The bidder must have on its roll at least 30 technically qualified professionals inthe ICT domains like security, networking, system software, systems integration, storage who have prior experience in providing the Data Center Infrastructure maintenance	may kindly refer the corrigendum-II
26		5.B, PAGE NO. 28	The bidder’s organization must on its roll have at least three (3) ITIL/ISO 20000 Lead Auditor (LA) or Lead Implementer (LI) resources and three (3) BS7799 / ISO 27001 lead Auditor /Lead Implementer certified resources as 31st March 2017.	The bidder’s organization must on its roll have at least three (3) ITIL/ISO 20000 Lead Auditor (LA) or Lead Implementer (LI) resources and three (3) BS7799 / ISO 27001 lead Auditor /Lead Implementer certified resources as on date of award of tender.	may kindly refer the corrigendum-II
27		5.C, PAGE NO. 28	The service operations manager deployed for the project,”Appointment of an agency for Supply,Installation, Configuration, Maintenance and Operations of ICT Infrastructure for the establishment of a Data Centre at Delhi” must have an IT experience of 10-15 years with minimum 5 years of relevant experience in Data Center and should have a Post Graduate Degree in Computer Science/graduate degree in computer/IT engineering and should be PMP certified. The designated service operations manager should also be on rolls of the organization for a minimum of 2 years.	kindly mention "the designated service operations manager should also be on rolls of the organization as on date of award of tender.	may kindly refer the corrigendum-II

28		26.6.3. (5), PAGE NO. 31	5. During the last three financial years, viz; 2014-2015,2015-2016,2016-17 the bidder must have implemented at least one projects in government/PSU for India organizations like the ISP - Internet Service Provider/ TSP- Telecom Service Provider etc, which include activities like Supply, Installation, Configuration, Maintenance and Operations of the ICT Infrastructure like Security equipment and Networking equipment, where the value of each project should be more than (INR) Three crores and eighty five lakhs (Rs 3.85 crores) Out of the above one projects one of the projects should meet the following parameters: ISP providing services in multiple states/regions Should have deployed enterprise class core routers/switches, security systems like Secure DNS, SSl off loader etc.	It should not be limited to IPS & TSP but should also include all Govt & Psu's, so that there will be a level playing field and railtel will get more seriuos vendor partcipation.	may kindly refer the corrigendum-II
29		26.6.4, PAGE NO. 33	Technical Bids receiving a score greater than or equal to a cut-off score of 75% will be eligible for consideration in the subsequent rounds.	Technical Bids receiving a score greater than or equal to a cut-off score of 60% will be eligible for consideration in the subsequent rounds.	No change to the tender condition
30		36, PAGE NO. 38	Payment - 75% payment of the value of the hardware items and 20% payment of the value of the software items against LOA/Sub PO/PO would be made on receipt of material by the consignee (at site /the stores, to be decided by RailTel) 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:	Payment - 75% payment of the value of the hardware items and 75% payment of the value of the software items against LOA/Sub PO/PO. would be made on receipt of material by the consignee (at site /the stores, to be decided by RailTel) 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:	may kindly refer the corrigendum-II
31		36.1, PAGE NO. 39	15% payment of the value of hardware items and 20% of the value of software items of the PO shall be made by RailTel on Installation at site, 5% payment of value of hardware items and 50% of the value of software items of the PO on issue of Provisional Acceptance Certificate (PAC), 5% payment of the value of hardware items and 10% of the value of software items of the PO shall be made by RailTel on issue of Final Acceptance Certificate (FAC) which will be issued by GGM/DNM. (15% + 5 %) payment of value of hardware items of the Sub PO/PO which could not be installed for want of site readiness or as per the decision of RailTel, will be made on issue of PAC and remaining 5% on issue of FAC.	10% payment of the value of hardware items and 15% of the value of software items of the PO shall be made by RailTel on Installation at site. 10 % payment of value of hardware items and 5% of the value of software items of the PO on issue of Provisional Acceptance Certificate (PAC).5% payment of the value of hardware items and 5% of the value of software items of the PO shall be made by RailTel on issue of Final Acceptance Certificate (FAC) which will be issued by GGM/DNM.	may kindly refer the corrigendum-II
32		36.5.1, PAGE NO. 39	Payment of service items shall be made in Indian Currency (Rs.) only. 30% payment of item towards “Installation, Testing & Commissioning" shall be made by Corporate Office on successful Installation, testing & commissioning, 60% on issue of PAC and final 10% on issue of Final Acceptance Certificate.	need clarity.	may kindly refer the corrigendum-II
33		36.5.2, PAGE NO. 39	Payment for Long Term Maintenance / Annual Maintenance Contract (AMC): Payment would be made bi-annually by RailTel after satisfactory completion of AMC Services of that period and on certificate furnished by concerned RailTel’s representative.	The payment should be made quarterly basis.	No change to the tender condition
34		36.5.3 , PAGE NO. 39	Payment towards operations & maintenance would be paid bi-annually by the concerned invoicing subject to adherence to the SLAs mentioned in this tender document subject to any deductions or recovery (which the RailTel may be entitled to make under contract) through RTGS.	The payment should be made quarterly basis.	may kindly refer the corrigendum-II
35		Backup , page No. 126	Backup	Data retention period	may kindly refer the tender documents

36		Backup , page No. 126	Tape Library	How many drives should be in the tape library?	may kindly refer the tender documents
37		page No. 155	The proposed system should be able to auto-calculate resource utilization baselines for the entire managed systems and networks and allow user to set corresponding upper and lower threshold limits.	Criteria is not defined by Railtel for FAT	may kindly refer the tender documents
38		page no. 80	Application Black Box Testing	Not Cleared-what is the reports parameter	may kindly refer the tender documents
39		Page No. 167	Successful completion of Factory Acceptance Tests and submission of necessary reports and certificates to RAILTEL	Criteria is not defined by Railtel for FAT	may kindly refer the tender documents
40	1494136743_annexure-1---technical-specifications1[3].pdf	7	Comprehensive onsite warranty for 3 years with Next business Day (NBD) resolution.	This is software component and OEM can't provide NBD resolution, this is generally for hardware component, kinldy remove this point from AV component.	may kindly refer the corrigendum-II
41	UTM Solution Annex 1	7	UTM appliance should have a on device storage of min 100GB to be able to hold multiple OS images, logs, backups etc	May please be changed to "UTM appliance should have a on device storage of min 500GB to be able to hold multiple OS images, logs, backups etc	No change to the tender condition
42	UTM Solution Annex 1	73	The solution must be present as Leaders in Gartner's Magic Quadrant for 2016/2017 and have atleast 90% in the NSS NGFW security effectiveness value.	May please be changed to " The solution must be present as Leaders in Gartner's Magic Quadrant for enterprise network firewalls for 2016/2017 and have atleast 90% in the NSS NGFW security effectiveness value."	No change to the tender condition
43	UTM Solution Annex 1	9	Firewall should support 5 Million concurrent sessions	May please be changed to "Firewall should support 12 Million concurrent sessions"	No change to the tender condition
44	UTM Solution Annex 1	15	Support at least 10 firewall domains/instants/context	May please be changed to "Support at least 20 firewall domains/ instants/ context"	No change to the tender condition
45	NGFW Annex 1	7	The solution appliance should have a on device storage of min 200GB to be able to hold multiple OS images, logs, backups etc	May please be changed to "The solution appliance should have a on device storage of min 500GB to be able to hold multiple OS images, logs, backups etc"	No change to the tender condition
46	NGFW Annex 1		Additional Point	The solution appliance must have support for addition of 40G SFP interfaces in future	No change to the tender condition
47	NGFW Annex 1	52	The management solution must offer console capability for managing the logs, policy, reporting and various features of the The solution.	May be changed to "The management solution must offer a separate centralized management system capable of managing the 10,000 indexed/analytical logs/sec, policy, reporting and various features of the The solution."	No change to the tender condition
48	Anti APT	10	The proposed solution should have the ability to analyze, detect and block malware in common file formats including but not limited to executables, JAVA, PDF, MS Office documents (doc, docx, xls etc), common multimedia contents like JPEG, GIF and ZIP/RAR/7ZIP/TNEF archives, to prevent advanced Malware and Zero-day attacks.	The proposed solution should have the ability to analyze, detect and block malware in common file formats including but not limited to executables, JAVA, PDF, MS Office documents (doc, docx, xls etc), common multimedia contents like JPEG, GIF, pif, com, scr, csv,iso, cpl, wsh and ZIP/RAR/7ZIP archives, to prevent advanced Malware and Zero-day attacks.	No change to the tender condition
49	Anti APT	2	The solution must employ an on premise (not on cloud) analysis engine using virtual execution to detect zero day and unknown threats and must not be signature based.'	May be changed to " The solution must employ an on premise (not on cloud) analysis engine using virtual execution(OS Emulation) and CPU flow detection (CPU Emulation) to detect ROP, zero day and unknown threats and must not be signature based."	No change to the tender condition
50	Anti APT	17	The proposed solution should have the ability to scan and analyze emails to identify malicious attachments or URLs.	May be changed to "The proposed solution should have the ability to scan,analyze, clean and remediate emails of malicious attachments or URLs. The solution should be able to convert the attachment to clean PDFs"	No change to the tender condition

51	UTM,NGFW, IPS, APT, IPS		Additional Point	No backdoor/malicious code should have been identified in the OEM solution for all security products like UTM, NGFW, IPS, APT, WAF etc in the past 3 years. The OEM should present a written and signed undertaking from the head of engineering/legal divison in this regard.	No change to the tender condition
52	UTM,NGFW, IPS, APT , IPS		Additional Point	In case multiple security products like UTM, NGFW, IPS, APT are from the same OEM a single centraized management solution must be provided	No change to the tender condition
53	Backup	Add-ON	Request RAILTEL to add Gartner	Proposed backup solution must be in Gartner's leader quadrant consequently from last three years.	No change to the tender condition
54	Backup	Add-ON	Is Ransomware alert is required in Backup fot clients	The proposed backup solution must have native inbuilt alert capability for Ransomware affected clients	No change to the tender condition
55	Backup	Add-ON	Is backed up storage disk need to be protected from Ransomware	Proposed backup solution must have inbuilt capability to protect the backed up disk volume from Ransomware.	No change to the tender condition
56	Backup	Add-ON	RFP has asked for two solutions i.e. Security and Backup. We understand both solutions are independent of each other with respective OEM's. iHence it is our submission that separate price should be taken for both the solution; for final individual evaluation.		No change to the tender condition
57	II	12.3	The EMD shall be denominated in Indian Rupees, and shall be in the form of a Demand Draft	Can we furnish EMD in form of bank Guarantee.	No change to the tender condition
58	II	26.5	During the last three financial years, viz; 2014-15, 2015-16 and 2016-17 the bidder must have implemented at least one data center project(s) in government/PSU for India, which include activities like Supply, Installation, Configuration, Maintenance and Operations of the ICT Infrastructure like Security Equipment, Storage and Backup Equipment, for the Data Centre, where the value of each project should be more than (INR) Three crores and Eighty five lakhs (Rs 3.85 crores). Out of the above project(s), at least one of the projects should meet the following parameters: - Data Centre of Tier II / III - Should have deployed security systems like firewall, End point protection, storage and backup systems, EMS, etc. Note: - Bidder’s in house data centers shall not be considered. - Bidders who have built their own Data Centre (IDC), for commercial use will be considered	During the last three financial years, viz; 2014-15, 2015-16 and 2016-17 the bidder must have implemented at least one data center project(s) in government/PSU/ Government bank for India, which include activities like Supply, Installation, Configuration, Maintenance and Operations of the ICT Infrastructure like Security Equipment/ Storage / Backup Equipment for the Data Centre, where the value of each project should be more than (INR) Three crores and Eighty five lakhs (Rs 3.85 crores). Out of the above project(s), at least one of the projects should meet the following parameters: - Data Centre of Tier II / III - Should have deployed security systems like firewall/ End point protection/ storage / backup systems/ EMS etc. Note: - Bidder’s in house data centers shall not be considered. - Bidders who have built their own Data Centre (IDC), for commercial use will be considered	may kindly refer the corrigendum-II
59	II	26.6.3 (1)	Bidder’s experience in India for govt/psu, quantified in terms of number of years will be evaluated. *Experience would mean where the bidder has implemented activities like Supply, Installation, Configuration, Maintenance and Operations of the ICT Infrastructure like Security, Network equipment, Storage and Backup equipment, Servers, for the Data Centre*	It is requested to please condsider bidder’s experience in India for govt/psu quantified in terms of number of years will be evaluated. *Experience would mean where the bidder has implemented activities like Supply, Installation, Configuration, Maintenance and Operations of the ICT Infrastructure like Security/ Network equipment/ Storage / Backup equipment/ Servers, for the Data Centre*	may kindly refer the corrigendum-II
60	II	26.6.3 (2)	Projects where the bidder has implemented activities like Supply, Installation, Configuration, Maintenance and Operations of the ICT Infrastructure like Security equipment, Storage and Backup equipment for the Data Centre in Govt/PSU with an order value more than Rs 3.85 Crores each shall be considered.	IT is requested to please consider projects where bidder has implemented activities like Supply, Installation, Configuration, Maintenance and Operations of the ICT Infrastructure like Security equipment or storage/ backup equipment for Data centre in Govt/ PSU/ Govt Banks with an order value of more than 3.85 crores	may kindly refer the corrigendum-II

61	II	26.6.3 (3)	Cumulative Turnover of the company from the sale of equipment's like Security systems, Storage Systems, Tape Library, Servers, Networking, software and SAN Integration services for each of the last three financial year ending 31st March 2017	What would be the suporting doxument which would be required to be furnished by the bidders.	may kindly refer the tender documents
62	II	26.6.3 (5)	During the last three financial years, viz; 2014-2015,2015-2016,2016-17 the bidder must have implemented at least one projects in government/PSU for India organizations like the ISP - Internet Service Provider/ TSP- Telecom Service Provider etc, which include activities like Supply, Installation, Configuration, Maintenance and Operations of the ICT Infrastructure like Security equipment and Networking equipment, where the value of each project should be more than (INR) Three crores and eighty five lakhs (Rs 3.85 crores) Out of the above one projects one of the projects should meet the following parameters: -ISP providing services in multiple states/regions - Should have deployed enterprise class core routers/switches,	It is requested to consider experience of of atleast one project of value greater than 3.85 crs for implementation of enterprise routers/ switches for government agencies other than ISPs as well in last 7 years starting from 2011.	may kindly refer the corrigendum-II
63	II	32.1	Within 15 days after the receipt of notification of award of the Contract from the Purchaser, the successful Tenderer shall furnish Contract Performance Guarantee to the Purchaser, which shall be equal to 20% of the value of the Contract and shall be in the form of a Bank Guarantee Bond from a Nationalized Bank	Request to please consider Contract performance Guarantee equal to 10% as this is as per industry standards prevailant.	may kindly refer corrigendum-II
64	II	36	payment terms	Request to please consider software payment terms in proportion to hardware payment terms as software would be loaded on hardware only and terms should be subsequent.	may kindly refer the corrigendum-II
65	III	4.1	The warranty would be valid for a period 36 months from the date of Provisional Acceptance Certificate (PAC).	It is submitted to have warranty started from date of suply of equipments from site for 36 months. As warranty certificate is mandatory document as part of list of documents for claimining supply related payment as well.	No change to the tender condition
66	III	4	The warranty would be valid for a period 36 months from the date of Provisional Acceptance Certificate (PAC).	It is rquested that as no warranty is provided by OEM on software items so warranty certificate requirement for claiming software related payment to be waived off.	No change to the tender condition
67	III	9.1	Within 15 days after the receipt of notification of award of the Contract from the Purchaser, the successful Tenderer shall furnish Contract Performance Guarantee to the Purchaser, which shall be equal to 20% of the value of the Contract and shall be in the form of a Bank Guarantee Bond from a Nationalized Bank	Request to please consider Contract performance Guarantee equal to 10% as this is as per industry standards prevailant.	may kindly refer corrigendum-II
68	Add on	Add on	Is RAILTEL has concerned for Gartner leaders backup & recovery solution for their datacentre requirement? This will help RAILTEL to get best product for their dynamic environment & requirement	Proposed backup solution must be in Gartner's leader quadrant atleast from last three years.	No change to the tender condition
69	Add on	Add on	Is Ransomware alert is required in Backup for clients. Ransomware best practice suggest to keep good backup for recovery. Timely alert can help organisation in reducing the risk in many fashions	The proposed solution must have inbuilt Ransomware alert capability for clients.	No change to the tender condition
70	Add on	Add on	Is Windows backed up disk volume need to be protected from Ransomware. Disk protection can help in securing backed up disk/volume from ransomware attack.	Proposed backup solution must have inbuilt capability to protect the backed up disk volume from Ransomware.	No change to the tender condition

71	Add on	Add on	RFP has for two solution - Backup & Security. As both the solutions are independent of each other with respective OEM's, it is suggested as separate price schedule is taken to evalaute for finalisation independent of each other. This will help the Railtel to get the best solution for both the requirements.	This will help the Railtel to get the best solution for both the requirements.	No change to the tender condition
72	8. UTM Solution	Add on	UTM appliance should have at least 04 x 10/100/1000 GE RJ45 ports and 2 x 1GE SFP+ ports with fully populated (SFP+ transceivers) from day one	Request to please clarify whether 2 x 1GE SFP ports are required or 2 x10G SFP+ ports required	may kindly refer the corrigendum-II
73	8. UTM Solution	Add on	The management solution must offer console capability for managing the logs, policy, reporting and various features of the UTM.	It is suggested that the Reporting solution should have minimum 12 GB of storage capacity to take logs from all UTMs at central location for a longer duration for foriensics	No change to the tender condition
74	8. UTM Solution	Add on	The management solution must offer console capability for managing the logs, policy, reporting and various features of the UTM.	It is suggested that Per day log retrieve capacity must be 40 GB / day with at least 12 TB of storage	No change to the tender condition
75	9. Next-Gen Firewall (NGFW)	Add on	IPS throughput should be atleast 3 Gbps or better for real world/production throughput	Considering Firewall throughput of 20 Gbps, 3 Gbps IPS throughput is very less. It is suggested that the IPS throughput should be 6 Gbps or more for real world / production traffic	No change to the tender condition
76	9. Next-Gen Firewall (NGFW)	Add on	Logging and Reporting up to layer 7 traffic details (firewall policy level, denied traffic details etc.)	It is suggested that the Reporting solution should have minimum 12 GB of storage capacity to take logs from all NGFWs at central location for a longer duration for foriensics	No change to the tender condition
77	2. Web Application Firewall	Add on	g) File upload violations.	It is suggested to include scanning for malicious content in Uploads along with File upload violations. Most of Web applications are encrypted and the Firewall / IPS in the network cannot inspect the traffic which is SSL. In order to check and drop any malicious content which is being uploaded to web server it will save the web server from being infected	No change to the tender condition
78	Tape Library		The Tenderer should provision tape library as a backup device for the purpose of data backup & restoration.	Requesting you to pls add the Drive & Tape Slot Count as "It shall have min. 6 Nos. LTO-7 Drives and 400 Tape Slot License with LTO-7 Media with Barcode"	may kindly refer the corrigendum-II
79	Tape Library		The tape library should include a bar-code reader to enable managing the inventory of tape cartridges.	Kindly Include the Scalability criteria of the Tape Library in Terms of Tape Drives Slot minimum to double capacity in PB as 24 Drives & 800 Tape Slots.	may kindly refer the corrigendum-II
80	Tape Library		The tape library should have mixed media support and should be proposed along with necessary software/licenses	Kindly Change it to- The tape library should have mixed media support and should be proposed along with necessary software/licenses, If applicable.	may kindly refer the corrigendum-II
81	Tape Library		The Tenderer should provision adequate number of native full-duplex Fibre Channel ports on the tape library so as to stream data for full-utilization of all the tape drives and also ensuring the backup requirement indicated above.	Kindly modify the Tape Drive as a FULL Height Drives, as Full Height drives are more robust and durable in performance Delivery. Cost of the Half-Height drives & Full Height drives are same for users.	No change to the tender condition
82	Tape Library		Proposed Tape library should be supplied along with required rack mounting kit which should fit into 42U rack or should be 45U library frame size. Supply should include all the required cables/PDUs/equipment's necessary for making the system operational.	PDUs and other Rack equipments shall be covered bu the Bidders, as the Tape library will come with their own power supply and cables , NOT with PDU & other rack cables.	may kindly refer the corrigendum-II
83	Tape Library		Tenderer should provision native web-based remote management tool for remote administration.	Shall also provide Advance level of Reporting to have all the reports on Media & Jobs	No change to the tender condition
84	Tape Library		Offered Tape drive should be native FC/ SAS LTO-7.	Shall be 8 Gbps FC interface. SAS interface comes in standalone drives only.	No change to the tender condition
85	Tape Library		Tape drives with Encryption capability	Shall proposed with Encryption enabled Drives and Encryption manager to manage the encrytion keys in Redundant fashion in the form of additional Hardware.	may kindly refer the corrigendum-II

86	26.6. Evaluation of Technical Bids		Backup Solution - Tape Library scalability (1 mark): The proposed Tape library will be evaluated with respect to the max no.of drive supported in a single library and partitioning. The bidder with maximum drives in a single library will beconsidered for maximum marks and the rest will be given marks on pro rata.	Evaluation Criteria shall be based on the Total PetaByte of Capacity handling / Total Tape Slots, along with the No. of Full Height Drives in the Offered Single/ same Library.	may kindly refer the corrigendum-II
87	27	26.5. Evaluation of Eligibility Criteria	During the last three financial years, viz; 2014-15, 2015-16 and 2016-17 the bidder must have implemented at least one data center project(s) in government/PSU for India, which include activities like Supply, Installation, Configuration, Maintenance and Operations of the ICT Infrastructure like Security Equipment, Storage and Backup Equipment, for the Data Centre, where the value of each project should be more than (INR) Three crores and Eighty five lakhs (Rs 3.85 crores). Out of the above project(s), at least one of the projects should meet the following parameters: • Data Centre of Tier II / III • Should have deployed security systems like firewall, End point protection, storage and backup systems, EMS, etc. Note: Bidder’s in house data centers shall not be considered. Bidders who have built their own Data Centre (IDC), for commercial use will be considered	During the last three financial years, viz; 2014-15, 2015-16 and 2016-17 the bidder must have supplied & implemented at least one data center IT Hardware project(s) in government/PSU/BFSI for India, which include activities like Supply, Installation, Configuration, Maintenance and Operations of the ICT Infrastructure like Server/Security Equipment/ Storage/Backup Equipment for the Data Centre, where the value of each project should be more than (INR) Three crores and Eighty five lakhs (Rs 3.85 crores).	may kindly refer the corrigendum-II
88	28	26.5. Evaluation of Eligibility Criteria	(a) Certificate from bidder’s HR Department for the number of Technically Qualified professionals employed by the company. Along with their Curriculum Vitae delineating their experience as per the format specified in Annexure 4.16 Section IV – Contents of the Bid	(a) Certificate from bidder’s HR Department for the number of Technically Qualified professionals employed by the company,as per the format specified in Annexure 4.16 Section IV – Contents of the Bid	may kindly refer the corrigendum-II
89	28	26.5. Evaluation of Eligibility Criteria	(b) The bidder’s organization must on its roll have at least three (3) ITIL/ISO 20000 Lead Auditor (LA) or Lead Implementer (LI) resources and three (3) BS7799 / ISO 27001 lead Auditor / Lead Implementer certified resources as 31st March 2017.	(b) The bidder’s organization must on its roll have at least three (15) ITIL/ISO 20000 Lead Auditor (LA) or Lead Implementer (LI) resources and three (1) BS7799 / ISO 27001 lead Auditor / Lead Implementer certified resources as 31st March 2017.	may kindly refer the corrigendum-II
90	28	26.5. Evaluation of Eligibility Criteria	(c) The service operations manager deployed for the project,” Appointment of an agency for Supply, Installation, Configuration, Maintenance and Operations of ICT Infrastructure for the establishment of a Data Centre at Delhi” must have an IT experience of 10-15 years with minimum 5 years of relevant experience in Data Center and should have a Post Graduate Degree in Computer Science/graduate degree in computer/IT engineering and should be PMP certified. The designated service operations manager should also be on rolls of the organization for a minimum of 2 years.	(c) The service operations manager deployed for the project,” Appointment of an agency for Supply, Installation, Configuration, Maintenance and Operations of ICT Infrastructure for the establishment of a Data Centre at Delhi” must have an IT experience of 10-15 years with minimum 2 years of relevant experience in Data Center should be PMP certified. The designated service operations manager should also be on rolls of the organization for a minimum of 2 years.	may kindly refer the corrigendum-II
91		Experience in number of years	Bidder’s experience in India for govt/psu, quantified in terms of number of years will be evaluated. *Experience would mean where the bidder has implemented activities like Supply, Installation, Configuration, Maintenance and Operations of the ICT Infrastructure like Security, Network equipment, Storage and Backup equipment, Servers, for the Data Centre*	Bidder’s experience in India for govt/psu/BFSI, quantified in terms of number of years will be evaluated. *Experience would mean where the bidder has implemented activities like Supply, Installation, Configuration, Maintenance and Operations of the ICT Infrastructure like Security, Network equipment, Storage and Backup equipment, Servers.	may kindly refer the corrigendum-II

92		Experience in number of projects	Projects where the bidder has implemented activities like Supply, Installation, Configuration, Maintenance and Operations of the ICT Infrastructure like Security equipment, Storage and Backup equipment for the Data Centre in Govt/PSU with an order value more than Rs 3.85 Crores each shall be considered.	Projects where the bidder has implemented activities like Supply, Installation, Configuration, Maintenance and Operations of the ICT Infrastructure like Security equipment,Server, Storage and Backup equipment in Govt/PSU /BFSI with an order value more than Rs 3.85 Crores each shall be considered.	may kindly refer the corrigendum-II
93		Manpower	The bidder must have on its roll at least 50 technically qualified professionals in the ICT domains like networking, system software, systems integration, storage who have prior experience in providing the Data Center Infrastructure maintenance services.	The bidder must have on its roll at least 50 technically qualified professionals in the ICT domains like Server, networking, system software, systems integration, storage.	may kindly refer the corrigendum-II
94		Resource Allocation	During the last three financial years, viz; 2014-2015,2015-2016,2016-17 the bidder must have implemented at least one projects in government/PSU for India organizations like the ISP - Internet Service Provider/ TSP- Telecom Service Provider etc, which include activities like Supply, Installation, Configuration, Maintenance and Operations of the ICT Infrastructure like Security equipment and Networking equipment, where the value of each project should be more than (INR) Three crores and eighty five lakhs (Rs 3.85 crores) Out of the above one projects one of the projects should meet the following parameters: · ISP providing services in multiple states/regions · Should have deployed enterprise class core routers/switches, security systems like Secure DNS, SSl off loader etc.	During the last three financial years, viz; 2014-2015,2015-2016,2016-17 the bidder must have implemented at least one projects in government/PSU/BFSI for India organizations, which include activities like Supply, Installation, Configuration, Maintenance and Operations of the ICT Infrastructure like Security equipment and Networking equipment, where the value of each project should be more than (INR) Three crores and eighty five lakhs (Rs 3.85 crores)	may kindly refer the corrigendum-II
95	14	Annexure -1, Technical Specifications; 7. EMS Solution		As per the Annexure -1, Technical Specifications, there is a comprehensive set of Minimum Software Requirements Specifications for Enterprise Management System (EMS) on Pg -14 ; then what is the purpose of defining a separate set of technical EMS specifications on Pg -150 of the RFP in section "6.3 Ongoing Operations and Maintenance Services "which are again very detailed in nature. Pls help to understand if the bidder needs to share the technical compliance of EMS of Pg -14 OR of Pg -150. Which set of compliances will be part of the technial bid response for submission.	may kindly refer the corrigendum-II
96	150	6.3.9 Monitoring, Management & Reporting with Enterprise Management System (EMS)	Following functionalities are desired by use of such EMS tools: Availability Monitoring, Management and Reporting Performance Monitoring, Management and Reporting Helpdesk Monitoring, Management and Reporting Securing critical servers using Server based Access Control & recording user activity through audit logs.	This is a security requirement but has been mentioned under EMS solutions. It seems that this security solution has to be given by EMS vendor. However big EMS vendors like HP and IBM differentiate between management software and security solution and hence do not offer this solution. With the current specs, the solution offering is proprietary to one of the OEMs. The solution is provided by companies like MacAfee, RSA etc. and any bidder can quote solutions from them. Request these requirements to be removed from EMS section and included as part of "Railtel Security Framework" or included in FMS services specifications. Please re-phrase the clause as: Following functionalities are desired by use of such EMS tools: Availability Monitoring, Management and Reporting Performance Monitoring, Management and Reporting Helpdesk Monitoring, Management and Reporting	may kindly refer the corrigendum-II

97	160	6.3.9 Monitoring, Management & Reporting with Enterprise Management System (EMS)	The system must support seamless bi-directional integration to the existing helpdesk system for trouble ticketing.	Please share the details of the existing Helpdesk system referred here. Also, there is a detailed fresh technical specifications mentioned for "Helpdesk Management " under Section 7. EMS on Pg 17 of Annexure 1, Technical Specifications; then what is the objective of this integration.	may kindly refer the corrigendum-II
98	14	Annexure -1, Technical Specifications; 7. EMS Solution	9. Ability to deliver comprehensive, tightly integrated management capabilities, including performance and availability of database servers, application servers, web servers, other servers, desktop, network, storage, security, etc	Desktop Performance monitoring is never the scope of the Monitoring Landscape as per the industry's best practices, also polling the client nodes for health/performance management adds the incremental load on the network. Hence, Please rephrase the same as: "Ability to deliver comprehensive, tightly integrated management capabilities, including performance and availability of database servers, application servers, web servers, other servers, network, storage, security, etc "	may kindly refer the corrigendum-II
99		7 > UTM Solution Annex 1	UTM appliance should have a on device storage of min 100GB to be able to hold multiple OS images, logs, backups etc	May please be changed to "UTM appliance should have a on device storage of min 500GB to be able to hold multiple OS images, logs, backups etc	no change to the tender condition
100		73 > UTM Solution Annex 1	The solution must be present as Leaders in Gartner's Magic Quadrant for 2016/2017 and have atleast 90% in the NSS NGFW security effectiveness value.	May please be changed to " The solution must be present as Leaders in Gartner's Magic Quadrant for enterprise network firewalls for 2016/2017 and have atleast 90% in the NSS NGFW security effectiveness value."	no change to the tender condition
101		9 > UTM Solution Annex 1	Firewall should support 5 Million concurrent sessions	May please be changed to "Firewall should support 12 Million concurrent sessions"	no change to the tender condition
102		15 >UTM Solution Annex 1	Support at least 10 firewall domains/instants/context	May please be changed to "Support at least 20 firewall domains/ instants/ context"	no change to the tender condition
103		58 > UTM Solution Annex 1	Should provide protection against viruses, worms or any other malicious content in traffic like SMTP, SMTPs, POP3, POP3s, IMAP, IMAPs, HTTP, HTTPs, FTP, FTPs etc. and must be configurable/applicable on specific firewall Policy	May please be chnaged to "Should provide protection against viruses, worms or any other malicious content in traffic like SMTP, SMTPs, POP3, POP3s, IMAP, IMAPs, HTTP, HTTPs, FTP, FTPs etc. and must be configurable/applicable on specific firewall / threat prevention Policy"	may kindly refer the corrigendum-II
104		7>NGFW Annex 1	The solution appliance should have a on device storage of min 200GB to be able to hold multiple OS images, logs, backups etc	May please be changed to "The solution appliance should have a on device storage of min 500GB to be able to hold multiple OS images, logs, backups etc"	no change to the tender condition
105		NGFW Annex 1	Additional Point	The solution appliance must have support for addition of 40G SFP interfaces in future	no change to the tender condition
106		52>NGFW Annex 1	The management solution must offer console capability for managing the logs, policy, reporting and various features of the The solution.	May be changed to "The management solution must offer a separate centralized management system capable of managing the 10,000 indexed/analytical logs/sec, policy, reporting and various features of the The solution."	no change to the tender condition
107		Anti APT	Query	Please indicate the locations other than Gurgaon where the Anti APT device needs to be installed and Qty if any	may kindly refer the corrigendum-II

108		10> Anti APT	The proposed solution should have the ability to analyze, detect and block malware in common file formats including but not limited to executables, JAVA, PDF, MS Office documents (doc, docx, xls etc), common multimedia contents like JPEG, GIF and ZIP/RAR/7ZIP/TNEF archives, to prevent advanced Malware and Zero-day attacks.	The proposed solution should have the ability to analyze, detect and block malware in common file formats including but not limited to executables, JAVA, PDF, MS Office documents (doc, docx, xls etc), common multimedia contents like JPEG, GIF, pif, com, scr, csv,iso, cpl, wsh and ZIP/RAR/7ZIP archives, to prevent advanced Malware and Zero-day attacks.	no change to the tender condition
109		2>Anti APT	The solution must employ an on premise (not on cloud) analysis engine using virtual execution to detect zero day and unknown threats and must not be signature based.'	May be changed to " The solution must employ an on premise (not on cloud) analysis engine using virtual execution(OS Emulation) and CPU flow detection (CPU Emulation) to detect ROP, zero day and unknown threats and must not be signature based."	no change to the tender condition
110		17>Anti APT	The proposed solution should have the ability to scan and analyze emails to identify malicious attachments or URLs.	May be changed to "The proposed solution should have the ability to scan,analyze, clean and remediate emails of malicious attachments or URLs. The solution should be able to convert the attachment to clean PDFs"	no change to the tender condition
111		UTM,NGFW, APT	Additional Point	No backdoor/malicious code should have been identified in the OEM solution for all security products like UTM, NGFW, APT, WAF etc in the past 3 years. The OEM should present a written and signed undertaking from the head of engineering/legal divison in this regard.	no change to the tender condition
112		UTM,NGFW, APT	Additional Point	In case multiple security products like UTM, NGFW, APT are from the same OEM a single centraized management solution must be provided	no change to the tender condition
113	128	Tape Library	The Tenderer should provision tape library as a backup device for the purpose of data backup & restoration.	Requesting you to pls add the Drive & Tape Slot Count as "It shall have min. 6 Nos. LTO-7 Drives and 400 Tape Slot License with LTO-7 Media with Barcode"	may kindly refer the corrigendum-II
114	128	Tape Library	The tape library should include a bar-code reader to enable managing the inventory of tape cartridges.	Kindly Include the Scalability criteria of the Tape Library in Terms of Tape Drives Slot minimum to double capacity in PB as 24 Drives & 800 Tape Slots.	may kindly refer the corrigendum-II
115	128	Tape Library	The tape library should have mixed media support and should be proposed along with necessary software/licenses	Kindly Change it to- The tape library should have mixed media support and should be proposed along with necessary software/licenses, If applicable.	may kindly refer the corrigendum-II
116	128	Tape Library	The Tenderer should provision adequate number of native full-duplex Fibre Channel ports on the tape library so as to stream data for full-utilization of all the tape drives and also ensuring the backup requirement indicated above.	Kindly modify the Tape Drive as a FULL Height Drives, as Full Height drives are more robust and durable in performance Delivery. Cost of the Half-Height drives & Full Height drives are same for users.	no change to the tender condition
117	128	Tape Library	Proposed Tape library should be supplied along with required rack mounting kit which should fit into 42U rack or should be 45U library frame size. Supply should include all the required cables/PDUs/equipment's necessary for making the system operational.	PDUs and other Rack equipments shall be covered bu the Bidders, as the Tape library will come with their own power supply and cables , NOT with PDU & other rack cables.	may kindly refer the corrigendum-II
118	128	Tape Library	Tenderer should provision native web-based remote management tool for remote administration.	Shall also provide Advance level of Reporting to have all the reports on Media & Jobs	no change to the tender condition
119	128	Tape Library	Offered Tape drive should be native FC/ SAS LTO-7.	Shall be 8 Gbps FC interface. SAS interface comes in standalone drives only.	no change to the tender condition
120	128	Tape Library	Tape drives with Encryption capability	Shall proposed with Encryption enabled Drives and Encryption manager to manage the encrytion keys in Redundant fashion in the form of additional Hardware.	may kindly refer the corrigendum-II
121	32	26.6. Evaluation of Technical Bids	Backup Solution - Tape Library scalability (1 mark): The proposed Tape library will be evaluated with respect to the max no.of drive supported in a single library and partitioning. The bidder with maximum drives in a single library will beconsidered for maximum marks and the rest will be given marks on pro rata.	Evaluation Criteria shall be based on the Total PetaByte of Capacity handling / Total Tape Slots, along with the No. of Full Height Drives in the Offered Single/ same Library.	may kindly refer the corrigendum-II
122		Annexure 1	4. Should have the ability of caching, compression of web content and SSL acceleration.	we would like to suggest that Railtel should ask for Compression and caching at hardware level to reduce the CPU and Memory utilization and it will help railtel to leverage same appliances with better functionality at high loads...	no change to the tender condition

123		Annexure 1	7. Should inspect both web page content, such as Hypertext Markup Language (HTML), Dynamic HTML (DHTML), and Cascading Style Sheets (CSS), and the underlying protocols that deliver content, such as Hypertext Transport Protocol (HTTP) and Hypertext Transport Protocol over SSL (HTTPS). (In addition to SSL, HTTPS includes Hypertext Transport Protocol over TLS.)	As every application is different and few applications would be public facing and that will be accessed over different browsers possibly, so waf solution shall provide flexibility per application policies. Thus The solution should support TLS v1.2 and v1.3 with ciphers supporting forward secrecy that have the capability to define the key exchange algorithm, ciphers, cipher strength and renegotiation parameters granularly at a per application level.	no change to the tender condition
124		Annexure 1	8. WAF should support dynamic source IP blocking and should be able to block attacks based on IP source.	Request to consider a solution that should give Administrator the capability to manually unblock a specific source IP in the event of a false positive.	no change to the tender condition
125		Annexure 1	9. The solution must be able to perform validation on all types of input, including URLs, forms, cookies, query strings, hidden fields, and parameters, HTTP methods, XML elements and SOAP actions.	In order to have a holostic solution the proposed solution should also have the capability to perform validation at granual level such as :- a. Define character set per parameter b. Define signatures per parameter	no change to the tender condition
126		Annexure 1	10. Inspect any web socket protocol (proprietary or standardized) or data construct (proprietary or standardized) that is used to transmit data to or from a web application, when such protocols or data are not otherwise inspected at another point in the message flow.	Web Socket can also be over SSL, in that case Railtel would need more than just inspection and a Waf solution should have capability to look at content to check and ensure no attack going through the enrcrtpted WEb socket protocol and WAF should be able to attach signature for security. thus"WAF should support both WS and WSS URLs. Should have the capability to dynamically learn the websocket URLs, content type within the URL (text, binary or JSON). WAF should have the capability to define attack signature set for the websocket URLs."	no change to the tender condition
127		Annexure 1	13. Actions taken by WAF to prevent malicious activity should include the ability to drop requests and responses, block the TCP session, block the application user, or block the IP address.	when you just drop the trafffic and send connection reset to both parties eg. "page not found", again debug process will start and in that case user will not be aware why he was not able to access the requested page in that case a customizable page with updated mesage like call help desk number xxxxxxx will be better way of approach maintin user ecperience, also a data masking feature in case to restrict any confidential information going out in response to user. Also when data needs to be uploaded you cannot and will not want let any document to get uploaded as it is and would like to check in case of any malacious code or virus is present thus a waf should also have a capability to integrate with ICAP server for further inspection eg. Antivirus severs etc . . . "WAF should have the capability to provide a custom block page. WAF should have the capabilty to identify credit card numbers or any custom expression in the payload response and mask the same without blocking the response. WAF should have the capability to integrate with an external ICAP server for content inspection."	no change to the tender condition
128		Annexure 1	16 The Web application firewall should allow signatures to be modified or added by the administrator.	Administrator should have the capability to create a custom signature set choosing selectively signatures.	no change to the tender condition
129		Annexure 1	17 The Web application firewall should support automatic updates (if required) to the signature database, ensuring complete protection against the latest application threats.	WAF should have the capability to update the signature set and signature engine either manually or automated schedule.	no change to the tender condition
130		Annexure 1	20 WAF should support different policies for different application sections.	a Waf solution should have all the three major parameters for application section like Hostname, URL and Header, this will help to railtel to have granular policy defination and control.	no change to the tender condition

131		Annexure 1	21 The Web application firewall should automatically learn the Web application structure and elements.	Request to add minimum parameters which a Waf solution should have capability to earn like : "a. Hostname b. URLs c. File Type d. Logon Page e. Response Type f. Parameters at URL level g. Hidden Form Parameters h. Cookies i. Encoding & j. Application Framework"	no change to the tender condition
132		Annexure 1	26 The Web Application Firewall should have "anti-automation" protection which can block the automated attacks that use hacking tools, scripts, frame work etc.	While looking at Anti Automation Protection in WAF "The proposed solution should have the ability to define a custom BOT signature. ability to allow, block or log the activity of BOT., to challenge a suspicious BOT activity with built-in image CAPTCHA."	no change to the tender condition
133		Annexure 1	32 Should be able to generate comprehensive event reports with filters:	The proposed solution must have a report based on severity level	no change to the tender condition
134		Annexure 1	35 Unique transaction ID should be assigned to every HTTP transaction (a transaction being a request and response pair), and included with every log message.	The proposed should have the capability to send logs to one or many remote logging servers. Should support remote logging via HSL.(high speed logging). Should have the capability to select the fields to be sent to each log destination.	no change to the tender condition
135		Annexure 1	36 Web application firewall should provide notifications through Email, Syslog, SNMP Trap etc.	WAF should have the capability to schedule automated reports via email.	no change to the tender condition
136		Annexure 1	DNS Functional Requirement:- 17 Should support NXDOMAIN redirection	the proposed DNS solution should have capabilities to support negative caching to absorb repeat NXDOMAIN attacks. As it will ensure absorption of DNS NXdomain attack for repeat domain requests. It ensures that no repeat request for Non-existant domain hits Root hints	no change to the tender condition
137		Annexure 1	DNS Functional Requirement:- 27 Specific portions of the cache can be discarded without restarting the server	"The proposed solution should support event based TCL scripting to manipulate data traffic. Because "Scripting capability can help service provider to modify the DNS traffic as per demand . For instance, on day 0, if Department of Telecom demands blocking of certain type of domains and wants a Walled garden response – Scripting can help (also RPZ can do this). Other than than scripting can also help influence overriding multiple parameters in DNS traffic to tweak responses from DNS system according to service providers – there by giving flexibility."	no change to the tender condition
138		Annexure 1	DNS Functional Requirement:- 28 The DNS must provide appropriate automated failover and disaster recovery mechanisms	The proposed DNS solution should support state table synchronization to ensure seamless failure. This will ensures immediate failover without loss of sessions	no change to the tender condition
139		Annexure 1	Logging Alerting & Trouble shooting:- 50 The product must allow configuration of TCP or UDP for the Syslog transport mechanism	The proposed solution should also have capability for setting up UDP idle timeout to ensures that sessions are timed out when not used & system doesn't necessarily holds old connection. In events of High DNS queries – where there could be high session table demand – quick idle timeout would free up system for handling more new subscriber DNS requests.	no change to the tender condition

140	7	3. Anti–Virus Solution)- point 31	Comprehensive onsite warranty for 3 years with Next business Day (NBD) resolution.	This is software component and OEM can't provide NBD resolution, this is generally for hardware component, kinldy remove this point from AV component.	may kindly refer the corrigendum-II
141	127		Request RAILTEL to add Gartner	Proposed backup solution must be in Gartner's leader quadrant consequently from last three years.	no change to the tender condition
142	127		Is Ransomware alert is required in Backup fot clients	The proposed backup solution must have native inbuilt alert capability for Ransomware affected clients	no change to the tender condition
143	127		Is backed up storage disk need to be protected from Ransomware	Proposed backup solution must have inbuilt capability to protect the backed up disk volume from Ransomware.	no change to the tender condition
144	127		RFP has asked for two solutions i.e. Security and Backup. We understand both solutions are independent of each other with respective OEM's. iHence it is our submission that separate price should be taken for both the solution; for final individual evaluation.		no change to the tender condition
145	Annexure 1-Technical Specifications page 2&3/33 RailTel/Tender/OT/CO/DNM/2017-18/DC page number 126/195	1. SSL device 2. Web application firewall 4. Data Centre Infrastructure	Suggestion for next generation multi-tenant network function virtualization platform with SSL and WAF support on same hardware with dedicated hardware resources with guaranteed performance	Traditional hardware based networking appliances does not offer flexibility, agility and multi-tenancy to meet modern networking requirements such as portability, automation, consolidation of multiple network functions, management and orchestration. Cloud computing, SDN and network function virtualization are key attributes for next gen data centers. Moreover DC requirements in RFP (page number 126/195) are aligned to virtualization and cloud computing offerings. SSL and WAF being AFE (application front end) device must comply with next generation NFV and cloud computing requirements, having said that it is recommended that *“SSL and WAF network functions should be deployed on next generation multi-tenant platform and must support traffic isolation, fault isolation and network isolation in order to meet the architectural environment. Each network function must have assigned dedicated hardware resources including I/O interfaces, memory, CPU, SSL card in order to ensure every network functions guarantee the desired performance without affecting other functions”.* *“SSL and WAF network functions to be offered from different OEM to ensure reduced surface attack area and maximum security”* . Platform should also support 3rd party virtual function to meet the current and future requirements along with scalability to accommodate additional instance for SSL and WAF on same hardware with license upgrade	no change to the tender condition
146	Annexure 1-Technical Specifications page 2/33	1. SSL device	System must support at least 30 Application Delivery partitioning / Virtual context, dedicated configuration file, routes for each customer's traffic, where in resources can be either dedicated to each partition or can leverage common pool of resources i.e. CPU and Memory, concurrent connection for each context should be configurable	Number of partition / virtual context requirements is not inline to performance numbers. 4Gbps SSL throughput across 30 virtual contexts is equivalent 130Mbps assumingly equal distribution of resources. Moreover common pool of resources does not guarantees performance and may negatively affect the application performance.. Specs are favoring to specific OEM. It is suggested to remove this clause	no change to the tender condition

147	Annexure 1-Technical Specifications page 2/33	2. Web application firewall	System should support different protocol parsers such as HTTP, SSL, DNS, FTP,TFTP, SIP, SMTP, SPDY, RTSP, RADIUS,	SPDY has been standardized to HTTP2 by IEEE. Most of the current and future adoption is on http2 protocol. It is suggested to remove SPDY support. Refer. https://blog.stackpath.com/spdy-to-http2 https://blog.cloudflare.com/introducing-http2/	no change to the tender condition
148	Annexure 1-Technical Specifications page 5/33	2. Web application firewall	The solution must support the web application vulnerability assessment tools (Web application scanners in Leaders of Latest Gartner Magic Quadrant Application Security Testing) to virtually patch web application vulnerabilities.	web application vulnerability assessment Specs are favoring to specific OEM. It is suggested to modify the caluse The solution must support the web application vulnerability assessment tools to virtually patch web application vulnerabilities.	no change to the tender condition
149	Annexure 1-Technical Specifications page 5/33	1. SSL device 2. Web application firewall	The solution must be a Leader or Challenger in the Gartner Magic Quadrant of Web Application Firewalls 2016/2017	As per Gartner, Visionaries understand where the market is going or have a vision for changing market rules with next generation features and functionalities. Vendor in Visionary quadrant does offer better feature/functionalities than challengers.. It is suggested to include Gartner visionary quadrant as well.	no change to the tender condition
150	Annexure 1-Technical Specifications	8. UTM Solution	IPS throughput should be atleast 1 Gbps or better for real world/production throughput	Considering Firewall throughput of 8 Gbps, 1 Gbps IPS throughput is very less. It is suggested that the IPS throughput should be 2Gbps or more for real world / production traffic	no change to the tender condition
151	Annexure 1-Technical Specifications	8. UTM Solution	Firewall should support 120,000 new sessions per second	Today there are many applications which keep running on PCs / Servers / Laptops and which try to connect to internet for various downloads like windows updates / antivirus updates and other online applications. These application keeps opening sessions automatically. The firewall should not become a bottleneck in case of a virus or trojan generating huge nos of connections. To ensure that the firewall is capable of handling such traffic scenarios it is important that firewall is capable of handling very high concurrent sessions and new sessions per second. It is suggested that the Firewall should support minimum 220,000 new sessions per second	no change to the tender condition
152	Annexure 1-Technical Specifications	9. Next-Gen Firewall (NGFW)	Firewall should support 180,000 new sessions per second	Today there are many applications which keep running on PCs / Servers / Laptops and which try to connect to internet for various downloads like windows updates / antivirus updates and other online applications. These application keeps opening sessions automatically. The firewall should not become a bottleneck in case of a virus or trojan generating huge nos of connections. To ensure that the firewall is capable of handling such traffic scenarios it is important that firewall is capable of handling very high concurrent sessions and new sessions per second. It is suggested that the Firewall should support minimum 280,000 new sessions per second	no change to the tender condition
153	Annexure 1-Technical Specifications	11- APT solution - point 1	The solution should be able to communicate birectionally with the proposed UTM and NGFW solution for automatic blocking/threat update	Due to this clause, that means only UTM vendor can participate in anti-APT solution and required Anti-APT solution bundled with UTM box. Please delete this point so that Anti_APT vendor can also participiate.	may kindly refer the corrigendum-II
154	Annexure 1-Technical Specifications	11- APT solution - point 30	It should support Sandbox Analysis for multiple operating systems like WinXP,Win7,Win8,Win10	Why sandboxing analysis for end user OS, threat can be designed ;for server OS, so please add server 2003 and 2008 OS as well for sanboxing.	no change to the tender condition
155	Annexure 1-Technical Specifications	11 - WAF	WAF should support inline bridge or proxy mode of deployment.	WAF should support full reverse proxy in inline bridge or Proxy mode of deployment	no change to the tender condition

156	Annexure 1-Technical Specifications	55 - WAF	System must have minimum(fully populated) 2 x10G SFP/SFP+ Ports and option of min. 2 SFP/SFP+ for 10G connectivity (field upgradable on same hardware)	WAF should have minimum (fully populated) 2 x 10GbE w/bypass SPF+ (MM) + 6 x 1 GbE w/bypass SPF (MM) + 1 x 1GbE Mgmt Ports from day one.	no change to the tender condition
157	Section II	9.3	Firm Price Purchaser reserves the right to review the charges payable for the Data Centre Operations and Management at the beginning of each year or at any time at the request of Purchaser whichever is earlier to incorporate downward revisions if applicable and necessary.	Bidder clarifies that the bidder will submit a fixed price an any revision on the price will be subjected to mutual agreement	No change to the tender condition
158	Section II	28.1 and 28.3	Purchaser's Right to Vary Scope of Contract at the time of Award The Purchaser may at any time, by a written order given to the Tenderer, make changes to the scope of the Contract without assigning any reasons. The bidder shall comply with such modifications unconditionally provided these are made before completion of the deliveries under the LOA/SPO/PO. Any such change in quantity shall have no impact on the rates mentioned in the LOA/SPO/PO for any such item. Rate Contract If required, RailTel would also enter into Rate Contract with the firm to whom the contract is awarded for catering to additional requirement of Equipment / Card / Software / Module as and when arise in future. Rate Contract on the successful tenderer would be placed separately and would be operative from the date of PAC and would be valid for a period of 24 months. This Rate Contract would be at the same rates as finalized in main contract.	Bidder clarifies 1. The price will be submitted as per the requirement of RFP and price for any changes in the quantity will required to be mutually agreed. 2. Rate contract if required will be at re-negotiated price. 3. Payment for additional requirement of Equipment /Card /Software /Module, will be 100% on delivery with no requirement of additional PBG	No change to the tender condition
159	Section II	32.1 and 32.2	Bank Guarantee for Contract Performance Within 15 days after the receipt of notification of award of the Contract from the Purchaser, the successful Tenderer shall furnish Contract Performance Guarantee to the Purchaser, which shall be equal to 20% of the value of the Contract and shall be in the form of a Bank Guarantee Bond from a Nationalized Bank in the Proforma given at Section VI – Additional Requirements/ Pro forma. Failure of the successful Tenderer to comply with the requirement of Clause 31 or Clause Error! Reference source not found. shall constitute sufficient grounds for the annulment of the award and forfeiture of the EMD. In case of exigency, if the Purchaser gets the work done from elsewhere, the difference in the cost of getting the work done will be borne by the successful Tenderer.	1. Bidder request to change the requirement of Contract Performance Guarantee to 10% of the value of the contract. 2. Bidder request to remove "or Clause Error! Reference source not found" from clause 32.2	may kindly refer the corrigendum-II
160	Section II	36	Payment Term	Bidder request 1. To pay 100% of the Hardware and software value on delivery as bidder is also submitting PGB 2. To change the payment for Services as: i) 60% of "Installation, Testing and Commission" on successful Installation, Testing and Commission, 30% on issue of PAC and 10% on issue of FAC ii) Payment for Long term Maintenance (AMC) - Quarterly in arrear iii) Payment for Operation and Maintenance - Quarterly in arrear	may kindly refer the corrigendum-II

161	Section II	36	Payment Term	As per RFP Clause 36.5.3 Payment for operations phase will be made within 30 days of invoice. Please clarify that the same applies to supply phase also.	may kindly refer the tender document
162	Section III	4.4.3	Warranty Support	Bidder clarifies the maximum penalty will 10% of the affected product	No change to the tender condition
163	Section III	4.4.3 & 4.4.5	During the warranty period, agency should stabilize the working of the system. Purchaser has the right to extend the period of warranty 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 agency at no cost to RailTel as to make good all the deficiencies	Since SLA penalty will be charged during warranty period, bidder request to remove this clause	No change to the tender condition
164	Section III	9	Contract performance Guarantee Within 15 days after the receipt of notification of award of the Contract from the Purchaser, the successful Tenderer shall furnish Contract Performance Guarantee to the Purchaser, which shall be equal to 20% of the value of the Contract and shall be in the form of a Bank Guarantee Bond from a Nationalized Bank in the Proforma given at Section VI – Additional Requirements/ Pro forma	In line with the request made to the PBG sought in section II, it is requested to revise the value of the BG to 10% of the contract value. The clause does not contain conditions of invocation of the PBG. Kindly confirm that the below will be the only conditions under which the BG may be invoked: "Performance Bank Guarantee shall be invoked only in the event of the contract being terminated for non-performance by the bidder and after provision of a 30 day written notice of the intent to invoke the guarantee. "	may kindly refer the corrigendum-II
165	Section III	16.3	Penalty for Delay in Implementation	Bidder request to change the penalty to 0.5% per week of the undelivered value limited to 10% of the cost of supply, Installation and commission	may kindly refer the corrigendum-II
166	Section III	18.2	Agency shall provide “Most Preferred Customer” status to the Purchaser. Accordingly, the prices payable for services relating to the Maintenance and Management of the ICT infrastructure and shall in no event exceed the lowest price at which the Agency offers similar services to any other customer during the currency of the contract.	Bidder request to delete this clause as this is RFP price competitive bid.	may kindly refer the corrigendum-II
167	Section III	18.3	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 Advanced purchase order, the equal benefit of lower prices will be passed on to purchaser. The tenderer will submit an undertaking to his effect while claiming the payment.	Bidder request to change the clause as The tenderer shall undertake that in case the tenderer offered identical material at a lower price to central/state/government organization or public sector undertaking during the last one year from the date of submission of this RFP, the equal benefit of lower prices will be passed on to purchaser.	No change to the tender condition
168	Section III	25	Liquidated damages	Bidder request to delete this clause as the penalty for delay in implementation has already been covered in Section III clause 16.3	No change to the tender condition
169	Section VII	4	Service Level Agreement & Targets	Bidder request to cap the SLA penalty to 10% of the quarterly payout.	No change to the tender condition
170	Annexure -1, Technical Specifications; 7. EMS Solution	14		As per the Annexure -1, Technical Specifications, there is a comprehensive set of Minimum Software Requirements Specifications for Enterprise Management System (EMS) on Pg -14 ; then what is the purpose of defining a separate set of technical EMS specifications on Pg -150 of the RFP in section "6.3 Ongoing Operations and Maintenance Services "which are again very detailed in nature. Pls help to understand if the bidder needs to share the technical compliance of EMS of Pg -14 OR of Pg -150. Which set of compliances will be part of the technial bid response for submission.	may kindly refer the corrigendum-II

171	6.3.9 Monitoring, Management & Reporting with Enterprise Management System (EMS)	150	Following functionalities are desired by use of such EMS tools: Availability Monitoring, Management and Reporting Performance Monitoring, Management and Reporting Helpdesk Monitoring, Management and Reporting Securing critical servers using Server based Access Control & recording user activity through audit logs.	This is a security requirement but has been mentioned under EMS solutions. It seems that this security solution has to be given by EMS vendor. However big EMS vendors like HP and IBM differentiate between management software and security solution and hence do not offer this solution. With the current specs, the solution offering is proprietary to one of the OEMs. The solution is provided by companies like MacAfee, RSA etc. and any bidder can quote solutions from them. Request these requirements to be removed from EMS section and included as part of "Railtel Security Framework" or included in FMS services specifications. Please re-phrase the clause as: Following functionalities are desired by use of such EMS tools: Availability Monitoring, Management and Reporting Performance Monitoring, Management and Reporting Helpdesk Monitoring, Management and Reporting	may kindly refer the corrigendum-II
172	6.3.9 Monitoring, Management & Reporting with Enterprise Management System (EMS)	160	The system must support seamless bi-directional integration to the existing helpdesk system for trouble ticketing.	Please share the details of the existing Helpdesk system referred here. Also, there is a detailed fresh technical specifications mentioned for "Helpdesk Management " under Section 7. EMS on Pg 17 of Annexure 1, Technical Specifications; then what is the objective of this integration.	may kindly refer to the corrigendum-II
173	Annexure -1, Technical Specifications; 7. EMS Solution	14	9. Ability to deliver comprehensive, tightly integrated management capabilities, including performance and availability of database servers, application servers, web servers, other servers, desktop, network, storage, security, etc	Desktop Performance monitoring is never the scope of the Monitoring Landscape as per the industry's best practices, also polling the client nodes for health/performance management adds the incremental load on the network. Hence, Please rephrase the same as: "Ability to deliver comprehensive, tightly integrated management capabilities, including performance and availability of database servers, application servers, web servers, other servers, network, storage, security, etc "	may kindly refer to the corrigendum-II
174	36	5.2	AMC Payment Terms	Request you to make the payment terms as monthy deffered for AMC support.	No change to the tender condition
175	36	5.3	Payment Terms for Operation & Maintennace Services	Request you to make the payment terms as monthy deffered for O&M services.	may kindly refer the corrigendum-II
176	3	1.19	That the Agency shall provide adequate and appropriate support and participation, on a continuing basis, in tuning all supplied ICT infrastructure to meet the requirements of the applications.	As per our understanding the inputs for the tuning of the infra will come from the application team. Infra team will act acoordingly in conjunction with the application team. Please confirm the understanding.	may kindly refer the tender document
177	4	4.2	To enforce fulfillment of support objectives, bidder shall make available services of qualified engineer(s) at the Data Center / location to be decided by RailTel to the satisfaction of RailTel.	Please share the location details? Also as per our understanding no dedicated resource is required, resources will be required on call basis, please confirm?	may kindly refer the tender document
178	4	4.5	During the warranty period, agency should stabilize the working of the system. Purchaser has the right to extend the period of warranty 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 agency at no cost to RailTel as to make good all the deficiencies.	Reuquest you to share what are the parameters for stabilization? HPE will share the stabilization period in their proposal. If the stabilization time increases beyond that time Railtel and HPE shall come and mutually discuss on the support changes.	may kindly refer the tender document

179	5	1	Tenderer/OEM/OSSP shall provide maintenance support after successful completion of the warranty obligations for a minimum period of 24 months for hardware and 24 months software items (further extendable after negotiation). The long term maintenance support shall be comprehensive and include all hardware and software of equipment etc. supplied against this contract. RailTel should be extended the benefits of software update/up-grades made by OEM/OSSP on the system from time to time to improve performance. During this period the scope of work as mentioned in clause 4 & its sub-clauses, above, will be applicable.	While HPE will be able to provide the hardware AMC support after warranty support for a duartion of 2 years, Software warranty shall be for the complete duration of the contract as this will fulfill the requirement of software update/up-grades made by OEM/OSSP on the system from time to time to improve performance.	No change to the tender condition
180	5	2	Separate agreement for AMC after warranty period shall be entered with tenderer by RailTel. A fresh Bank Guarantee for a value of 10% of the value of the AMC contract's annual value valid for a period of 4 months beyond the AMC period from the date of issue of LOA shall be required to be submitted by OEM/Tenderer for due fulfillment of long term maintenance support obligation.	This bank guarantee for the AMC shall be submitted at the time of AMC contract as per our understanding, pls confirm?	may kindly refer the tender document
181	12	1	The Agency shall not sub-contract any part of the scope of the work.	It is requested to delete this clause. Certain portions require sub-contracting and the Bidder will keep Railtel informed of the particular scope being sub-contracted along with the details of the sub-contractor employed. The overall responsibility of completing the works shall remain with the Bidder.	may kindly refer the corrigendum-II
182	13	6.9	The Agency should provide technology refresh information to the Purchaser as and when the OEM comes out with the same.	AS per our understanding HPE has to provide the information of new refresh. Bidder is not liable for doing a technology refresh, please confirm the understanding?	may kindly refer the tender document
183	2		Onsite support for Data Centre Operations on 8x5x365 basis by qualified and trained engineers/personnel for a period of one year (with extension to 2 more year) to ensure more than 99.9% service availability.	Please clarify, are onsite resources only required for a duration of 1 year(Which might get extended to 2 years) from the date of commissioning?? Also to mainatain an availability of 99.9% the resource shall be available round the clock. If the resources are only available onsite during 8*5 shift then how will the availaibility of the services be maintained during hours, please clarify?	may kindly refer the tender document
184	General		Location	As per our understanding the location for DC and DR will be Gururgram(For DC) and secunderabad(For DR), please confirm?	Both the location currenly act as a DC
185	General		Resources Deployment	As per our understanding the resources asked in the RFP will be deployed similarily for both sites, please confirm?	Resources will be deployed only at Gurugram Data Centre
186	6	3.1	The Tenderer shall provide a 24x7x365 Help Desk facility for reporting issues / problems with the ICT infrastructure as well as non-IT components	As pe rour understanding the help desk will be onsite and railtel will provide the space, dedicated line, required enviornemt for the operation of the help desk, please confirm?	RailTel shall provide the necessary physical infrastructure/environe mnt
187	6	3.4	Proactive monitoring of all the applications hosted in the Data Center.	As per our understanding application management is our of the scope of HPE, HPE role will be limited to monitoing the application and doing vendor anagement for the ticket resolution with the respective vendor, please confirm? Application management, administration,operation will be out of the scope of the bidder, please confirm?	may kindly refer the tender document

188	6	3.5	Facilitate application migration in coordination with application owners/departments	Please clarify what will be bidder responsibility in "Application Migration" activity?	Provide the necessary network/ICT infra facilitation
189	6	3.8	Monitor NIPS for 24*7 availability	As per the RFP the expectation is to monitor NIPS 24*7 while the resources asked shall be only available for 8*5 shift, please share how shall the monitoring be done after the resources are not available onsite?	Recources deployed are for L2 and above levels, L1 level monitoring will be carried by RailTel
190	8		The total quarterly deduction should not exceed 25% of the applicable fee.	Request you to please limit the penalty to 10% of the quarterly payment.	No change to the tender condition
191	Section III	6	Scope of Contract 6.3 If any services, functions or responsibilities not specifically described in this Contract are an inherent, necessary or customary part of the Services or are required for proper performance or provision of the Services in accordance with this Contract, they shall be deemed to be included within the scope of the work to be delivered for the Charges, as if such services, functions or responsibilities were specifically described in this Contract. 6.4 The Purchaser or Purchaser's Technical Representative reserves the right to amend any of the terms and conditions with mutual agreement in relation to the Scope of Work and may issue any such directions which are not necessarily stipulated therein if it deems necessary for the fulfillment of the Scope of Work.	It is requested to delete this clause. The proposal from the Bidder shall be based on the Scope of Work provided by Railtel, which we believe was prepared with support from an external consultant. The exhaustive scope shall be as per the executed SOW and any further modifications shall be solely vide a Change Order accounting for the additional costs involved in implementing such changes. Any amendment to terms shall be subject to mutual agreement as stated in the clause. All new directions shall need to be mutually agreed prior to implementation of the same.	No change to the tender condition
192	Section III	13.6.2	Obligations related to ICT infrastructure Incase of any dissatisfaction or default on part of the Agency in providing the level of support desired by the Purchaser or Purchaser's Technical Representative in relation to the ICT infrastructure supplied by the Agency, the Agency shall extend the necessary support required to meet the commitments without any financial liability to the Purchaser	It is requested to clarify that the reference to dissatisfaction in the clause shall pertain to the objective criteria of SLAs and obligations as mentioned in the Scope of Work document.	Tender conditions are clear
193	Section III	13.6.4 13.6.9	In case of any problems / issues arising due to integration of the ICT infrastructure components supplied by the Agency with any other component(s)/product(s) under the purview of the overall solution, the Agency shall replace the required component(s) with an equivalent or better substitute that is acceptable to Purchaser without any additional cost to the Purchaser and without impacting the performance of the solution in any manner whatsoever The Agency should provide technology refresh information to the Purchaser as and when the OEM comes out with the same.	The problems/issues shall be handled as per the warranty obligations and the repair/replacement shall be made as per the applicable warranty entitlements. The overall performance levels are to be maintained by the Bidder as per the defined SLAs. Unless covered by the warranty, the technology refresh shall be at additional costs which are to be mutually agreed at the applicable time.	No change to the tender condition
194	Section III	17	Term and Extension of the Contract	It has been stated that the term of the contract shall be initially for a period of one year. It is requested to delete such reference to any term of the Agreement since this is an obligation oriented contract where the Agreement will be automatically terminated upon successful discharge of the obligations. Placing a specific term as the valid period of the Agreement will result in a confusion in the operation of the Agreement.	No change to the tender condition
195	Section III	18.1	Prices quoted must be firm and shall not be subject to any upward revision on any account whatsoever throughout the period of contract.	It is requested to clarify that in the event of change in tax regime, the suitbale implication (upward/downward) will be found on the prices.	may refer the tender documents

196	Section III	21.2	Termination for Default However, the security deposit of tenderer shall be forfeited and Performance Guarantee shall be encashed.	It is requested to clarify that the PBG shall be invoked only to the extent of actual loss/damage suffered in the event of termination.	Tender conditions are clear
197	Section III	25	Liquidated damages	Bidder request to delete this clause as the penalty for delay in implementation has already been covered in Section III clause 16.3	No change to the tender condition
198	Section III	26	Settlement of Disputes	It is requested to introduce an intial layer of internal escalation mechanism before reaching out to the Arbitrators.	No change to the tender condition
199	Section III	27	Insurance	It is requested to delete the requirement of insurance since: i. The title in all goods shall be transferred to Railtel upon delivery and hence Bidder cannot further insure them. Until the time of delivery, the risk associated with goods shall lie with the Bidder. ii. the insurance policies cannot be pledged in the name of Railtel. iii. Where there is any damage or loss, the claim may be placed on the Bidder and reference to insurance would not be required.	No change to the tender condition
200	Section III	33	System Performance Guarantee	It is requested to clarify that there will be a clear acceptance provided by Railtel as per the Accteptance Test Criteria on objective parameters which confirms that the deliverables meet the requirements as anticipated.	Tender conditions are clear
201	Section VII	4	Service Level Agreement & Targets	Bidder request to cap the SLA penalty to 10% of the quarterly payout.	No change to the tender condition
202	Annexure 1- Techn	DNS Security	The Proposed Appliance should be able to handle 200K QPS for Non Authoritative	No. of Locations where DNS Server need to Be Commissioned Both Authoritative and Caching.	Two DC locations
203	Annexure 1- Techn	DNS Security		The QPS mentioned in the RFP is cumulative or per location	Per location based
204	Annexure 1- Techn	DNS Security	Should be able to secure the system from DNS DOS/DDoS attacks.- LAND Attack	is there any requirement to provide implement the mitigation policies per IP/Network	The solution should support implementation of Security policy per IP/Network.
205	Annexure 1- Techn	DNS Security	DNS record type ACL		The solution should support implementation of Security policy per IP/Network.
206	Section V	4	The system should support IPSEC VPN, PPTP VPN, L2TP VPN and SSL VPN.	Please change the clause to "The system should support IPSEC VPN and SSL VPN. "	may kindly refer to the corrigendum-II
207	Section V	4	The proposed solution should support Virtualization (Virtual Firewall, Security zones and VLAN).	Please change the clause to "The proposed solution should support Virtualization (Security zones and VLAN). "	may kindly refer to the corrigendum-II
208	Section V	4	Administrator shall be able to define sensitive data patterns, and data matching these patterns that will be blocked and/or logged when passing through the unit.	Please remove this clause	may kindly refer to the corrigendum-II
209	Section V	4	The IPS should be capable of detecting and blocking zero-day attacks without requiring an update.	Please change this claue to "The IPS should be capable of detecting and blocking zero-day attacks/vulnerabilities without requiring an update. "	no change to the tender condition
210	Section V	4	The solution should be able to communicate bi-directionally with the proposed UTM solution for automatic blocking.	Please remove this clause	may kindly refer to the corrigendum-II
211	Section V	4	The proposed solution should perform dynamic real-time analysis of advanced malware on the appliance itself to confirm true zero-day and targeted attacks. No information should be sent to third party systems or cloud infrastructure system for analysis and detection of Malware.	Please change the clause to "The proposed solution should perform dynamic real-time analysis of advanced malware to confirm true zero-day and targeted attacks. No information should be sent to third party systems or cloud infrastructure system for analysis and detection of Malware. "	no change to the tender condition

212	Section V	4	The proposed solution should have the ability to analyze, detect and block malware in common file formats including but not limited to executables, JAVA, PDF, MS Office documents, common multimedia contents such as JPEG, GIF and ZIP/RAR/7ZIP/TNEF archives to prevent advanced Malware and Zero-day attacks.	Please change the clause to "The proposed solution should have the ability to analyze, detect and block malware in common file formats including but not limited to executables, JAVA, PDF, MS Office documents, common multimedia contents such as JPEG/GIF/BMP/WMF and ZIP/RAR/7ZIP/TNEF archives to prevent advanced Malware and Zero-day attacks. "	no change to the tender condition
213	Section V	4	The bidder needs to supply, install and configure the UTM at Railtel offices at the following locations	Please change the clause "The bidder needs to supply, install and configure the UTM/NGFW at Railtel offices at the following locations"	no change to the tender condition
214	Section V	4	The appliance should combine firewall, application control, IP Sec and SSL VPN, intrusion prevention, antivirus, antimalware, anti-spam and web filtering into a single device.	Please change the clause "The appliance should combine firewall, application control, IP Sec and SSL VPN, intrusion prevention, antivirus / antimalware, anti-spam / web filtering into a single device"	may kindly refer the corrigendum-II
215	Section V	4	The system should support IPSEC VPN, PPTP VPN, L2TP VPN and SSL VPN.	Please change the clause to "The system should support IPSEC VPN and SSL VPN. "	may kindly refer the corrigendum-II
216	Section V	4	The proposed solution should support Virtualization (Virtual Firewall, Security zones and VLAN).	Please change the clause to "The proposed solution should support Virtualization (Security zones and VLAN). "	may kindly refer the corrigendum-II
217	Section V	4	Administrator shall be able to define sensitive data patterns, and data matching these patterns that will be blocked and/or logged when passing through the unit.	Please remove this clause	may kindly refer the corrigendum-II
218	Section V	4	Solution should be able to inspect https traffic on the fly for infected file using its own Anti-virus (AV) engine. It should be able to notify users if the traffic is blocked due to upload of infected file	Please change the clause to "Solution should be able to inspect https traffic on the fly for infected file using its own Anti-virus (AV) / Anti-Malware engine."	may kindly refer the corrigendum-II
219	Section V	4	Anti-virus scanning should support file based and stream mode Anti virus detection.	Please change the clase to " Anti-virus scanning should support file based and stream mode Anti virus detection or using Anti-APT"	may kindly refer the corrigendum-II
220	Section V	4	Solution should give information related to Perfomance impact and confidence level of protections while creating profiles.	Please remove this clause	may kindly refer the corrigendum-II
221	Section V	4	New Clause	Firewall OEM should be in Leader / Challenger Quadrant of Gartner's Enterprise Firewall / UTM	may kindly refer the corrigendum-II
222	Section V	4	The bidder needs to supply, install and configure the solution at Railtel Data cenre(s) at the following locations	Please clarify whether this solution is requieed for protecting inbound DNS request from Internet or Outbound DNS request going to internet from Railnet network	Both Inbound and Outbound
223	Section V	4	The offered product shall support secure remote login using SSH	Please confirm if cloud based solution is permitted, if the requirement is to protect outbound DNS request to internet	Cloud Based solution are not permitted
224	Section V	4	Should support DNSSEC	Please change the clause to "Should support DNSSEC /DNSCrypt"	no change to the tender condition
225	Section V	4	DNS DDoS threshold alerting	Please remove this clause	no change to the tender condition
226	Section V	4	Shall have SNMP support v2 and v3 (for sending alerts in case of some failures).	Please change clauseto " Shall have SNMP support v2 and v3 (for sending alerts in case of some failures). or logs"	no change to the tender condition
227	Section V	4	Shall support for external RADIUS, & LDAP and TACACS integration for administrator authentication.	Please remove this clause	no change to the tender condition
228	Section V	4	SOW for connectivity towards Railtel's multiple networks like MPLS backbone, NLD, CGNAT, Data centre infrstructure etc.	DC Switches, Routers may be required as a network Data Centre infrastructure equipments. Whether Bidder should add or provision for such equipments or may be part of Railtel's scope, please clarify	may kindly refer the tender document
229	Section II	26.5.3 - 9	The OEM must have direct presence in India with at least ten (10) no's of technical manpower direct support in India for the offered technology. An undertaking from the OEM for the requisite number of technical manpower for direct support in India.	Please remove this clause of direct presence in India.	no change to the tender condition

230	Annexure -1, Technical Specifications;	SSL Device	system must support bulk encryption of 4 Gbps	System must support bulk encryption of 8 Gbps	no change to the tender condition
231	Annexure -1, Technical Specifications;	SSL Device	System must have Minimum 2 x10G SFP+ Ports (fully populated) and options for min. 2 SFP+ for 10G connectivity	System must have Minimum 4 x10G SFP+ Ports (fully populated) and 4 x 1 G ports	no change to the tender condition
232	Annexure -1, Technical Specifications;	SSL Device	System must support at least 30 Application Delivery partitioning / Virtual context, dedicated configuration file, routes for each customer's traffic, where in resources can be either dedicated to each partition or can leverage common pool of resources i.e. CPU and Memory, concurrent connection for each context should be configurable	System must support at least 64 Application Delivery partitioning / Virtual context, dedicated configuration file, routes for each customer's traffic, where in resources can be either dedicated to each partition or can leverage common pool of resources for each context should be configurable	no change to the tender condition
233	Annexure -1, Technical Specifications;	SSL Device	New Clause	System must support inerception of outbound SSL traffic using RootCA/SubCA internal certificates	no change to the tender condition
234	Annexure -1, Technical Specifications;	SSL Device	Device should support day 1 Layer 7 throughput of atleast 10 Gbps	Device should support day 1 Throughput of atleast 10 Gbps	no change to the tender condition
235	Annexure -1, Technical Specifications;	SSL Device	System should support different protocol parsers such as HTTP, SSL, DNS, FTP,TFTP, SIP, SMTP, SPDY, RTSP, RADIUS,	All major browsers are already supporting HTTP2.0, So we request you to please ammend this clause involve industry standard parser only. **Suggested Clause:-** System should support different protocol parsers such as HTTP, SSL, DNS, FTP,TFTP, RADIUS, SIP, SMTP, RTSP XML	no change to the tender condition
236	Annexure -1, Technical Specifications;	SSL Device	System should support Hashing Algorithms like MD5, SHA-1, SHA-2, SHA256, SHA384 , SHA3	We request you to please refer the industry standard hashing algorithm and dilute the clause. **Suggested Clause:-** System should support Hashing Algorithms like MD5, SHA-1, SHA256, SHA384	no change to the tender condition
237	Annexure -1, Technical Specifications;	SSL Device	System must support at least 30 Application Delivery partitioning / Virtual context, dedicated configuration file, routes for each customer's traffic, where in resources can be either dedicated to each partition or can leverage common pool of resources i.e. CPU and Memmory, concurrent connection for each context should be configurable	Different OEM's have their own architectures, We request to please dilute the clause and mention concurrent connections/Connections per second for each context. **Suggested Clause:-** System must support at least 30 Application Delivery partitioning / Virtual context, dedicated configuration file, routes for each customer's traffic, where in resources can be either dedicated to each partition or can leverage common pool of resources i.e. CPU and Memory, Connections per second/Connections per second for each context should be configurable	no change to the tender condition
238	Annexure -1, Technical Specifications;	SSL Device		OEM should be present in Gartner's LEADER magic quadrant in the latest report (2016/2017) for ADC and should have OEM TAC based in INDIA.	no change to the tender condition
239	Annexure -1, Technical Specifications;	Web Application Firewall	WAF should support inline bridge or proxy mode of deployment.	We request to mention the standard Mode of deployements. **Suggested Clause:-** WAF should support inline/proxy/Out-Of-path mode of deployment.	no change to the tender condition
240	Annexure -1, Technical Specifications;	Web Application Firewall	The WAF database should include a preconfigured comprehensive and accurate list of attack signatures.	WAF works on the combination of negative and positive security models. We suggest you to please dilute this clause. **Suggested Clause:-** The WAF should support an auto-attack signatures and geo-location data update service	no change to the tender condition

241	Annexure -1, Technical Specifications;	Web Application Firewall	The WAF should have the ability to perform behavioral learning to examine traffic and highlight anomalies and provide recommendations that can be turned into actions such as apply, change and apply, ignore etc. The WAF should allows the administrator to define the rules and patterns to apply to a specific page in a Web Application.	Different OEM's does have their own method to examine and highlight anamolies. Please dilute the clause. **Suggested Clause:-** The WAF should allows the administrator to define the rules and patterns to apply to a specific page in a Web Application	no change to the tender condition
242	Annexure -1, Technical Specifications;	Web Application Firewall	The solution must support the web application vulnerability assessment tools (Web application scanners in Leaders of Latest Gartner Magic Quadrant Application Security Testing) to virtually patch web application vulnerabilities.	**Suggested Clause:-** The solution must support the web application vulnerability assessment tools to virtually patch web application vulnerabilities.	no change to the tender condition
243	Annexure -1, Technical Specifications;	Web Application Firewall	The solution must be a Leader or Challenger in the Gartner Magic Quadrant of Web Application Firewalls 2016/2017	**Suggested Clause:-** The WAF solution must be ICSA certified. WAF may be proposed part of ADC solution (ADC OEM must be present in Gartner Leader's quadrant in the latest report published).	no change to the tender condition
244	Annexure -1, Technical Specifications;	Web Application Firewall	System must have minimum(fully populated) 2 x10G SFP/SFP+ Ports and option of min. 2 SFP/SFP+ for 10G connectivity (field upgradable on same hardware)	**Suggested Clause:-** System must have minimum(fully populated) 2 x10G SFP/SFP+ Ports	no change to the tender condition
245	Annexure -1, Technical Specifications;	IPS	The IPS should be a dedicated purpose built hardware, not a part of Router, Firewall module and UTM solution with Real World Throughput 6 Gbps or better	With Scalability high performance in terms of throughput can be achieved on the same hardware. **Suggested Clause:-** The IPS should be a dedicated purpose built hardware, not a part of Router, Firewall module and UTM solution with Real World Throughput 4 Gbps scalable upto 12 Gbps.	no change to the tender condition
246	Annexure -1, Technical Specifications;	IPS	New Clause	**Bandwidth Management:** a) Policies should be defined to restrict or maintain the bandwidth that can be sent or received by each application, user, or segment. b) Guarantee bandwidth for each critical application or limit non-critical traffic such as P2P. c) Set rules to block or allow specific traffic types.	no change to the tender condition
247	Annexure -1, Technical Specifications;	IPS	New Clause	**Zero Day Attack Protection:** The proposed device should support Automatic Real-time Signatures creation (no manual intervention) based on Rate Variant/Invariant, Challenge – Response Mechanism, and which should be able to Detect and protect attacks in less than a minute. The proposed solution should NOT be based on RATE LIMITING technology for detecting Zero Day attacks. It should be able to detect & mitigate zero day DDoS attacks, based on behavioural DoS detection & mitigation automatically (without human intervention). The proposed solution should support DoS Flood Rate prevention rate upto 10 Mpps (Internal/External).	no change to the tender condition

248	Section II	26.5 Eligibility Criteria	d) The OEM (s) should be an established industry player in its respective domain like security, network, storage etc. and should form a part of the Industry standard leader's/challenger's quadrant on the likes of Gartner, Forrester, IDC etc.	We understand that annexure to the RFP has been released and the annexure's OEM eligibility criteria superceeds the RFP OEM eligibilty citeria. Please confirm	Yes, if specified in the Annexure -1 : Technical Specification.
249	Annexure -1, Technical Specifications;	10. Intrusion Prevention System (IPS)	The IPS should employ full seven-layer protocol analysis of over maximum internet protocols and data file format.	For superior security effectiveness of an NIPS appliance, it is highly recommended that the NIPS technology understands and analyze high numbers of Protocols and FileFormats. Please rephrase the sprcification as "The IPS should employ full seven-layer protocol analysis of 450+ internet protocols and data file format."	no change to the tender condition
250	Annexure -1, Technical Specifications;	10. Intrusion Prevention System (IPS)	The IPS capability should have NSS / ICSA or other equivalent Certification.	IBM reccomends that NIPS solution should not just be recommended by NSS but has high security effectiveness of more than 99% rating. Requesting to rephrase the specification as "The IPS capability should have NSS / ICSA or other equivalent Certification with a score of 99% and above"	no change to the tender condition
251	Annexure -1, Technical Specifications;	10. Intrusion Prevention System (IPS)	The IPS should be capable of detecting and blocking zero-day attacks without requiring an update.	Zero day protection is very critical with new and dangerous attacks. It is recommended to show proofs for NIPS showcasing Ahead of Threat (Zero Day Coverage) instances. It is recommended to rephrase the specificationas "The IPS should be capable of detecting and blocking zero-day attacks without requiring an update. Provide refrenses and proofs for Ahead of Threat Detection"	no change to the tender condition
252	Annexure -1, Technical Specifications;	10. Intrusion Prevention System (IPS)	The solution appliance should have at least 4 x 10G SFP+/XFP ports (fully populated) from day one	Please change the specification to mention SR or LR connector type.	may kindly refer the corrigendum-II
253	Section V	Point 3 3 Schedule of Requirements	The Tenderer should ensure there is a 24 x 7 x 365 comprehensive onsite support arrangement for a period of 5 years (breakup as of 3years plus 2 years) with all the OEM for respective components.	Are you looking at a onsite support engineer/resource for 5 years (3+2 yrs) for 24*7 and 365 days from the OEM or from the Bidder?	may kindly refer the tender document
254	Section V	6.7 Training – Information Security	The Tenderer should also provide OEM technical training on all equipment to officials as designated by RAILTEL.	Are you looking for Training from OEM directly. If yes, for how many days, for hoe many people and for what all locations in India?	may kindly refer the tender document
255	Section V	6.2 Onsite support	The Tenderer along with all the associated OEMs should commit to provide all necessary resources and expertise to resolve any issues and carry out required changes, optimizations and modification to ensure that the ICT infrastructure is operational in accordance with the stipulated service standards in Section VII – Service Level Agreement.	Are you expecting the OEM to also sign the SLA document otr will the SLA document will be signed between RAILTEL & the bidder?	Tender conditions are clear
256	Annexure -1, Technical Specifications;	10. Intrusion Prevention System (IPS)	Comprehensive onsite hardware warranty for 3 years with Next business Day (NBD) resolution.	Please clarify by NBD resolution, (1) responding to a SR by next business day over email/phone (2) suggesting a resolution next step by the OEM TAC by Next Business day, while resolution may itself take more number of days (3) replacement of a RMA by NBD.	As per industry standard
257	Annexure-1 Technical specifications	Next Generation Firewall	The solution should be Hardware based and enterprise class (complete control from GUI as well as CLI)	Please change the clause "The solution should be Hardware based and enterprise class	No change to the tender condition

258	Annexure-1 Technical specifications	Next Generation Firewall	Firewall should provide at least 20 Gbps of real world/ production envoirnment throughput	Please change the clause to "Firewall should provide at least 20 Gbps of NGFW real world/ production envoirnment throughput"	No change to the tender condition
259	Annexure-1 Technical specifications	Next Generation Firewall	Firewall should support 180,000 new sessions per second	Please change the clause "Firewall should support 120,000 new sessions per second"	No change to the tender condition
260	Annexure-1 Technical specifications	Next Generation Firewall	Rack Mountable not exceeding 2U with redundant/dual AC power supply fully populated (within box) from day one	Please change the clause to "Rack Mountable not exceeding 1U with redundant/dual AC power supply fully populated (within box) from day one"	No change to the tender condition
261	Annexure-1 Technical specifications	Next Generation Firewall	The proposed system should have integrated Traffic Shaping functionality.	Please change the clause to "The proposed system should have integrated Traffic Shaping functionality / Rate limiting user/application basis"	may kindly refer the corrigendum-II
262	Annexure-1 Technical specifications	Next Generation Firewall	Support at least 10 firewall domains/instants/virtual context	Please remove this clause	may kindly refer the corrigendum-II
263	Annexure-1 Technical specifications	Next Generation Firewall	Should facilitate to apply policy like Traffic shaping & policy based routing decision	Please change the clause to "Should facilitate to apply policy like Traffic shaping / Rate Limiting & policy based routing decision"	may kindly refer the corrigendum-II
264	Annexure-1 Technical specifications	Next Generation Firewall	User authentication facilitated by services like LDAP and RADIUS.	Please change the clause to "User authentication facilitated by services like LDAP and RADIUS/AD"	No change to the tender condition
265	Annexure-1 Technical specifications	Next Generation Firewall	The appliance based security platform should be capable of providing firewall and VPN (both IPSec and SSL) functionality in a single appliance	Please remove this clause	No change to the tender condition
266	Annexure-1 Technical specifications	Next Generation Firewall	Firewall should support client based and clientless SSL vpn peers from day one.	Please remove this clause	may kindly refer the corrigendum-II
267	Annexure-1 Technical specifications	Next Generation Firewall	IPS throughput should be atleast 3 Gbps or better for real world/production throughput	Please change the clause to "Firewall should provide at least 20 Gbps of NGFW (FW, AVC and IPS) real world/ production envoirnment throughput"	No change to the tender condition
268	Annexure-1 Technical specifications	Next Generation Firewall	The IPS system should have at least 7,000 signatures with support for custom IPS signatures	Please change the clause to "The IPS system should have at least 20,000 signatures with support for custom IPS signatures"	No change to the tender condition
269	Annexure-1 Technical specifications	Next Generation Firewall	The proposed solution shall be able to support various form of user Authentication methods simultaneously , including: a) Local Database entries b) LDAP server entries c) RADIUS server entries d) Native Windows AD (Single sign on capability)	Please change the clause to: The proposed solution shall be able to support various form of user Authentication methods simultaneously , including: Local Database entries / LDAP server entries / RADIUS server entries / Native Windows AD (Single sign on capability)	may kindly refer the corrigendum-II
270	Annexure-1 Technical specifications	Intrusion Prevention System	The IPS should be a dedicated purpose built hardware, not a part of Router, Firewall module and UTM solution with Real World Throughput 6 Gbps or better	Please change it to "The IPS should be a dedicated purpose built hardware, not a part of Router, Firewall module and UTM solution with Real World Throughput 10 Gbps or better"	No change to the tender condition
271	Annexure-1 Technical specifications	Intrusion Prevention System	The IPS system should have at least 4,500 signatures with support for custom IPS signature	Please change the clause to "The IPS system should have at least 20,000 signatures with support for custom IPS signature"	No change to the tender condition

272	Annexure-1 Technical specifications	Intrusion Prevention System	IPS signatures should have a configurable actions like terminate a TCP session by issuing TCP Reset packets to each end of the connection, or silently drop traffic in addition to sending an alert and logging the incident	Please change the clause to "IPS signatures / Access Policy should have a configurable actions like terminate a TCP session by issuing TCP 44 Reset packets to each end of the connection, or silently drop traffic in addition to sending an alert and logging the incident"	may kindly refer the corrigendum-II
273	Annexure-1 Technical specifications	Advance Persistence Threat Solution	The solution should be able to communicate bi-directionally with the proposed UTM solution for automatic blocking.	Please remove this clause	may kindly refer the corrigendum-II
274	Annexure-1 Technical specifications	Advance Persistence Threat Solution	The proposed solution should perform dynamic real-time analysis of advanced malware on the appliance itself to confirm true zero-day and targeted attacks. No information should be sent to third party systems or cloud infrastructure system for analysis and detection of Malware.	Please change the clause to "The proposed solution should perform dynamic real-time analysis of advanced malware to confirm true zero-day and targeted attacks. No file should be sent to third party systems or cloud infrastructure system for analysis and detection of Malware. "	may kindly refer the corrigendum-II
275	Annexure-1 Technical specifications	Advance Persistence Threat Solution	The proposed solution should have the ability to analyze, detect and block malware in common file formats including but not limited to executables, JAVA, PDF, MS Office documents, common multimedia contents such as JPEG, GIF and ZIP/RAR/7ZIP/TNEF archives to prevent advanced Malware and Zero-day attacks.	Please change the clause to "The proposed solution should have the ability to analyze, detect and block malware in common file formats including but not limited to executables, JAVA, PDF, MS Office documents, common multimedia contents such as JPEG/GIF/BMP/WMF and ZIP/RAR/7ZIP/TNEF archives to prevent advanced Malware and Zero-day attacks. "	may kindly refer the corrigendum-II
276	Annexure-1 Technical specifications	Advance Persistence Threat Solution	The proposed solution should have the ability to scan and analyze emails to identify malicious attachments or URLs.	Please change the clause to "The proposed solution should have the ability to scan and analyze emails to identify malicious attachments or URLs."	may kindly refer the corrigendum-II
277	Annexure-1 Technical specifications	Advance Persistence Threat Solution	The proposed solution should be able to scan servers that support CIFS and NFS protocol for sharing and transferring files.	Please change the clause to "The proposed solution should support SMB / CIFS / NFS protocol for sharing and transferring files."	may kindly refer the corrigendum-II
278	Annexure-1 Technical specifications	Advance Persistence Threat Solution	The proposed solution should provide visibility into scan histories of each file scanned that are aborted, completed, or in progress.	Please remove this clause	may kindly refer the corrigendum-II
279	Annexure-1 Technical specifications	Advance Persistence Threat Solution	The proposed solution should be able to analyze saved email (.eml) files for malicious attachments	Please remove this clause	may kindly refer the corrigendum-II
280	Annexure-1 Technical specifications	Advance Persistence Threat Solution	It should support Sandbox Analysis for multiple operating systems like WinXP,Win7,Win8,Win10	Please change the clause to "It should support Sandbox Analysis for multiple operating systems like WinXP / Win7 / Win8 /Win10"	may kindly refer the corrigendum-II
281	Annexure-1 Technical specifications	Advance Persistence Threat Solution	The APT appliance should be able to process minimum of 1000 files/hour or 1,000,000 files/month (either web or mail or both) on the VM sandboxing	Please change the clause to "The APT appliance should be able to process minimum of 1000 files/hour or 1,00,000 files/month (either web or mail or both) on the VM sandboxing"	may kindly refer the corrigendum-II
282	Annexure-1 Technical specifications	Next Generation Firewall	the solution appliance should have at least 4 GE ports and 4 x 10G SFP+ ports with fully populated (SFP+ transceivers) from day one	the solution appliance should have at least 4 GE ports , 8 x 10G SFP+ ports, 2 x 40G QSFP+ with fully populated (SFP+ transceivers) from day one. 40 Gig interfaces are mandatory considering future requirements.	no change to the tender condition
283	Annexure-1 Technical specifications	Next Generation Firewall	The solution appliance must have separate SYNC and management ports other than the above mentioned ports	The solution should show real time details on the CPU usage for management activities and CPU usage for traffic processing activities.	no change to the tender condition
284	Annexure-1 Technical specifications	Next Generation Firewall	Firewall should provide at least 20 Gbps of real world/ production envoirnment throughput	Firewall should provide at least 8 Gbps of throughput with Firewall, Application visibility and control, IPS, Anti-Virus, Anti-spyware enabled (8 Gbps with all these features enabled).	no change to the tender condition
285	Annexure-1 Technical specifications	Next Generation Firewall	The solution appliance should have at least 16 GB RAM	The solution appliance should have at least 64 GB RAM	no change to the tender condition

286	Annexure-1 Technical specifications	Next Generation Firewall	Firewall should support 180,000 new sessions per second	Firewall should support 160,000 new sessions per second	no change to the tender condition
287	Annexure-1 Technical specifications	Next Generation Firewall	Firewall should support 10 Million concurrent sessions	Firewall should support 4 Million concurrent sessions	no change to the tender condition
288	Annexure-1 Technical specifications	Next Generation Firewall	Certified by ICSA 4.1x OR EAL4 OR NDPP	Certified by Gartner Leader/Challenger or ICSA 4.1x OR EAL4 OR NDPP	no change to the tender condition
289	Annexure-1 Technical specifications	Next Generation Firewall	User authentication facilitated by services like LDAP and RADIUS.	User authentication facilitated by services like LDAP and RADIUS. Solution should support policy based multi-factor authentication e.g. if any user attempts to access FTP server, user must be challenged with MFA every 3 hours.	may kindly refer the corrigendum-II
290	Annexure-1 Technical specifications	Next Generation Firewall	Management access control using Profile/Role based for granular control.	Management access control using Profile/Role based for granular control. The proposed solution must allow single policy rule creation for application control, user based control, host profile, threat prevention, Anti-virus, file filtering, content filtering, QoS and scheduling at single place within a single rule and not at multiple locations. There must not be different places and options to difine policy rules based on these parameters.	no change to the tender condition
291	Annexure-1 Technical specifications	Next Generation Firewall	NGFW should support SSL VPN throughput of atleast 3Gbps	NGFW should support IPSec VPN throughput of atleast 5 Gbps	no change to the tender condition
292	Annexure-1 Technical specifications	Next Generation Firewall	IPS throughput should be atleast 3 Gbps or better for real world/production throughput	IPS throughput should be atleast 8 Gbps or better	no change to the tender condition
293	Annexure-1 Technical specifications	Next Generation Firewall	The IPS should be able to inspect SSL sessions by decrypting the traffic	The IPS should be able to inspect SSL and SSH sessions by decrypting both inbound and the outbound traffic	no change to the tender condition
294	Annexure-1 Technical specifications	Next Generation Firewall	Signatures should have severity level defined to it so that the administrator can understand and decide which signatures to enable for what traffic (e.g. for severity level: high medium low)	Signatures should have severity level defined to it so that the administrator can understand and decide which signatures to enable for what traffic (e.g. for severity level: high medium low) . System should allow custom IPS policies based on Users and applications.	no change to the tender condition
295	Annexure-1 Technical specifications	Next Generation Firewall	System should have built-in high availability (HA) features without extra cost/license or hardware component from day one	System should have built-in high availability (HA) features without extra cost/license or hardware component from day one. System should support state synchronization for all features including IPS, AV, Anti-spyware.	no change to the tender condition
296	Annexure-1 Technical specifications	Anti APT	The solution should be able to communicate birectionally with the proposed UTM and NGFW solution for automatic blocking/threat update	The solution should be able to communicate birectionally with the proposed UTM NGFW solution for automatic blocking/threat update	may kindly refer the corrigendum-II
297	Annexure-1 Technical specifications	Anti APT	The proposed solution should be able to detect and prevent advanced Malware, Zero-day attack, spear phishing attack, drive by download, watering hole and targeted Advanced Persistent Threat without relying on just Signature database.	The proposed solution should be able to detect and prevent zero-day attacks and should provide payload based automated signature (not just hash based) within 5 mins of dynamic analysis.	no change to the tender condition
298	Annexure-1 Technical specifications	Anti APT	The proposed solution should utilize a state-full attack analysis to detect the entire infection lifecycle, and trace the stage-by-stage analysis of an advanced attack, from system exploitation to outbound malware communication protocols leading to data exfiltration.	The solution should support protection against anti-VM evasion techniques that include sleep calls, enumerating for processes and debuggers, simulating user environments (key clicks, mouse clicks, mouse movement, etc.), detection of malware attempting to determine what port the VM process is connected to, determining if the VM is running in a single processer versus a multi-core processors, etc.	no change to the tender condition

299	Annexure-1 Technical specifications	Anti APT	The proposed solution should analyze advanced malware against a cross-matrix of different operating systems and various versions of pre-defined applications.	The proposed solution should analyze advanced malware against a cross-matrix of different operating systems and various versions of pre-defined applications. The solution must support minimum four level of decompression/decoding for any combination of decoding: ZIP, gzip, base64,chunked, uuencode. The solution must provide the ability to block files with multi-level-encoding with 5 or more level of compression e.g office file in 5 levels of zip.	no change to the tender condition
300	Annexure-1 Technical specifications	Anti APT	The proposed solution should have the ability to analyze, detect and block malware in common file formats including but not limited to executables, JAVA, PDF, MS Office documents (doc, docx, xls etc), common multimedia contents like JPEG, GIF and ZIP/RAR/7ZIP/TNEF archives, to prevent advanced Malware and Zero-day attacks.	The proposed solution should support enhanced File type support: .exe, .dll, .scr, .ocx, .sys, .drv, Adobe (.pdf), Microsoft Office Documents (.doc, .docx., .xls, .xlsx, .ppt, and .pptx), Non-Microsoft document types (.rtf), Java (.jar and class files), Adobe Flash .swf	may kindly refer the corrigendum-II
301	Annexure-1 Technical specifications	Anti APT	The proposed solution should have the ability to be deployed in out-of-band mode (also SPAN/TAP) & inline mode	The proposed solution should have the ability to be deployed in out-of-band mode and should integrate with the NGFW over secure channel.	no change to the tender condition
302	Annexure-1 Technical specifications	Anti APT	The solution should have anti-evasion capabilities to prevent malwares detection of being run/executed in the vitualized environment.	The solution should support protection against anti-VM evasion techniques that include sleep calls, enumerating for processes and debuggers, simulating user environments (key clicks, mouse clicks, mouse movement, etc.), detection of malware attempting to determine what port the VM process is connected to, determining if the VM is running in a single processer versus a multi-core processors, etc.	no change to the tender condition
303	Annexure-1 Technical specifications	Anti APT	The proposed solution should be able to analyze saved email (.eml) files for malicious attachments.	The proposed solution should be able to analyze emal attachments and malicious links for static and dynamic analysis.	may kindly refer the corrigendum-II
304	Annexure-1 Technical specifications	Anti APT	Minimum number of Interfaces - 2x GE & 2 x 10G	Minimum number of Interfaces - 4x 10/100/1000.	no change to the tender condition
305	Annexure-1 Technical specifications	Anti APT	Number of VM's should be atleast 24	Number of VM's should be atleast 36	no change to the tender condition
306	Annexure-1 Technical specifications	Anti APT	It should support Sandbox Analysis for multiple operating systems like WinXP,Win7,Win8,Win10	It should support Sandbox Analysis for multiple operating systems like WinXP,Win7,Android etc.	no change to the tender condition
307	Annexure-1 Technical specifications	Anti APT	The APT appliance should be able to process minimum of 1000 files/hour or 1,000,000 files/month (either web or mail or both) on the VM sandboxing	The licensing of the solution must not be based on number of files/samples submitted to the on-premise APT solution.	may kindly refer the corrigendum-II
308	Annexure-1 Technical specifications	Anti APT	Proposed solution must have secured at least 95% security effective-ness in latest NSS Breach Detection System Report	Proposed solution should be in the Leader's quadrant of 2016 Forrester's Automated malware analysis report.	no change to the tender condition
309	Section II	clause 9	The OEM must have direct presence in India with at least ten (10) no's of technical manpower direct support in India for the offered technology.	The OEM must have direct presence in India.	no change to the tender condition