Annexure-A

S. No.	Tender Page No.	Tender Clause Reference	Tender Clause	Bidder's Clarification Sought	ERNET India Response
1	24	8.4 Earnest Money Deposit (EMD):	Earnest Money Deposit (EMD): The bidder is requested to provide an Earnest Money Deposit (EMD) of a sum equivalent to INR 15,00,00,000/- (Rupees Fifteen Crore Only) as a demonstration of their serious intent and commitment to participate in this tender process. The EMD shall be as prescribed in NIT clause no 2.3	CPSUs are exempted from EMD in GeM portal. Kindly confirm. Note: As a result there is no provision to upload the EMD douments in the GeM portal for the exempted Bidders.	Kindly refer to respective updated clause in Annexure-B
2	55	9.5 Extension of Delivery Period and Liquidated Damages: 2) Liquidated Damages (LD):	Note: Overall Liquidated Damages shall be restricted to 10% of the total contract value.	Note: Overall Liquidated Damages shall be restricted to 10% of the undelivered value.	Kindly refer to respective updated clause in Annexure-B
3	73	Minimum Qualification, Relevant Experience & Certifications at DC/DR & Shastri Park, Delhi	**1. Cyber security expert** B.E./B.Tech/MCA/M.Tech# with 10 Years relevant experience in IT/ITeS + CISA/CISSP/CISM # Refers to - Desirable M.Tech in Cyber Security	Clause to be modified as "required professionals will be outsourced through OEM / implementation partner" or "Employees will be appointed as fixed term/contractual basis, post award of the contract. Accordingly, undertaking will be submitted as part of the bid submission by the bidder.	No Change
4	73	Minimum Qualification, Relevant Experience & Certifications at DC/DR & Shastri Park, Delhi	**2. Data center IT networking & architecture expert** B.E./B.Tech/MCA with 10 Years relevant experience in IT/ITeS + CCIE-ENT	Clause to be modified as "required professionals will be outsourced through OEM / implementation partner" or "Employees will be appointed as fixed term/contractual basis, post award of the contract. Accordingly, undertaking will be submitted as part of the bid submission by the bidder.	The clause may be read as : **Data center IT networking & architecture expert** B.E./B.Tech/MCA with 10 Years relevant experience in IT/ITeS + CCNP-DC/JNCIP-DC
5	73	Minimum Qualification, Relevant Experience & Certifications at DC/DR & Shastri Park, Delhi	**3. Remote Site Engineer** B.E./B.Tech/MCA in Computer/IT / Electronics + 4 Years relevant experience in Network Management + OEM certified engineer on proposed networking equipment Such as JNCIA, CCNA or equivalent.	Clause to be modified as "required professionals will be outsourced through OEM / implementation partner" or "Employees will be appointed as fixed term/contractual basis, post award of the contract. Accordingly, undertaking will be submitted as part of the bid submission by the bidder.	No Change
6	73	Minimum Qualification, Relevant Experience & Certifications at DC/DR & Shastri Park, Delhi	**4. Project Manager** B.E./B.Tech/MCA 8 Years relevant experience in IT/ITeS (minimum 6 years' experience for managing large data centers) + CCNP-DC/ JNCIP-DC or equivalent Certified. In case of Existing DC, DR- Project Manager should have preferably JNCIP-DC.	Clause to be modified as "required professionals will be outsourced through OEM / implementation partner" or "Employees will be appointed as fixed term/contractual basis, post award of the contract. Accordingly, undertaking will be submitted as part of the bid submission by the bidder.	No Change
7	73	Minimum Qualification, Relevant Experience & Certifications at DC/DR & Shastri Park, Delhi	**5. Security Specialist** B.E./B.Tech/MCA in Computer/IT / Electronics + 8 Years relevant experience in IT Network Management + Certification: OEM certified engineer on proposed security equipment Such as JNCIP- SEC, Fortigate NSE 4, PCNSE, CCNP Security or equivalent. In case of Existing DC, DR- Security specialist should have preferably JNCIP-SEC.	Clause to be modified as "required professionals will be outsourced through OEM / implementation partner" or "Employees will be appointed as fixed term/contractual basis, post award of the contract. Accordingly, undertaking will be submitted as part of the bid submission by the bidder.	No Change

8	73	Minimum Qualification, Relevant Experience & Certifications at DC/DR & Shastri Park, Delhi	**6. OEM Security Specialist** B.E./B.Tech/MCA in Computer/IT / Electronics + 5 Years relevant experience in IT Network Management + Certification: OEM certified engineer on proposed security equipment Such as JNCIP- SEC, Fortigate NSE 4, PCNSE, CCNP Security or equivalent.	Clause to be modified as "required professionals will be outsourced through OEM / implementation partner" or "Employees will be appointed as fixed term/contractual basis, post award of the contract. Accordingly, undertaking will be submitted as part of the bid submission by the bidder.	No Change
9	74	Minimum Qualification, Relevant Experience & Certifications at DC/DR & Shastri Park, Delhi	**7. OEM Network Specialist** B.E./B.Tech/MCA in Computer/IT / Electronics + Atleast 5 Years relevant experience in IT Network Management + OEM certified engineer on proposed networking equipment Such as JNCIP, CCNP or equivalent. Must have 5 years of work experience on leaf and spine architecture.	Clause to be modified as "required professionals will be outsourced through OEM / implementation partner" or "Employees will be appointed as fixed term/contractual basis, post award of the contract. Accordingly, undertaking will be submitted as part of the bid submission by the bidder.	No Change
10	74	Minimum Qualification, Relevant Experience & Certifications at DC/DR & Shastri Park, Delhi	**8. Network Specialist** B.E./B.Tech/MCA in Computer/IT / Electronics + Atleast 8 Years relevant experience in IT Network Management + OEM certified engineer on proposed networking equipment Such as JNCIP, CCNP or equivalent. Must have 5 years of work experience on leaf and spine architecture In case of Existing DC, DR- Network specialist should have preferably JNCIP-ENT.	Clause to be modified as "required professionals will be outsourced through OEM / implementation partner" or "Employees will be appointed as fixed term/contractual basis, post award of the contract. Accordingly, undertaking will be submitted as part of the bid submission by the bidder.	No Change
11	74	Minimum Qualification, Relevant Experience & Certifications at DC/DR & Shastri Park, Delhi	**9. Network Engineer** B.E./B.Tech/MCA in Computer/IT / Electronics + Atleast 4 Years relevant experience in Network Management + OEM certified engineer on proposed networking equipment Such as JNCIP, CCNP or equivalent. In case of Existing DC, DR- Network engineer should have preferably, JNCIP-ENT.	Clause to be modified as "required professionals will be outsourced through OEM / implementation partner" or "Employees will be appointed as fixed term/contractual basis, post award of the contract. Accordingly, undertaking will be submitted as part of the bid submission by the bidder.	No Change
12	75	Minimum Qualification, Relevant Experience & Certifications at DC/DR & Shastri Park, Delhi	**10. Server Maintainance Specialist** At least One Server Maintainance Specialist should have Linux/RedHat Administrator/LFCS at each data center.	Clause to be modified as "required professionals will be outsourced through OEM / implementation partner" or "Employees will be appointed as fixed term/contractual basis, post award of the contract. Accordingly, undertaking will be submitted as part of the bid submission by the bidder.	No Change

13	84	A. Bidder’s Qualification Criteria	7. The bidder must have following professional* working on its payroll: a. Prince-2/ PMP - 5 numbers b. CISA/CISSP/CISM - 2 numbers c. CDCP - 2 numbers d. CCIE-Sec/JNCIE-Sec - 1 numbers e. CCIE-ENT/JNCIE-ENT - 1 numbers f. CCIE-DC/CCNP-DC/JNCIE-DC/JNCIP-DC - 2 numbers g. CCNP-Sec/ JNCIP-Sec/Fortigate NSE-4/PCNSE - 3 numbers h. CCNP-ENT/ JNCIP-ENT - 3 numbers *Professionals must be regular employee of bidder as on date of submission of this bid. Fixed term contract/contractual employee will not be accepted. Valid certificate(s) of above professional to be submitted along with the bid with covering letter of Director HR of bidder’s organisation.		Kindly refer to respective updated clause in Annexure-B
14	85	A. Bidder’s Qualification Criteria	8. The bidder on the date of publishing of this bid; should already have in-house capabilities to discharge the roles & responsibilities as a System Integrator. Therefore, the bidder is not allowed to float any EoI or Tender against this Tender requirement for identifying any system integrator, consultant, empanelment, sub-contractor or a partner or a teaming partner etc by whatever name called; for discharging/sharing its responsibilities as a System Integrator. Further, it may also be noted that consortium, arrangements, joint-ventures, teaming, subletting, sub-contracting is strictly prohibited in this bid. In case, at any stage of the project, if its identified that any kind of above mentioned prohibitions were violated, ERNET India reserves the right to take suitable actions such as mentioned in Section III Clause 12. The bidder needs to submit an undertaking in this regard.	Kindly allow for subcontracting or subletting of passive activities like cabling, racking, stacking, civil or electrical works etc.	No Change
15	173	Form 12 financial BoQ, PART -C (Opex)	As per bid format, bidder has to quote for existing DC & DR O&M charges except manpower cost	Bid is evaluated on L1 price. This clause is giving an undue advantage to existing MSI because of this clause. Hence, we request not consider the value of O&M charges of existing DC & DR scope for evaluation of L1 price.	No Change

16	55	2) Liquidated Damages (LD	2) Liquidated Damages (LD): a. If the Contractor fails to meet the prescribed timelines for respective milestones due to any reason whatsoever then in such a case ERNET India would be entitled to impose the Liquidated Damages for the delay: i. Delay in Delivery of the Equipments (only for DC & DR): @ 0.5 % of the value of delayed equipments (of the respective milestones); per week or part of the week of delayed period. ii. Delay in Commissioning & offering for acceptance (for DC, DR & Remote Sites): @ 0.5 % of the sum total value of all the equipments for respective milestone; per week or part of the week of delayed period. Note: Overall Liquidated Damages shall be restricted to 10% of the total contract value. While calculating LD; GST will be excluded from the value on which LD is calculated; thereafter GST may be charged (if applicable) on the LD value as per S.No. 4 clause 5.3 of Section II of this document. In case, delay beyond 20 weeks, ERNET India may initiate termination for default and take remedial action(s) accordingly as per GCC Clause 12.1	**Request revision of this clause:** 2) Liquidated Damages (LD): a. If the Contractor fails to meet the prescribed timelines for respective milestones due to any reason whatsoever then in such a case ERNET India would be entitled to impose the Liquidated Damages for the delay: i. Delay in Delivery of the Equipments (only for DC & DR): @ **0.2%** ~~0.5 %~~ of the value of delayed equipments (of the respective milestones); per week or part of the week of delayed period. ii. Delay in Commissioning & offering for acceptance (for DC, DR & Remote Sites): @ **0.2%** ~~0.5 %~~ of the sum total value of all the equipments for respective milestone; per week or part of the week of delayed period. Note: Overall Liquidated Damages shall be restricted to **5%** ~~10%~~ of the total contract value. While calculating LD; GST will be excluded from the value on which LD is calculated; thereafter GST may be charged (if applicable) on the LD value as per S.No. 4 clause 5.3 of Section II of this document. In case, delay beyond 20 weeks, ERNET India may initiate termination for default and take remedial action(s) accordingly as per GCC Clause 12.1	Kindly refer to respective updated clause in Annexure-B
17	60	12.1.4 Contractual Remedies for Breaches/Defaults or Termination for Default	6) Risk and Cost Procurement: In addition to termination for default, the ERNET India shall be entitled, and it shall be lawful on its part, to procure Equipment and servicessimilar to those terminated, with such terms and conditions and in such manner as it deems fit at the "Risk and Cost" of the contractor. Such 'Risk and Cost Procurement' will be contracted within nine months from the breach of Contract. The Contractor shall be liable for any loss which the ERNET India may sustain on that account provided the procurement, or, if there is an agreement to procure, such agreement is made. The Contractor shall not be entitled to any gain on such procurement, and the manner and method of such procurement shall be in the entire discretion of the ERNET India. It shall not be necessary for the ERNET India to notify the contractor of such procurement. It shall, however, be at the discretion of the ERNET India to collect or not the security deposit from the firm/ firms on whom the contract is placed at the risk and cost of the defaulted firm.	**Request deletion of this entire clause:** ~~6) Risk and Cost Procurement: In addition to termination for default, the ERNET India shall be entitled, and it shall be lawful on its part, to procure Equipment and servicessimilar to those terminated, with such terms and conditions and in such manner as it deems fit at the "Risk and Cost" of the contractor. Such 'Risk and Cost Procurement' will be contracted within nine months from the breach of Contract. The Contractor shall be liable for any loss which the ERNET India may sustain on that account provided the procurement, or, if there is an agreement to procure, such agreement is made. The Contractor shall not be entitled to any gain on such procurement, and the manner and method of such procurement shall be in the entire discretion of the ERNET India. It shall not be necessary for the ERNET India to notify the contractor of such procurement. It shall, however, be at the discretion of the ERNET India to collect or not the security deposit from the firm/ firms on whom the contract is placed at the risk and cost of the defaulted firm.~~ Or Request ERNET to cap the risk purchase to maximum increment of 5% of the undelivered value.	No Change

18	61	12.1.5 Limitation of Liability	12.1.5 Limitation of Liability Except in cases of criminal negligence or wilful misconduct, the aggregate liability of the contractor to the ERNET India, whether under the contract, in tort or otherwise, shall not exceed the total Contract value, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment, or to any obligation of the contractor to indemnify the ERNET India concerning IPR infringement	**Request revision of this clause:** 12.1.5 Limitation of Liability Except in cases of criminal negligence or wilful misconduct, the aggregate liability of the contractor to the ERNET India, whether under the contract, in tort or otherwise, shall not exceed the total Contract value, provided that this limitation shall not apply ~~to the cost of repairing or replacing defective equipment, or~~ to any obligation of the contractor to indemnify the ERNET India concerning IPR infringement. And request addtion of the below clause: **Notwithstanding anything mentioned in this Agreement/ RFP contractor shall not be liable for lost profits or other financial loss of any type or description including any special, incidental, indirect or consequential damages, whether or not contractor has been advised of the possibility of such damages.**	No Change
19		12.2.1 Notice for Determination of Contract	12.2.1 Notice for Determination of Contract 1) The ERNET India reserves the right to terminate the contract, in whole or in part for its (the ERNET India's) convenience, by serving written 'Notice for Determination of Contract' on the contractor by giving sixty (60) days prior notice during the currency of the contract. The notice shall specify that the termination is for the convenience of the ERNET India of the contract. The notice shall also indicate inter-alia, the extent to which the contractor's performance under the contract is terminated, and the date with effect from which such termination shall become effective. 2) Such termination shall not prejudice or affect the rights and remedies accrued and/ or shall accrue after that to the Parties. 3) Unless otherwise instructed by the ERNET India, the contractor shall continue to perform the contract to the extent not terminated. 4) All warranty obligations, shall continue to survive despite the termination	**Request deletion of this clause:** ~~12.2.1 Notice for Determination of Contract~~ ~~1) The ERNET India reserves the right to terminate the contract, in whole or in part for its (the ERNET India's) convenience, by serving written 'Notice for Determination of Contract' on the contractor by giving sixty (60) days prior notice during the currency of the contract. The notice shall specify that the termination is for the convenience of the ERNET India of the contract. The notice shall also indicate inter-alia, the extent to which the contractor's performance under the contract is terminated, and the date with effect from which such termination shall become effective.~~ ~~2) Such termination shall not prejudice or affect the rights and remedies accrued and/ or shall accrue after that to the Parties.~~ ~~3) Unless otherwise instructed by the ERNET India, the contractor shall continue to perform the contract to the extent not terminated.~~ ~~4) All warranty obligations, shall continue to survive despite the termination~~	No Change
20	127	Section VIII: Service Level Agreement during Operation & Maintenance	- The overall Penalties (for Clause 1-A,B,C,D in Section-VIII) per quarter shall be capped at a maximum of 25% of the respective Quarterly payment of Grand Total Value.	**Request revision of this clause:** The overall Penalties (for Clause 1-A,B,C,D,**E, F,** in Section-VIII) per quarter shall be capped at a maximum of ~~25%~~ **5%** of the respective Quarterly payment of Grand Total Value.	No Change
21	48	14) SLA during warranty period and penalties for breach thereof:	The overall Penalties for non-adherence with the SLA of warranty support (during 3rd , 4th & 5th year of warranty period) per quarter shall be capped at a maximum of 25% of the respective Quarterly payment (CAPEX).	**Request revision of this clause:** The overall Penalties for non-adherence with the SLA of warranty support (during 3rd , 4th & 5th year of warranty period) per quarter shall be capped at a maximum of ~~25%~~ 5% of the respective Quarterly payment (CAPEX).	No Change
22	56	10) Prices and Payme	Suggest addition of this clause	All the Payments shall be made within a period of 30 days from the date of submission of invoice.	No Change

23	60	12.1.3 Terminations for Default	12.1.3 Terminations for Default 1) Notice for Termination for Default: In the event of unsatisfactory resolution of 'Notice of Default' within two weeks of its issue as per sub-clause above, the ERNET India, if so decided, shall by written Notice of Termination for Default sent to the contractor, terminate the contract in whole or in part, without compensation to the contractor.	**Request revision of this clause:** 12.1.3 Terminations for Default 1) Notice for Termination for Default: In the event of unsatisfactory resolution of 'Notice of Default' within **five** ~~two~~ weeks of its issue as per sub-clause above, the ERNET India, if so decided, shall by written Notice of Termination for Default sent to the contractor, terminate the contract in whole or in part, without compensation to the contractor.	No Change
24	47	6.4 Warranty for equipments/solutions procured via this tender at New DC-DR & remote sites	All ongoing software upgrades, patches for all major and minor releases should be provided during the warranty period.	Request you to confirm that the understanding of bidder's responsibility is for any patch update will be on Quarterly basis and any version upgrade will be Once in Year.	All software upgrades, patches for all major and minor releases or any other releases , should be done regularly on immediate basis as soon as the new release is available.
25	49	7 Inspection and Quality Assurance	In addition, ERNET India reserves the right to do the FAT (Factory Acceptance Testing) for any equipment(s) before delivery of equipment(s).	Please clarify if ERNET intends to do FAT from the Bidder/OEM/Distrubutor/Partner's or bidder's designated place/ Warehouse before despatch of the devices	No Change
26	83	A. Bidder's Qualification Criteria	Bidder should have experience of successful implementation of data center with leaf and spine architecture in Central/State Government/ Govt. undertakings/ UT's/Autonomous Bodies/Public listed companies/reputed Private organisation in India as:	We understand that Spine & Leaf mentioned here means Bidder should have supplied the Spine & Leaf/Network/Access switches with SDN(software defined network) solution. Pls. confirm if the understanding is correct.	Kindly refer to respective updated clause in Annexure-B
27	89	1. Project Overview	Provisioning of Co-Location Services w.r.t New DC and DR	We understand Co-Location facility will be finalised/provided by ERNET	Yes,Co-Location facility will be finalised/provided by ERNET
28	89	2.Scope of Work of Contractor	Site survey report of DC & DR.	We understand that DC & DR referred here is as Co-Location to be finalized by ERNET. Pls. confirm if the understanding is correct.	Yes,Co-Location facility will be finalised/provided by ERNET
29	89	2.Scope of Work of Contractor	Site survey report of DC & DR.	Bidder request ERNET to share scope under Site Survey.	In general a Site Survey will include at least Survey w.r.t Space, Power, Cooling , Cabling, Availability of Interfaces/Ports , etc. Site Survey Report Template will be created by bidder & finalized in consultation with ERNET India/CERT-In.
30	95	7. Role and Responsibilities of Contractor i.r.o AAA,AD,EMS and related software applications:	Integration with Email Gateways/servers, SMS Gateways. Please note that Supplied EMS must have the capability to get integrated with standard solutions available in market w.r.t Email Gateways/servers, SMS Gateways.	We understand that this is just a functionality asked in the RFP and not the actual integration required in the RFP with Email Gateways/servers, SMS Gateways. Pls. confirm if the understanding is correct	Effort for integration of sought functionality must be considered while bidding . Additionally many of these solutions (not procured in this bid) shall be procured separately in future. Hence, the current estimates shall include such integration efforts.
31	167	Form 12 Financial Bid (BoQ)	SFTP Solution in HA (with NAS)	Please confirm if the understanding is to provide the SFTP solution is only at New-DC location and not required at New-DR site	Yes
32	167	Form 12 Financial Bid (BoQ)	Enterprise Data Log Analytics Management with Application & Infrastructure monitoring	Please confirm if the understanding is to provide the mentioned solution is only at New-DC location and not required at New-DR site	Yes
33	182	Storage capacity in all Storage & Server	Each Server With Minimum Storage capacity(mentioned in each section/category)	We understand that the capacity mentioned here is RAW i.e. before any RAID configuration. Please confirm if the understanding is different	Yes

34	84	A. Bidder's Qualification Criteria Point #5	5. Bidder should have experience of successful implementation of Supply & Installation or operation and maintenance at 50 locations, of WAN setup in customer office premises in single or multiple orders in Central/State Government/ Govt. undertakings / UT's /Autonomous Bodies/Public listed companies.	Requesting changes in the clause as highlighted in Green below: 5. Bidder should have experience of successful implementation of Supply & Installation or operation and maintenance at 50 locations, of WAN setup / LAN setup/ Network Management/ provisioning of Network Connectivity in customer office premises in single or multiple orders in Central/State Government/ Govt. undertakings / UT's /Autonomous Bodies/Public listed companies.	Kindly refer to respective updated clause in Annexure-B
35	84	A. Bidder's Qualification Criteria Point #4, 5 & 6	Note i.r.o clause 4,5&6- Bidder shall provide relevant copies of the customer purchase orders in support of scope of work, deliverables, project value and satisfactory work completion certificate from client. Bidder shall also provide Name, Address, email and contact no. of organization whose Purchase orders are submitted by Bidder. Order Completion date/date(s) should fall between 01/11/2019 to 31/10/2024.	Requesting changes in the clause as highlighted in Green below: Note i.r.o clause 4,5&6- Bidder shall provide relevant copies of the customer purchase orders in support of scope of work, deliverables, project value and satisfactory work completion certificate from client. Bidder shall also provide Name, Address, email and contact no. of organization whose Purchase orders are submitted by Bidder. Order Completion date/date(s) should fall between 01/11/~~2019~~ 2017 to 31/10/2024.	Kindly refer to respective updated clause in Annexure-B
36	84	A. Bidder's Qualification Criteria Point #7	7. The bidder must have following professional* working on its payroll: a. Prince-2/ PMP - 5 numbers b. CISA/CISSP/CISM - 2 numbers c. CDCP - 2 numbers d. CCIE-Sec/JNCIE-Sec - 1 numbers e. CCIE-ENT/JNCIE-ENT - 1 numbers f. CCIE-DC/CCNP-DC/JNCIE-DC/JNCIP-DC - 2 numbers g. CCNP-Sec/ JNCIP-Sec/Fortigate NSE-4/PCNSE - 3 numbers h. CCNP-ENT/ JNCIP-ENT - 3 numbers *Professionals must be regular employee of bidder as on date of submission of this bid. Fixed term contract/contractual employee will not be accepted. Valid certificate(s) of above professional to be submitted along with the bid with covering letter of Director HR of bidder's organisation.	Requesting changing this clause to the below suggested one: 7. The bidder must have atleast 100 technical resources for Network / Security/ Storage / Compute/ Data Center Operations working on its payroll: A letter of from HR of bidder's organization to be submitted for the same.	Kindly refer to respective updated clause in Annexure-B

37	85	A. Bidder’s Qualification Criteria Point #8	8. The bidder on the date of publishing of this bid; should already have in-house capabilities to discharge the roles & responsibilities as a System Integrator. Therefore, the bidder is not allowed to float any EoI or Tender against this Tender requirement for identifying any system integrator, consultant, empanelment, sub-contractor or a partner or a teaming partner etc by whatever name called; for discharging/sharing its responsibilities as a System Integrator. Further, it may also be noted that consortium, arrangements, joint-ventures, teaming, subletting, sub-contracting is strictly prohibited in this bid. In case, at any stage of the project, if its identified that any kind of above mentioned prohibitions were violated, ERNET India reserves the right to take suitable actions such as mentioned in Section III Clause 12. The bidder needs to submit an undertaking in this regard.	This is a complex project it requires multi location delivery & implementation. Coforge leverages its wide network of empaneled partners to ensure smooth and timely execution of the projects. We request ERNET to allow sub-contracting of some of the activities of the project. The entire ownership of the deliverables shall lie with Coforge and prior approval shall be taken for any such arrangement. Hence, requesting ERNET to remove submission of this undertaking.	No Change
38	99	Section 9, Clause 5.d point 5	Existing infra with Remote Sites (within 1 months of start of O&M by this bid’s contractor)	Need clarification on points 5 and 6 in the table on page 99. Specifically, does SI need to conduct VAPT within one month and then again within 11 months?	Yes
39	46	Section 6, Clause 14 - ii	SLA during warranty period and penalties for breach	Six resident engineers are inadequate to manage 24/7 operations after two years of O&M.	Read section VI, Clause 'ix' along with this clause.
40	51	Section 9, clause 9.3	Logistics and delivery of equipment to remote sites.	Will ERNET provide any logistical support or facilitate local clearances for delivery to remote or restricted locations?	No Change
41	113	Manpower Deployment	Minimum manpower requirements.	Can the deployment of manpower be staggered based on project milestones, or is it full deployment required from day one?	Full deployment required from day one
42	83	A. Bidder’s Qualification Criteria. Point no. 3	Bidder should have experience of successful implementation of similar project(s) in Central/State Government/ Govt. undertakings/ UT’s/Autonomous Bodies/Public listed companies/reputed Private organisation in India as: Single order of Rs. Rs.500 Crore or more; OR Two orders each having minimum of Rs. 250 Crore of estimated cost or more; OR Three orders each having minimum of Rs. 200 Crore of estimated cost or more	Considering the complexity of the project, we request to revise this clause as: Bidder should have experience of successful implementation of similar project(s) in Central/State Government/ Govt. undertakings/ UT’s/Autonomous Bodies/Public listed companies/reputed Private organisation in India as: **Single order of Rs. Rs.300 Crore or more**; OR **Two orders each having minimum of Rs. 150 Crore or more**; OR **Three orders each having minimum of Rs. 100 Crore or more**	Kindly refer to respective updated clause in Annexure-B
43	84	A. Bidder’s Qualification Criteria. Point no. 5	Bidder should have experience of successful implementation of Supply & Installation or operation and maintenance at 50 locations, of WAN setup in customer office premises in single or multiple orders in Central/State Government/ Govt. undertakings / UT’s /Autonomous Bodies/Public listed companies.	We request you to revise this clause as: Bidder should have experience of successful implementation of Supply & Installation or operation and maintenance at 50 locations, of **WAN / SDWAN** setup in customer office premises in single or multiple orders in Central/State Government/ Govt. undertakings / UT’s /Autonomous Bodies/Public listed companies.	Kindly refer to respective updated clause in Annexure-B

44	85	A. Bidder’s Qualification Criteria. Point no. 7	The bidder must have following professional* working on its payroll: a. Prince-2/ PMP - 5 numbers b. CISA/CISSP/CISM - 2 numbers c. CDCP - 2 numbers d. CCIE-Sec/JNCIE-Sec - 1 numbers e. CCIE-ENT/JNCIE-ENT - 1 numbers f. CCIE-DC/CCNP-DC/JNCIE-DC/JNCIP-DC - 2 numbers g. CCNP-Sec/ JNCIP-Sec/Fortigate NSE-4/PCNSE - 3 numbers h. CCNP-ENT/ JNCIP-ENT - 3 numbers *Professionals must be regular employee of bidder as on date of submission of this bid. Fixed term contract/contractual employee will not be accepted. Valid certificate(s) of above professional to be submitted along with the bid with covering letter of Director HR of bidder’s organisation.	Undertaking along with Valid certificate(s) of above professional to be submitted from HR Head of bidder’s organisation.	Kindly refer to respective updated clause in Annexure-B
45	52	9 Terms of Delivery and delays : 6. Timeline for Delivery, Installation, testing, commissioning & Acceptance, Sr. No. 2	Delivery of the Equipments at DC - 8 Weeks	We request you to revise the delivery timeline as below: **"**Delivery of the Equipments at DC **- 12 Weeks"**	Kindly refer to respective updated clause in Annexure-B
46	52	9 Terms of Delivery and delays,6. Timeline for Delivery, Installation, testing, commissioning & Acceptance, Sr. No. 5	Delivery of the Equipments at DR - 10 Weeks	We request you to please change delivery timeline as below: **"**Delivery of the Equipments at DR **- 14 Weeks"**	Kindly refer to respective updated clause in Annexure-B
47	57	10 Prices and Payments Terms, Sr. No. 6	b. In respect of DC and DR equipment (s), 50% of the value of equipment(s) delivered at DC and similarly 50% of the value of equipment(s) delivered at DR shall be released only after submission of BG equivalent to the amount which is to be released. The BG should be valid for a minimum period of 6 months (with a claim period of additional 3 months). BG must be extendable till the successful completion of rack mounting & Power On Self Test (POST) of active equipments.	We request you to change the Payment Terms as below: "b. In respect of DC and DR equipment (s), **80%** of the value of equipment(s) delivered at DC and similarly **80%** of the value of equipment(s) delivered at DR shall be released only after submission of BG equivalent to the amount which is to be released. The BG should be valid for a minimum period of 6 months (with a claim period of additional 3 months). BG must be extendable till the successful completion of rack mounting & Power On Self Test (POST) of active equipments."	No Change
48	57	10 Prices and Payments Terms, Sr. No. 6	c. In respect of equipment (s) at DC and DR, additional 30% of the total value of items will be made after successful installation, integration, commissioning and acceptance as per the respective milestone(s).	We request you to change the Payment Terms as below: c. In respect of equipment (s) at DC and DR, additional **20%** of the total value of items will be made after successful installation, integration, commissioning and acceptance as per the respective milestone(s).	No Change

49	57	10 Prices and Payments Terms, Sr. No. 6	e. Thereafter, based on successful performance during warranty period, balance 20% value of the respective milestone shall be released in twenty (20) equal instalments on a quarterly basis after completion of every quarter. It would be duty of contractor to get the satisfactory performance certificate from CERT-In or (any other 3rd party to whom equipment's warranty has been transferred on the basis of instructions from ERNET India) along with necessary documents. ERNET India may give an option to contractor to claim Balance 20% payment against submission of Bank Guarantee. If this option is given by ERNET India and the same is accepted by Contractor, then the contractor would be having an option to submit Bank Guarantee (BG) for: -	Since O & M payment is in quarterly as per RFP & Bidder has to submit the PBG as Security, we request you to remove this clause.	No Change
50	83	4	Bidder should have experience of successful implementation of data center with leaf and spine architecture in Central/State Government/ Govt. undertakings/ UT's/Autonomous Bodies/Public listed companies/reputed Private organisation in India as: Single order of Rs. 100 Crore or more;	Experience of bidders own data center used for commercial purposes for other customers may be allowed to meet this eligibility requirement	**Not Allowed**
51	83	3	Bidder should have experience of successful implementation of similar project(s) in Central/State Government/ Govt. undertakings/ UT's/Autonomous Bodies/Public listed companies/reputed Private organisation in India as: Single order of Rs. Rs.500 Crore or more; OR Two orders each having minimum of Rs. 250Crore of estimated cost or more; OR Three orders each having minimum of Rs. 200Crore of estimated cost or more Similar Projects: - Setting up of Data Centre (including computing, storage & networking Infrastructure) / Ongoing Operation & Maintenance of Data Centres (done for minimum of two years)/ Completed or ongoing AMC of Data Center (done for minimum of two years)/ Network Operation Centres/ Security operation centres/ Smart City Projects/ Large IT networking.	Experience of bidders own data center used for commercial purposes for other customers may be allowed to meet this eligibility requirement	**Not Allowed**
52	84	7	The bidder must have following professional* working on its payroll a. Prince-2/ PMP - 5 numbers b. CISA/CISSP/CISM - 2 numbers c. CDCP - 2 numbers d. CCIE-Sec/JNCIE-Sec - 1 numbers e. CCIE-ENT/JNCIE-ENT - 1 numbers f. CCIE-DC/CCNP-DC/JNCIE-DC/JNCIP-DC - 2 numbers g. CCNP-Sec/ JNCIP-Sec/Fortigate NSE-4/PCNSE - 3 numbers h. CCNP-ENT/ JNCIP-ENT - 3 numbers *Professionals must be regular employee of bidder as on date of submission of this bid. Fixed term contract/contractual employee will not be accepted. Valid certificate(s) of above professional to be submitted along with the bid with covering letter of Director HR of bidder's organisation.	The eligibility may be allowed to be met as a consortium	Kindly refer to respective updated clause in Annexure-B

53		.....	The bidder must have following professional* working on its payroll a. Prince-2/ PMP - 5 numbers b. CISA/CISSP/CISM - 2 numbersc. CDCP - 2 numbers d. CCIE-Sec/JNCIE-Sec - 1 numbers e. CCIE-ENT/JNCIE-ENT - 1 numbers f. CCIE-DC/CCNP-DC/JNCIE-DC/JNCIP-DC - 2 numbers g. CCNP-Sec/ JNCIP-Sec/Fortigate NSE-4/PCNSE - 3 numbers h. CCNP-ENT/ JNCIP-ENT - 3 numbers *Professionals must be regular employee of bidder as on date of submission of this bid. Fixed term contract/contractual employee will not be accepted. Valid certificate(s) of above professional to be submitted along with the bid with covering letter of Director HR of bidder's organisation.	Undertaking that the biddder will be deploying the certified manpower, once we get order may be allowed	Kindly refer to respective updated clause in Annexure-B
54	85	8	The bidder on the date of publishing of this bid; should already have in-house capabilities to discharge the roles & responsibilities as a System Integrator. Therefore, the bidder is not allowed to float any EoI or Tender against this Tender requirement for identifying any system integrator, consultant, empanelment, sub-contractor or a partner or a teaming partner etc by whatever name called; for discharging/sharing its responsibilities as a System Integrator. Further, it may also be noted that consortium, arrangements, joint-ventures, teaming, subletting, sub-contracting is strictly prohibited in this bid. In case, at any stage of the project, if its identified that any kind of above mentioned prohibitions were violated, ERNET India reserves the right to take suitable actions such as mentioned in Section III Clause 12. The bidder needs to submit an undertaking in this regard.	As the project is too comprehensive with vast scope of work, the project may be allowed to be addressed as consortium with three partners including lead bidder	No Change
55	9	2.3	Earnest Money Deposit (EMD): INR 15,00,00,000/- (Rupees Fifteen Crore Only). EMD shall be shall be submitted in one of the following forms:	Central PSUs may be exempted from the submission of EMD and Bid securing declaration may be allowed to be submitted	Kindly refer to respective updated clause in Annexure-B
56	General	.....	Due date of bid submission	ITI Limited is in the process of addressing the tender and as the project has vast scope of work, request to extend the bid submission duedate for 4 weeks from the present due date of the tender	Kindly refer GeM portal for any Bid Submission Date Change
57	84	A. Bidder's Qualification Criteria Point 5	Note i.r.o clause 4,5&6- Bidder shall provide relevant copies of the customer purchase orders in support of scope of work, deliverables, project value and satisfactory work completion certificate from client. Bidder shall also provide Name, Address, email and contact no. of organization whose Purchase orders are submitted by Bidder. Order Completion date/date(s) should fall between 01/11/2019 to 31/10/2024.	Kindly amend the clause as below: Note i.r.o clause 4,5&6- Bidder shall provide relevant copies of the customer purchase orders in support of scope of work, deliverables, project value and satisfactory work completion certificate from client**/ Certificate signed by the CA of the bidding entity.**. Bidder shall also provide Name, Address, email and contact no. of organization whose Purchase orders are submitted by Bidder. Order completion date/date(s) should fall between **~~01/11/2019 to 31/10/2024~~ 01/01/2017 to 31/10/2024**	Kindly refer to respective updated clause in Annexure-B

58	84	A. Bidder's Qualification Criteria Point 5	Note i.r.o clause 4,5&6- Bidder shall provide relevant copies of the customer purchase orders in support of scope of work, deliverables, project value and satisfactory work completion certificate from client. Bidder shall also provide Name, Address, email and contact no. of organization whose Purchase orders are submitted by Bidder. Order Completion date/date(s) should fall between 01/11/2019 to 31/10/2024.	We understand order completion date is Project Go-Live date. Kinldy confirm.	Clause is self explanatory.
59	83	A. Bidder's Qualification Criteria Point 3	Bidder should have experience of successful implementation of similar project(s) in Central/State Government/ Govt. undertakings/ UT's/Autonomous Bodies/Public listed companies/reputed Private organisation in India as: Single order of Rs. Rs.500 Crore or more; OR Two orders each having minimum of Rs. 250Crore of estimated cost or more; OR Three orders each having minimum of Rs. 200Crore of estimated cost or more	We request to kindly ammend the clause as: Bidder should have experience of successful implementation of similar project(s) in Central/State Government/ Govt. undertakings/ UT's/Autonomous Bodies/Public listed companies/reputed Private organisation in India as: Single order of Rs. Rs.500 Crore or more; OR Two orders each having minimum of Rs. 250Crore of estimated cost or more; OR Three orders each having minimum of ~~Rs. 200~~ **Rs. 150** Crore of estimated cost or more	Kindly refer to respective updated clause in Annexure-B
60	85	A. Bidder's Qualification Criteria Point 7	Professionals must be regular employee of bidder as on date of submission of this bid. Fixed term contract/contractual employee will not be accepted. Valid certificate(s) of above professional to be submitted along with the bid with covering letter of Director HR of bidder's organisation	Kindly amend the clause as below: Professionals must be regular employee of bidder as on date of submission of this bid. Fixed term contract/contractual employee will not be accepted. Valid certificate(s) of above professional to be submitted along with the bid with covering letter of Director HR/**Head HR** of bidder's organisation	Kindly refer to respective updated clause in Annexure-B
61	58	10 Prices and Payments Terms: Point 7	It may be noted that the payment to the contractor are subject to making sufficient funds available by CERT-In to ERNET India . Contractor agrees and accepts that there can be delays in releasing the payment due to non-availability of funds.	As the project is CAPEX intensive, wherein contractor has to do the upfront payment to the OEMs with minimal credit days. Any delay in getting payment from ERNET will badly affect the cash flow of the Contractor. Hence we request not to delay the relasing of payment to contractor due to non-availability of funds, which is not attributable to the default of the contractor.	CERT-In is the funding agency of this project, accordingly , release of payments to contractor will be made upon receipt of funds .

62	57	10 Prices and Payments Terms, point no 6	a.Under this project, there are two types of Payments. One is CAPEX Payment i.e. price of equipment(s) and other is payment pertaining to OPEX i.e. Operation & Maintenance (O&M) services b.In respect of DC and DR equipment (s), 50% of the value of equipment(s) delivered at DC and similarly 50% of the value of equipment(s) delivered at DR shall be released only after submission of BG equivalent to the amount which is to be released. The BG should be valid for a minimum period of 6 months (with a claim period of additional 3 months). BG must be extendable till the successful completion of rack mounting & Power On Self Test (POST) of active equipments. c.In respect of equipment (s) at DC and DR, additional 30% of the total value of items will be made after successful installation, integration, commissioning and acceptance as per the respective milestone(s).. d. In respect of equipment at remote sites, 80% of the total value of items will be made after successful delivery, installation, integration, commissioning and acceptance of the individual remote sites. e. Thereafter, based on successful performance during warranty period, balance 20% value of the respective milestone shall be released in twenty (20) equal instalments on a quarterly basis after completion of every quarter. It would be duty of contractor to get the satisfactory performance	We request you to amend the payment terms as follows: - a. Under this project, there are two types of Payments. One is CAPEX Payment i.e. price of equipment(s) and other is payment pertaining to OPEX i.e. Operation & Maintenance (O&M) services. b. In respect of DC and DR equipment (s), ~~50%~~ **70%** of the value of equipment(s) delivered at DC and similarly ~~50%~~ **70%**of the value of equipment(s) delivered at DR shall be released only after submission of BG equivalent to the amount which is to be released. The BG should be valid for a minimum period of 6 months (with a claim period of additional 3 months). BG must be extendable till the successful completion of rack mounting & Power On Self Test (POST) of active equipments. c. In respect of equipment (s) at DC and DR, additional ~~30%~~ **20%** of the total value of items will be made after successful installation, integration, commissioning and acceptance as per the respective milestone(s).. d.In respect of equipment at remote sites, ~~80%~~ 70 % of the total value of items will be made after successful delivery ~~installation, integration, commissioning and acceptance~~ of the **equipments at** individual remote sites **e.**In respect of equipment at remote sites, ~~80%~~ **20 %** of the total value of items will be made after successful ~~delivery~~ installation, integration, commissioning and acceptance of the individual remote sites e. Thereafter, based on successful performance during warranty period, balance ~~20%~~ 10% value of the respective milestone shall be released ~~in twenty (20) equal instalments on a quarterly basis after completion of every quarter. It~~	Kindly refer to respective updated clause in Annexure-B
63	52	9 Terms of Delivery and delays	Delivery of the Equipments at DC T+8 Weeks	Due to global electronic semiconductor/chip shortage, delivery lead time of OEMs badly affected, hence we request to modify the clause as: Delivery of the Equipments at DC T+20 Weeks	Kindly refer to respective updated clause in Annexure-B
64	52	9 Terms of Delivery and delays	Installation, Testing & Commissioning of Complete Equipments at DC Offering of this infrastructure under Milestone-1 for Acceptance Testing (AT) to ERNET India as per Acceptance Testing Plan (ATP). T+28 Weeks	Request to modify as: Installation, Testing & Commissioning of Complete Equipments at DC Offering of this infrastructure under Milestone-1 for Acceptance Testing (AT) to ERNET India as per Acceptance Testing Plan (ATP). T+32 Weeks	No Change
65	52	9 Terms of Delivery and delays	Delivery of the Equipments at DR T+10 Weeks	Due to global electronic semiconductor/chip shortage, delivery lead time of OEMs badly affected, hence we request to modify the clause as: Delivery of the Equipments at DR T+24 Weeks	Kindly refer to respective updated clause in Annexure-B
66	52	9 Terms of Delivery and delays	Installation, Testing & Commissioning of Complete Equipments at DR Offering of this infrastructure under Milestone-1 for Acceptance Testing (AT) to ERNET India as per Acceptance Testing Plan (ATP). T+32 Weeks	Request to modify as: Installation, Testing & Commissioning of Complete Equipments at DR Offering of this infrastructure under Milestone-1 for Acceptance Testing (AT) to ERNET India as per Acceptance Testing Plan (ATP). T+36 Weeks	No Change
67	52	9 Terms of Delivery and delays	Site Survey (if required), Delivery, Installation, Testing & Commissioning of Complete equipments at Remote Sites and their integration with DC T+36 Weeks	Request to modify the timeline as Site Survey (if required), Delivery, Installation, Testing & Commissioning of Complete equipments at Remote Sites and their integration with DC **T+ 44 weeks**	No Change
68	52	9 Terms of Delivery and delays	Acceptance by ERNET India for Complete Milestone-3 and issuance of acceptance certificate subject to completion of complete work as per tender T+40 Weeks	Request to modify the timeline as: Acceptance by ERNET India for Complete Milestone-3 and issuance of acceptance certificate subject to completion of complete work as per tender T+52 Weeks	No Change

69	83	Section VI: Qualificati	**A. Bidder’s Qualification Criteria** 4. Bidder should have experience of successful implementation of data center with leaf and spine architecture in Central/State Government/ Govt. undertakings/ UT’s/Autonomous Bodies/Public listed companies/reputed Private organisation in India as: Single order of Rs. 100 Crore or more;	We request to kindly ammend the clause as: 4. Bidder should have experience of successful implementation of data center with leaf and spine architecture in Central/State Government/ Govt. undertakings/ UT’s/Autonomous Bodies/Public listed companies/reputed Private organisation in India as: Single order of ~~Rs. 100 Crore~~ **Rs. 80 Crore** or more;	Kindly refer to respective updated clause in Annexure-B
70	85	Section VI: Qualificati	7. The bidder must have following professional* working on its payroll: a. Prince-2/ PMP - 5 numbers b. CISA/CISSP/CISM - 2 numbers c. CDCP - 2 numbers d. CCIE-Sec/JNCIE-Sec - 1 numbers e. CCIE-ENT/JNCIE-ENT - 1 numbers f. CCIE-DC/CCNP-DC/JNCIE-DC/JNCIP-DC - 2 numbers g. CCNP-Sec/ JNCIP-Sec/Fortigate NSE-4/PCNSE - 3 numbers h. CCNP-ENT/ JNCIP-ENT - 3 numbers	We request to kindly ammend the clause as: 7. The bidder must have following professional* working on its payroll: a. Prince-2/ PMP - 5 numbers b. CISA/CISSP/CISM - 2 numbers c. ~~CDCP - 2 numbers~~ **CDCP/CDCS – 1 Number** d. ~~CCIE-Sec/JNCIE-Sec - 1 numbers~~ **CCIE-Sec/JNCIE-Sec/JNCIA-Sec - 1 numbers** e. ~~CCIE-ENT/JNCIE-ENT - 1 numbers~~ **CCIE-ENT/JNCIE-ENT / JNCIA-Junos - 1 numbers** f. ~~CCIE-DC/CCNP-DC/JNCIE-DC/JNCIP-DC - 2 numbers~~ **CCIE-DC/CCNP-DC/JNCIE-DC/JNCIP-DC/CCNP-ENT - - 2 numbers** g. CCNP-Sec/ JNCIP-Sec/Fortigate NSE-4/PCNSE - 3 numbers h. ~~CCNP-ENT/ JNCIP-ENT - 3 numbers~~ **CCNP-ENT/ JNCIP-ENT/CCNA - 3 numbers**	Kindly refer to respective updated clause in Annexure-B
71	30	12 Award of Contract	12.1.1 Right to Vary Quantities i. ERNET India reserves the right to increase/decrease the quantities to be ordered up to 25 % of sum total of final bid value; at the time of placement of contract.	Request to limit the increase/decrease in quantity to **10%** of the indicative quantity . Kindly amend the clause as follows: "i. ERNET India reserves the right to increase/decrease the quantities to be ordered up to ~~25 %~~ **10%** of sum total of final bid value; at the time of placement of contract."	No Change
72	60	12 Defaults, Breaches	**12.1.4 Contractual Remedies for Breaches/Defaults or Termination for Default** **6) Risk and Cost Procurement:** In addition to termination for default, the ERNET India shall be entitled, and it shall be lawful on its part, to procure Equipment and services similar to those terminated, with such terms and conditions and in such manner as it deems fit at the “Risk and Cost” of the contractor. Such ‘Risk and Cost Procurement’ will be contracted within nine months from the breach of Contract. The Contractor shall be liable for any loss which the ERNET India may sustain on that account provided the procurement, or, if there is an agreement to procure, such agreement is made. The Contractor shall not be entitled to any gain on such procurement, and the manner and method of such procurement shall be in the entire discretion of the ERNET India. It shall not be necessary for the ERNET India to notify the contractor of such procurement. It shall, however, be at the discretion of the ERNET India to collect or not the security deposit from the firm/ firms on whom the contract is placed at the risk and cost of the defaulted firm.	Request you to delete the Risk purchase clause.	No Change

73	18	Section II: Instructions to Bidders (ITB) 4.2 Eligibility to participate and purchase preference	a) Only Class-I and Class-II local Suppliers shall be eligible to participate in this bid. Local content percentage for qualifying as Class-I and Class-II local Suppliers shall be calculated and declared by the respective bidders on the basis of Letter no P45021/2/2017- (BE-II) dated 15.06.2017 Public Procurement (Preference to Make in India) Order 2017" (MII) of Department for Promotion of Industry and Internal Trade, (DPIIT - Public Procurement Section); as revised and amended time to time and also clarifications and FAQ issued by DPIIT in this respect from time to time	We understand for the calculation of local content percentage will be including the service cost and the O&M(OPEX) cost. Kindly confirm	No Change
74	21	Section II: Instructions to Bidders (ITB) 5.3 Goods and Services Tax (GST)	6) In case, in future any GST liability is required to be borne by ERNET India; which was the responsibility of the Bidder/Contractor, then the same shall be claimed from the Bidder/Contractor by way of raising debit notes	In future any change in current rate of taxation or introduction of new statutory levies then in such cases the bidder will be compensated as per actuals levied on bidder. Kindly confirm	No Change
75	30	Section II: Instructions to Bidders (ITB) 11.4.1 Financial Bids	1) Evaluation of the financial bids shall be on the price criteria only. Financial Bids of all Technically qualified bidders will be evaluated and an e-Reverse Auction (e-RA) process which will be conducted on GeM portal to determine the lowest cost (L-1) bidder.	In order to get the most competitive offer request to kindly delete the Reverse Auction clause	No Change
76	30	Section II: Instructions to Bidders (ITB) 12.1.1 Right to Vary Quantities	ii. Keeping in the view of the fact that the project requirements are dynamic and ever changing therefore ERNET India reserves the right to increase the ordered value by up to 25% of sum total of final bid value; till the completion of O&M activities, without any reference to the initial ordered quantities. iii. Successful Bidder/ Contractor is bound to accept the orders accordingly, failing which; ERNET India may declare this as an event of default and consequences for event of default will be applicable.	No OEM will hold the price validity during the entire period of contract owing to several factors like dollar price escalation, commodity/metal price escalation, inflation etc. Hence request to include the compensation for dollar escalation and commodity/metal price escalation, inflation factor for variation requirement post completion of Delivery Milestone. Please Confirm	No Change
77	40	Section III: General Conditions of Contract(GCC) 5.4 Assignment and Sub-contracting	1) All the manpower to be deployed in project for delivery, installation, testing & commissioning and operation & maintenance including onsite support should be on the payroll of the Contractor or OEM whose equipment(s) are offered. Outsourcing of manpower will not be allowed.	The bidder is liable for the overall RFP and will be providing the resources in line with the qualification defined in the RFP. Hence request to kindly allow the subcontracting of the Manpower considering the large volume of the Manpower requirement.	No Change

78	41	Section III: General Conditions of Contract (GCC)/ 5.5	**5.5 Indemnities for breach of IPR Rights or from other issues**- The contractor shall be solely responsible for any damage, loss or injury which may occur to any property or to any person by or arising out the execution of the works or temporary works or in carrying out of the contract otherwise than due to the matters referred to in this agreement hereinbefore. The Contractor would ensure for observance of all labour and other laws applicable in the matter and shall indemnify and keep indemnified the ERNET India, end users/ its customers against the effect of non observance of any such laws	We suggest the inclusion of the following verbiage: Notwithstanding as stated herein above; Contractor shall have no obligations with respect to any Infringement Claims to the extent that the Infringement Claim arises or results from: (i) Contractor's compliance with ERNET's specific technical designs or instructions; (ii) inclusion in a Deliverable of any content or other materials provided by ERNET and the infringement relates to or arises from such ERNET materials or provided material; (iii) modification of a Deliverable after delivery by Contractor to ERNET if such modification was not made by or on behalf of the Contractor; (iv) operation or use of some or all of the Deliverable in combination with products, information, specification, instructions, data, materials not provided or approved by Contractor; or (v) use of the Deliverables for any purposes for which the same have not been designed or developed or other than in accordance with any applicable specifications or documentation provided under the applicable Work Order by the Contractor; or (v) ERNET's failure to use any modification of the Deliverable furnished free of charge under this Agreement including, but not limited to, corrections, fixes, or enhancements made available by the Contractor. ERNET Infringement Indemnity. ERNET will defend, indemnify and hold harmless the Contractor, applicable Contractor affiliates ("Contractor Indemnified Party") from and against any third party suit, proceedings damages, judgments, cost and expenses (including reasonable	No Change
79	42	Section III: General Conditions of Contract(GCC) /5.6.2	5.6.2. **Confidentiality** All documents, drawings, samples, data, associated correspondence or other information furnished by or on behalf of the ERNET India/ CERT-In to the contractor, in connection with the contract, whether such information has been furnished before, during or following completion or termination of the contract, are confidential and shall remain the property of the ERNET India/ CERT-In and shall not, without the prior written consent of ERNET India/ CERT-In neither be divulged by the contractor to any third party..............	We suggest the inclusion of the following verbiage: Notwithstanding anything contrary stated under this Contract, ERNET hereby agrees that it has taken all technical and organizational security measures necessary to protect the information technology systems and data used in connection with the operation of the its businesses and has reasonably established, maintained, implemented and complied with, adequate information technology protection, information security, and cyber security controls, including integrity and confidentiality practices and procedures to prevent any breach, destruction, loss, unauthorized distribution, or other compromise or misuse of any information technology system or data used in connection with the operation of the its businesses. The ERNET confirms that the Contractor does not have any obligation to assess or evaluate the effectiveness of the ERNET's information security system and controls and hence, shall not be held responsible in the event of any loss, damage, destruction, misuse, alteration, modification, unauthorized access, or compromise arising out of ERNET's negligence, failure, or inability to implement appropriate information security controls and measures or to protect its own network. Further, if the ERNET requires Contractor to access or use ERNET's or third-party systems or devices, Contractor shall have no responsibility for the confidentiality, security or data protection controls of such systems or devices or for their performance or compliance with ERNET's requirements or applicable law	No Change

80	58	Section III: General Conditions of Contract(GCC) /11	**11. Dispute Resolution Mechanism**	We suggest the following revision in sub clause (i) Disputes having value less than Rs. 10 crore; shall be referred to and finally resolved by arbitration under Arbitration and Conciliation Act, 1996 and administered by the Indian Dispute Resolution Centre under the IDRC Domestic Arbitration Rules, 2019 in force when the Notice of Arbitration is submitted. The Arbitration panel shall consist of neutral arbitrators.	No Change
81	61	Section III: General Conditions of Contract(GCC) /12.1.5	**12.1.5 Limitation of Liability** Except in cases of criminal negligence or wilful misconduct, the aggregate liability of the contractor to the ERNET India, whether under the contract, in tort or otherwise, shall not exceed the total Contract value, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment, or to any obligation of the contractor to indemnify the ERNET India concerning IPR infringement	We suggest the inclusion of the following verbiage: Except in cases of criminal negligence or wilful misconduct, any special, indirect, incidental, consequential, exemplary damages arising out of the Contractor's engagement under this contract, including, without limitation, any costs, expenses or liabilities incurred as a result of lost profit or revenues the aggregate liability of the contractor to the ERNET India, whether under the contract, in tort or otherwise, or to any obligation of the contractor to indemnify the ERNET India concerning IPR infringement shall not exceed the total Contract value, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment, ~~or to any obligation of the contractor to indemnify the ERNET India concerning IPR infringement.~~	No Change
82	155	Form 10: Non-Disclosure Agreement/ Clause 14	14. This Agreement will remain in effect during the currency of agreement & shall survive even after expiry of the agreement or project	We suggest the following revision in Clause 14 of the Non-Disclosure Agreement : 14. This Agreement will remain in effect during the currency of agreement & shall survive ~~even~~ for a period of two years after expiry of the agreement or project	No Change
83	47	Section III: General Conditions of Contract(GCC) 6.4 Warranty for equipments/solutions procured via this tender at New DC-DR & remote sites	4) Obligations of the contractor under the warranty clause shall remain valid for all the sites installed, accepted and paid-for; even though the contract is terminated for any reason whatsoever.	Post termination or contract closure the obligation shall be with the OEMs as bidder will be providing the warranty certificate. Hence kindly amend the query accordingly.	No Change, SI Manpower is also required during waranty phase.
84	48	Section III: General Conditions of Contract(GCC) 6.4 Warranty for equipments/solutions procured via this tender at New DC-DR & remote sites 14) SLA during warranty period and penalties for breach thereof:	iv. At Data Centre (DC & DR) and remote Sites, for faults in any of the equipment , SLA Penalty @ 0.25 % of equipment cost per day or part thereof will be deducted beyond 24 hours from the reporting time of fault. In case fault persist for more than 48 hours from the reporting time of fault, then Penalty @ 0.5 % of equipment cost per day or part thereof will be deducted. SLA Penalty of Rs. 2,000/- per day or part thereof will be charged for equipment(s) (active and passive components) whose price could not be derived (e.g. Intelligent cables) from the price bid.	The penalties are very high and request to amend the clause as follows: "*iv. At Data Centre (DC & DR) and remote Sites, for faults in any of the equipment , SLA Penalty @ ~~0.25%~~* ***0.05%*** *of equipment cost per day or part thereof will be deducted beyond 24 hours from the reporting time of fault. In case fault persist for more than 48 hours from the reporting time of fault, then Penalty @ ~~0.5 %~~* ***0.1%*** *of equipment cost per day or part thereof will be deducted. SLA Penalty of Rs. ~~2,000/~~ -* ***500/-*** *per day or part thereof will be charged for equipment(s) (active and passive components) whose price could not be derived (e.g. Intelligent cables) from the price bid* ."	No Change

85	49	Section III: General Conditions of Contract(GCC) 6.4 Warranty for equipments/solutions procured via this tender at New DC-DR & remote sites 14) SLA during warranty period and penalties for breach thereof:	viii. The overall Penalties for non-adherence with the SLA of warranty support (during 3rd , 4th & 5th year of warranty period) per quarter shall be capped at a maximum of 25% of the respective Quarterly payment (CAPEX). In case penalty imposed on the contractor consecutively for two quarters reaches the maximum Penalty (i.e. 25%) then in such an eventuality ERNET India reserves the right to terminate the Contract as per Clause 12.1 & 12.2.	The overall cap is very high and per standard practice cap the penalty @10% of QGR and amend the clause as follows: "*viii. The overall Penalties for non-adherence with the SLA of warranty support (during 3rd , 4th & 5th year of warranty period) per quarter shall be capped at a maximum of* ~~*25%*~~ ***10%*** *of the respective Quarterly payment (CAPEX). In case penalty imposed on the contractor consecutively for two quarters reaches the maximum Penalty (i.e.* ~~*25%*~~ ***10%*** *)then in such an eventuality ERNET India reserves the right to terminate the Contract as per Clause 12.1 & 12.2."*	No Change
86	58	Section III: General Conditions of Contract(GCC) 10 Prices and Payments Terms:	6. The payment terms are: g. O&M Charges for remote sites will start from the completion of respective milestone and will be paid proportionately based on O&M price derived for each site from price bid.	Kindly confirm the calculation for deriving the O&M prices for remote sites	It is the duty of the bidder to attend any fault at remote site. For this bidder's field engineer needs to visit time to time. Accordingly, bidder may prepare their O&M prices for remote sites.
87	60	Section III: General Conditions of Contract(GCC) 12.1.4 Contractual Remedies for Breaches/Defaults or Termination for Default	4) Debar the contractor from participation in future procurements as follows: 5) ERNET India may debar the contractor or any of its successors from participating in any Tender Process undertaken by it for a period not exceeding two years commencing from the date of debarment. Terminate contract for default, fully or partially including its right for Risk-and-Cost Procurement as per following sub-clause.	Request to kindly limit the debarment clause for termination due to any wilful misconduct, gross neglect, fraudulent or any coercive action only.	No Change
88	61	Section III: General Conditions of Contract(GCC) 12.2 Termination for Default/ Convenience of ERNET India	1) The ERNET India reserves the right to terminate the contract, in whole or in part for its (the ERNET India's) convenience, by serving written 'Notice for Determination of Contract' on the contractor by giving sixty (60) days prior notice during the currency of the contract. The notice shall specify that the termination is for the convenience of the ERNET India of the contract. The notice shall also indicate inter-alia, the extent to which the contractor's performance under the contract is terminated, and the date with effect from which such termination shall become effective.	Kindly grant the bidder also the right to terminate for convenience and amend the clause as follows: "1) ~~The ERNET India~~ **Either Party** reserves the right to terminate the contract, in whole or in part for its (the ERNET India's) convenience, by serving written 'Notice for Determination of Contract' on the contractor by giving ~~sixty (60) days~~ **5 Months** prior notice during the currency of the contract. The notice shall specify that the termination is for the convenience ~~of the ERNET India~~ of the contract. The notice shall also indicate inter-alia, the extent to which the contractor's performance under the contract is terminated, and the date with effect from which such termination shall become effective."	No Change
89	61	Section III: General Conditions of Contract(GCC) 12.3.1 No Claim Certificate and Release of Contract Securities	After mutual reconciliations of outstanding payments and assets on either side, the contractor shall submit a 'No-claim certificate' to the ERNET India requesting the release of its contractual securities, if any. The ERNET India shall release the contractual securities without any interest if no outstanding obligation, asset, or payments are due from the contractor. The contractor shall not be entitled to make any claim whatsoever against the ERNET India under or arising out of this Contract, nor shall the ERNET India entertain or consider any such claim, if made by the contractor, after he shall have signed a "No Claim" Certificate in favour of the ERNET India. The Contractor shall be debarred from disputing the correctness of the items covered by the "No Claim" Certificate or demanding a clearance to arbitration in respect thereof.	Kindly amend the clause as follows: "*After mutual reconciliations of outstanding payments and assets on either side, the contractor shall submit a 'No-claim certificate' to the ERNET India requesting the release of its contractual securities, if any. The ERNET India shall release the contractual securities without any interest if no outstanding obligation, asset, or payments are due from the contractor. The contractor shall not be entitled to make any claim whatsoever against the ERNET India under or arising out of this Contract, nor shall the ERNET India entertain or consider any such claim, if made by the contractor, after he shall have signed a "No Claim" Certificate in favour of the ERNET India.* ~~*The Contractor shall be debarred from disputing the correctness of the items covered by the "No Claim" Certificate or demanding a clearance to arbitration in respect thereof*~~*."*	No Change

90	86	.....	10. Bidder should provide a dedicated/Toll free no. for service support. Relevant details to be submitted with Bid Document or an Undertaking to this effect that the same shall be provided within 15 days from the date of placement of contract.	We understand the toll free no should be from the OEMs. Please confirm	This clause stands deleted
91		Section VII: Scope of Work 1. Project Overview	i. To setup , commission and integrate IT Infrastructure/equipment(s) & solutions of DC, DR and 100+ remote locations.	Please clarify the location and actual no. of remote location	The clause may be read as follows : i. To setup , commission and integrate IT Infrastructure/equipment(s) & solutions of DC, DR and **34+ remote locations.** ii. To configure and establish MPLS/ P2P / ILL Links connectivity at DC, DR and **34+ remote locations** & configure the sought P2P & ILL Links. Please note that ERNET India will arrange MPLS P2P & ILL service provider, however, integration of supplied hardware with MPLS, P2P & ILL links will be the responsibility of contractor. iii. To Establish IPSec tunnels over MPLS, P2P & ILL links so as to create data path between commissioned remote sites & Data Centres in order to receive data from remote locations to Data Centres & within Data Centers. iv. Migration **& Maintainence** of 80 Links from existing DC & DR to New DC & DR. v. Operations & Maintenance (O&M) of exsisting & supplied Infrastructure and MPLS, P2P & ILL links. vi. Provisioning of Co-Location Services w.r.t New DC and DR.
92	102	Section VII: Scope of Work 12. Scope of Work for Operation and Maintenance	Comprehensive Onsite Maintenance with spare parts for all equipment's/items mentioned in BOM.	As per Bill of Material (BoM) we understand spare part needs to be maintained only for patch cords. Please confirm	It is the bidder's responsibility to maintain the SLA and plan the spare parts accordingly.
93	112	Section VII: Scope of Work 13. Manpower required at DC , DR, Delhi & other locations	1) Contractor must ensure that all the manpower deployed for Implementation/Operation & maintenance should be on Contractor's or OEM payroll as described in the tender T&Cs. ERNET India/CERT-In may increase (upto 25%) or decrease (upto 50%) the manpower as per the requirements with three month notice period, accordingly the manpower payment charges will be modified.	Request to allow contract based 3rd party man power to cater the variation in manpower requirement	No Change
94	112	Section VII: Scope of Work 13. Manpower required at DC , DR, Delhi & other locations	7) Contractor has to comply with local labour laws (minimum wages) as well as labour laws of government of India/ State Government.	Any bidder quoting significantly low quote for evading penalty or variation implication will be summarily rejected. Kindly confirm.	Clause is self explanatory.
95	115	Section VII: Scope of Work 13.2 Minimum Manpower to be deployed for two year(s) from the start of Operation and maintenance	In case deputed employee/staff is not available or is on leave, the Contractor is required to provide the alternative personnel with same or higher technical capabilities of the non-available personnel.	The manpower are entitled to yearly privelege leave. Kindly confirm the no. of days for yearly leave.	To maintain the 24x7 operations at DC/DR/Remote locations , Contractor needs to maintain required manpower strength at respective locations in all shifts, Accordingly Contractor needs to maintain sufficient manpower buffer to avoid any SLA breach.
96	124	Section VIII: Service Level Agreement during Operation & Maintenance B. For Equipment installed at existing DC , DR and Remote Sites :	3) The services down due to issues other than hardware fault i.e due to Operations and maintenance activities on existing DC, DR and Remote Sites equipment(s) at DC, DR and remote site, Penalty @ 0.5 % of quarterly payment of respective OPEX per day or part thereof will be deducted for downtime beyond permissible limit.	Request to amend the clause as follows" *"3) The services down due to issues other than hardware fault i.e due to Operations and maintenance activities on existing DC, DR and Remote Sites equipment(s) at DC, DR and remote site, Penalty @* ~~*0.5 %*~~ ***0.01%*** *of quarterly payment of respective OPEX per day or part thereof will be deducted for downtime beyond permissible limit."*	No Change

97	127	Section VIII: Service Level Agreement during Operation & Maintenance E. Security and Incident Management Service Levels for all DC and DR	(There will not be any penalty capping for this section)	Request to include the same under O&M capping	No Change
98	125	Section VIII: Service Level Agreement during Operation & Maintenance D. Help Desk Support Services Level	Penalty 0.1% of quarterly OPEX* value for every one hour delay (on incremental basis) beyond permissible time for High Priority level.0.05% of quarterly OPEX value for every one hour delay(on incremental basis) beyond permissible time for Low Priority level	Please clarify the rate of incremental basis	Rate of increment per hour will be 0.1%/ 0.05%/0.025% respectively as per the clause "Help Desk Support Services Level".
99	126	Section VIII: Service Level Agreement during Operation & Maintenance D. Help Desk Support Services Level	Penalty 0.1% of quarterly OPEX* value for every one hour delay (on incremental basis) beyond permissible time for High Priority level.0.05% of quarterly OPEX value for every one hour delay(on incremental basis) beyond permissible time for Low Priority level	Request to reduce the penalty and amend as follows: *" ~~0.1%~~ **0.01%** of quarterly OPEX* value for every one hour delay (on incremental basis) beyond permissible time for High Priority level. ~~0.05%~~ **0.001%** of quarterly OPEX value for every one hour delay(on incremental basis) beyond permissible time for Low Priority level "*	No Change
100	127	Section VIII: Service Level Agreement during Operation & Maintenance E. Security and Incident Management Service Levels for all DC and DR	For every instance of Data Theft, the bidder is subject to penalty and/or punishment applicable under the IT act/ ERNET India/CERT-In data theft policy or any other prevailing laws of the State/Country at that point of time, which shall be over and above the stated penalty Penalty Rs.5,00,000 per instance	Requet to reduce the penalty as follows: "Penalty Rs.~~5,00,000~~ **50,000** per instance	No Change
101	127	Section VIII: Service Level Agreement during Operation & Maintenance D. Help Desk Support Services Level	Note:- The overall Penalties (for Clause 1-A,B,C,D in Section-VIII) per quarter shall be capped at a maximum of 25% of the respective Quarterly payment of Grand Total Value. In case penalty imposed on the contractor consecutively for two quarters reaches the maximum Penalty (i.e 25%) then in such an eventuality ERNET India reserves the right to terminate the Contract as per Clause 12.1 & 12.2 of Section-III	The overall cap is very high and per standard practice cap the penalty @10% of QGR and amend the clause as follows: "*Note:- The overall Penalties (for Clause 1-A,B,C,D in Section-VIII) per quarter shall be capped at a maximum of ~~25%~~ **10%** of the respective Quarterly payment of Grand Total Value. In case penalty imposed on the contractor consecutively for two quarters reaches the maximum Penalty (i.e ~~25%~~ **10%** ~~)~~ then in such an eventuality ERNET India reserves the right to terminate the Contract as per Clause 12.1 & 12.2 of Section-III"*	No Change
102	128	Section VIII: Service Level Agreement during Operation & Maintenance F. Manpower Service Level Agreement:	Non-deployment of total manpower mentioned in the contract as per the date of joining Penalties for non-compliance Operation and Maintenance billing will be started only after minimum 75% deployment (atleast 1 manpower of each line item) of total Manpower as per contract. Further 0.5% of quarterly OPEX value per day will be deducted from due payments/ performance security for non-deployment of complete manpower	Request to limit the man power related non compliance penalty to the corresponding manpower payment only instead of complete OPEX value which is very high. Kindly amend the clause as follows: "*Penalties for non-compliance* *Operation and Maintenance billing will be started only after minimum 75% deployment (atleast 1 manpower of each line item) of total Manpower as per contract. Further ~~0.5% of quarterly OPEX value~~ per day manpower cost of the unavailable manpower ~~per day~~ will be deducted from due payments/ performance security for non-deployment of complete manpower "*	No Change

103	128	Section VIII: Service Level Agreement during Operation & Maintenance F. Manpower Service Level Agreement:	Sr. No-4 Penalties for non-compliance 0.5% of quarterly OPEX value for per day per manpower	Request to limit the man power related non compliance penalty to the corresponding manpower payment only instead of complete OPEX value which is very high. Kindly amend the clause as follows: " *~~0.5% of quarterly OPEX value for~~ per day* ***price*** *per manpower* ***for the no. of absent days*** "	No Change
104	128	Section VIII: Service Level Agreement during Operation & Maintenance F. Manpower Service Level Agreement:	Sr. No-5 Penalties for non-compliance Contractor shall arrange replacement of manpower during the leave of employee. 0.5% of quarterly OPEX value for per day per manpower, if no manpower arranged during the leave period of employee.	Request to limit the man power related non compliance penalty to the corresponding manpower payment only instead of complete OPEX value which is very high. Kindly amend the clause as follows: "*Contractor shall arrange replacement of manpower during the leave of employee. ~~0.5% of quarterly OPEX value for~~ per day* ***price*** *per manpower* ***for the no. of absent days*** *, if no manpower arranged during the leave period of employee* ."	No Change
105	128	Section VIII: Service Level Agreement during Operation & Maintenance F. Manpower Service Level Agreement:	Sr. No-6 Penalties for non-compliance Immediate replacement within 3 days/ cancellation of the contract with cancellation charges @ 5% of the contract value or as decided by ERNET India depending on the gravity of the act	The said deviation is beyond the control and we will be deploying manpower after thorough check The penalty is very high and hence request to amend the same as follows: "Immediate replacement within 3 days/ cancellation of the contract with cancellation charges @ 5% of the ~~contract value~~ **of the corresponding manpower cost** or ~~as decided by ERNET India~~ **mutual agreement** depending on the gravity of the act "	No Change
106	9	1. Notice Inviting Tender (hereinafter referred to as "NIT")	Only Class-I or Class-II Local Supplier are eligible to participate in the tender. Bidder must ensure that it complies with the Public Procurement (Preference to Make in India) Order 2017 (MII) (Letter no P45021/2/2017- (BE-II) dated 15.06.2017) of Department for Promotion of Industry and Internal Trade, (DPIIT - Public Procurement Section) as revised and amended from time to time until the date of submission of the bids by the bidders.	Kindly remove the clause for wide OEM participation	No Change
107	90	2.Scope of Work of Contractor	xiv. Operations and Maintenance (O&M) of existing IT infrastructure & solutions, equipment(s) i.e termed as exisiting IT Infra for new DC,DR & 300+ Remote Sites.	Kindly share the following details: 1. Existing Infra Details 2.Equipment's Warranty details 3. Equipment's End of Life details. Kindly share the Existing Partner Details.	Required information is attached as Annexure.
108	51	9.2 Place (destination/Location) of Delivery	DC and DR location is under finalisation and remote sites are spread across India where the Equipment are to be delivered have been stipulated in the Section IV – Bill of Material.	Kindly mention exact location details of existing DC & DR and remote location details.	DC & DR location is yet to be finalised. However DC/DR location will be tier-I/II cities of India. Further Remote locations are spreaded across India
109	90	2.Scope of Work of Contractor	x. To configure ILL, P2P , MPLS WAN links & respective IPSec Tunnels for all remote sites & Data Centre(s) under this bid. The ERNET India empanelled service provider will be providing the ILL, P2P , MPLS WAN links at remote locations . The sucessful bidder shall coodinate with service provider while configuring the equipment over MPLS WAN.	We understand that ILL, P2P, MPLS WAN link will be provided by ERNET Telecom/Internet Service provider. Current Bidder scope shall coordinate with ERNET TSP/ISP and they will be configuring the equipment over MPLS WAN. Kindly confirm. Kindly provide details of the existing network service provider.	Clause is Self Explanatory ; The equipment brought in this bid for installation at remote sites will be configured by Contractor only. PGCIL is the existing network service provider
110	90	2.Scope of Work of Contractor	Migration of 80 remote sites connected from existing DC, DR to new DC, DR	Kindly share the Existing 80 remote location details for migration from existing DC, DR to new DC, DR.	Remote Locations are spread across TIER-I / TIER-2 cities of India. Location details will be shared with successful contractor.

111	94	6. Role and Responsibilities of contractor at Remote Sites & its Integration	10) The power connection will be provided by end user. Thereafter, if any extension of power cable is required from power point to UPS/Rack or in case the RACK PDUs are not available in RACK, the same shall be in the scope of bidder.	We understand that customer wil be providing regulated UPS power supply so kindly request customer to provide power connection till Rack PDU.	Clause is Self Explanatory ;
112	93	5. High level Role and Responsibilities of contractor w.r.t existing IT infrastructure at Data Centers (DC/DR)& their Remote Sites:	4) Gather understanding of various deployed solutions such as AIM, EMS, PATS,DCIM, IT Helpdesk , AAA,AD,SSL VPN, PAM etc.	Kindly provide the details of existing AIM, EMS, PATS,DCIM.	Required information is attached as Annexure.
113	165	Form 12 Financial Bid (BoQ)	Interactive Video Wall- 2 Nos	Kindly clarify where we are going to deploy the Interactive Video Wall- 2 Nos since we understand that there is no command & Control Center mentioned in current bidder scope scope.	Video Wall will be installed at the NOC location in DC and DR
114	89	1.Project Overview	i.Setup of IT infrastructure in New DC and DR and at remote sites and therafterits Operation and Maintenance for two years.	Kindly share the following details: 1. What is the Total no. of New DC and DR and share the Location details. 2. What is the Total no of new Remote sites and share the location details. 3. Area of new DC and DR.	1. New DC - 1 , New DR - 1 ; Their locations is yet to be finalized & will be in Tier-I/Tier-II cities of India. 2. Total no of new Remote sites - 34 and will be in Tier-I/Tier-II cities of India. 3. Area of new DC and DR - for 100 Racks at new DC & 50 Racks for new DR + with an option to increase the 25% expansion of racks for future work.
115	91	4. High level Role and Responsibilities of contractor at New Data Centers (DC and DR)	Contractor shall submit DC-DR Rack layouts for Racking/Stacking of each equipment planned for supply as per BoM of DC and DR based on their power, cooling, space, and connectivity requirements. It needs to be submitted in first 2 weeks of issuance of contract for review and acceptance of ERNET India/CERT-In.	Kindly share the following details: 1. Kindly share the total no of Network, Server, storage rack at DC. 2. Kindly share the total no of Network, Server, storage rack at DR. 3. Kindly share the total no of Network, Server, storage rack at each Remote Location. 4. Kindly share the type of Rack for DC, DR and Remote Location.	1. Total no of Network, Server, storage rack at DC -100 Racks at DC 2. Total no of Network, Server, storage rack at DR -50 Racks at DR 3. For Remote Location Contractor needs to perform the Survey & One 4. Rack at each Remote Location with only a maximum of 2U space will be made available. 5. Standard sized 42-U rack will be provided.
116	91	4. High level Role and Responsibilities of contractor at New Data Centers (DC and DR)	Contractor shall submit DC-DR Rack layouts for Racking/Stacking of each equipment planned for supply as per BoM of DC and DR based on their power, cooling, space, and connectivity requirements. It needs to be submitted in first 2 weeks of issuance of contract for review and acceptance of ERNET India/CERT-In.	We understand that customer will be providing the following requirements in DC, DR and remote locations: 1. Civil & interior works like false floor and false ceiling etc. 2. ElectricalWorks (UPS for Rack equipment) and required Cabling, wiring and Earthing. 3. HVAC (PAC for Racks), and requirement Cooling for Command and Control Centre if any. 4. Safety & Security systems like FAS, FSS, BMS, ACS, WLD, RRS, CCTV. Kindly confirm Does redundant UPS power is available at DC, DR and remote location for Racks?	The colo services (Power,Cooling,Racks etc.) will be arranged by ERNET India. Yes. UPS power will be available at DC, DR and remote locations. However, at few remote locations, bidder needs to lay power cable to get the power from the UPS to the rack.
117	97	9. Acceptance Testing (AT)	It may be noted by bidder that VAPT to be done for entire setup . A Successful Vulnerability assessment (VA) and Penetration Testing (PT) report through a Third-party certified agency (CERT-In empanelled Security auditors) and Fixing of all identified Vulnerabilities and submission of “all clear” reports .	1. Please provide location-wise(DC/DR/Remote)number of Servers/Devices/IPs to be considered for scanning at AT Phase. 2. Please provide number of internal & external applications need to be scanned at AT Phase.	1. Based on the BoQ for DC + DR+ Remote Locations, Bidder may calculate the required information. 2. Regarding VAPT, kindly refer Page-98, 99 of tender document

118	102	12. Scope of Work for Operation & Maintenance	Contractor shall carry out Vulnerability assessment (VA) and Penetration Testing (PT) using certified tool through a Third-party certified agency certified by CERT In of complete IT infrastructure once in a year and shall submit report to ERNET India/CERT-In.	1. Please provide location-wise(DC/DR/Remote)number of Servers/Devices/IPs to be considered for scanning at O&M Phase. 2. Please provide number of internal & external applications need to be scanned at O&M Phase. 3. Please elaborate the VA & PT process expected to be conducted.	Based on the BoQ for DC + DR+ Remote Locations, Bidder may calculate the required information. Regarding VAPT, kindly refer Page-98, 99 of tender document
119	47	6 Scope of work, Project Management and Technical Specifications	**6.4 Warranty for equipments/solutions procured via this tender at New DC-DR & remote sites** 2) The warranty period shall start from the respective effective date(s) of successful acceptance by ERNET India of each milestone.	**Kindly request to amend the clause as** 2) The warranty period for all items shall start from the date of delivery.	No Change
120	29	Section II: Instructions to Bidders (ITB) 11.3.3 Evaluation of Conformity to Bill of Material and Technical Specifications and other parameters specified in Tender document	Further, TEC may ask the bidder to bring any selected Equipment(s)/items, sub items of their quoted equipment(s) for technical evaluation/demonstration at ERNET India or any other location decided by TEC in specified time limit i.e. within **Five days** or as mentioned in communication sent. In case, bidder fails to bring their quoted equipment(s)within the stipulated time, for whatever reasons, their bid will not be considered for further evaluation.	Five days time to for procuring and setting up any device POC is too short. Kindly increase the duration to three weeks and amend the clause as follows: "Further, TEC may ask the bidder to bring any selected Equipment(s)/items, sub items of their quoted equipment(s) for technical evaluation/demonstration at ERNET India or any other location decided by TEC in specified time limit i.e. within ~~Five days~~ **3 weeks** or as mentioned in communication sent. In case, bidder fails to bring their quoted equipment(s)within the stipulated time, for whatever reasons, their bid will not be considered for further evaluation."	No Change
121	179	BIDDING FORMS Annexure-1 (Technical Specifications)	l. Only the Manpower on OEM payrolls shall perform network planning, designing, implementation, integration and testing/validation for all Networking equipment(s) i.e. only direct OEM payroll manpower would be allowed to work on the project's designing, implementation & testing phase. An undertaking for same shall be provided.	The said clause will inflate the project cost and will impact the overall project commercials as well as timeline. Further the OEMs are not contractually bound and the bidder is liable for the overall scope. Hence request to allow OEM authorized personnel and amend the clause as follows: *"l. Only the Manpower on OEM payrolls or* ***OEM authorized personnel*** *shall perform network planning, designing, implementation, integration and testing/validation for all Networking equipment(s) i.e. only direct OEM payroll manpower or* ***OEM authorized Manpower*** *would be allowed to work on the project's designing, implementation & testing phase. An undertaking for same shall be provided."*	No Change
122	179	BIDDING FORMS Annexure-1 (Technical Specifications)	i. Quoting Multiple OEM for single product is not allowed.	In order to submit the most competitive techno commercial offer request to allow bidder to quote multiple make and model that can be finalized during design stage. Kindly amend the clause.	No Change
123	93	5. High level Role and Responsibilities of contractor w.r.t existing IT infrastructure at Data Centers (DC/DR)& their Remote Sites:	Existing IT infrastructure housed at DC, Bengaluru & DR, Mohali which are having IT solutions, networking and security equipments, servers etc. in 100 Racks & 50 Racks respectively. There are approximately 380+ remote sites.	Kindly mention below details regarding existing infra: a.Make & Model Details b.Currently working or out of services status c.Warranty period	Required information is attached as Annexure.
124	18	4 Preferential Policies	4.1 Applicability of Make in India (MII) Policy	Kindly remove the clause for wide OEM participation	No Change
125	18	4 Preferential Policies	4.2 Eligibility to participate and purchase preference	Kindly remove the clause for wide OEM participation	No Change
126	18	4 Preferential Policies	4.3 Classification of Procurement and purchase preference methodology:	Kindly remove the clause for wide OEM participation	No Change

127	19	4 Preferential Policies	4.4 Verification of local content and violations:		No Change
128	96	7. Role and Responsibilities of Contractor i.r.o AAA,AD,EMS and related software applications	18) It is responsibility of contractor to maintain the backup of EMS for at least one year which includes data, configuration, alarms, performance etc. Assets data must be maintained throughout. 19) Contractor may choose the best and optimized design to deploy the various sought applications / solutions on Hardware. The contractor must ascertain the hardware & other requirements of these servers as per the sought criticality, HA, scope of work, total users, backup, total concurrent users, amount of data to be saved per server per application and other factors. (Backup period is 01 Year. Contractor needs to arrange the equipments to suffice the backup requirements asked in the bid.)	As per RFP statement,it is understood that bidder need to propose a backup solution,but same has not mentioned in the Bill of material,kindly provide detail technical specification along with quantity to be proposed.	Backup period requirement is 01 Year. Bidders need to consider the required infra to support this requirement.
129	104	12.3 Installation/configuration and reconfiguration/rollback of equipment	2) Contractor shall keep backups of all the versions of equipment configuration.	Kindly mention for how many days backup need to be considered here.	Backup period requirement is 01 Year. Bidders need to consider the required infra to support this requirement.
130		Utility Server (Category 05)		Kindly mention types of Virtualization that need to be considered here.	Vmware, Hyper V, KVM
131	89	2. Scope of Work of Contractor	ix. Support the installation of third party Operating System and applications on the commissioned computing infrastructure.	As per RFP statement,it is understood that only installation support is in the scope of bidder.Supply of OS is in customer's scope,kindly confirm	Installation of OS , Facilitation of any configuration changes w.r.t OS, Supporting remote OS installation to authorized & approved members, network reachability or installation of any special purpose scripts/softwares will be the minimum responsbility w.r.t query asked.
132	95	2. Scope of Work of Contractor	13) Integration with Email Gateways/servers, SMS Gateways. Please note that Supplied EMS must have the capability to get integrated with standard solutions available in market w.r.t Email Gateways/servers, SMS Gateways.	Supply of SMS and Email gateway is in customer's scope,bidder will only be responsible for integration.Kindly confirm	Yes
133	85	Section VI: Qualification Criteria A. Bidder's Qualification Criteria	7. The bidder must have following professional* working on its payroll a. Prince-2/ PMP - 5 numbers b. CISA/CISSP/CISM - 2 numbers c. CDCP - 2 numbers d. CCIE-Sec/JNCIE-Sec - 1 numbers e. CCIE-ENT/JNCIE-ENT - 1 numbers f. CCIE-DC/CCNP-DC/JNCIE-DC/JNCIP-DC - 2 numbers g. CCNP-Sec/ JNCIP-Sec/Fortigate NSE-4/PCNSE - 3 numbers h. CCNP-ENT/ JNCIP-ENT - 3 numbers *Professionals must be regular employee of bidder as on date of submission of this bid. Fixed term contract/contractual employee will not be accepted. Valid certificate(s) of above professional to be submitted along with the bid with covering letter of Director HR of bidder's organisation.	We request to authority please amend this clause as mention below 7. The bidder must have following professional* working on its payroll in minimum two Certification categories out of 8 Category (a to h) as mentioned below. a. Prince-2/ PMP - 5 numbers b. CISA/CISSP/CISM - 2 numbers c. CDCP - 2 numbers d. CCIE-Sec/JNCIE-Sec - 1 numbers e. CCIE-ENT/JNCIE-ENT - 1 numbers f. CCIE-DC/CCNP-DC/JNCIE-DC/JNCIP-DC - 2 numbers g. CCNP-Sec/ JNCIP-Sec/Fortigate NSE-4/PCNSE - 3 numbers h. CCNP-ENT/ JNCIP-ENT - 3 numbers *Professionals must be regular employee of bidder as on date of submission of this bid. Fixed term contract/contractual employee will not be accepted. Valid certificate(s) of above professional to be submitted along with the bid with covering letter of Director HR of bidder's organisation and **Bidder needs to submit undertaking from HR Head that bidder shall provide the balance required certified profiles for the resources as per the category mentioned above at the time of Contract signing.**	Kindly refer to respective updated clause in Annexure-B

134	18	4.2 Eligibility to participate and purchase preference	Only Class-I and Class-II local Suppliers shall be eligible to participate in this bid. Local content percentage for qualifying as Class-I and Class-II local Suppliers shall be calculated and declared by the respective bidders on the basis of Letter no P45021/2/2017- (BE-II) dated 15.06.2017 Public Procurement (Preference to Make in India) Order 2017" (MII) of Department for Promotion of Industry and Internal Trade, (DPIIT - Public Procurement Section); as revised and amended time to time and also clarifications and FAQ issued by DPIIT in this respect from time to time.	Kindly remove the MII clause. Global competitors should be allowed to participate in such upscale projects for which we hold the capability to perform efficiently and serve better.	No change
135	52	.....	Timeline for Delivery, Installation, testing, commissioning & Acceptance Acceptance by ERNET India for Complete Milestone-3 and issuance of acceptance certificate subject to completion of complete work as per tender.	Kindly increase the delivery timeline to 6 months.	No Change
136	20	5.3 Goods and Services Tax (GST)	Bidder/Contractor undertakes that in case of non-compliance by the Bidder(s) of the GST provisions which results in blockage/reversal of any input tax credit to ERNET India, Bidder/Contractor shall be liable to indemnify the ERNET India any such loss of input credit including interest, penalty and all incidental expenses incurred by ERNET India. Such indemnification may also be by way of invocation of any security deposit, deduction from any payment that ERNET India has to make to the Bidder/Contractor, as per the discretion of the ERNET India.	ERNET should intimate any discrepency in case of non compliance of GST provisions before two months from statutory timeline allowed under GST for amendments. Without informing discrepency the amount shall not be recovered	It is agreed that ERNET India will intimate the discrepancy within 30 days from the date of coming of discrepancy in its notice. Bidder may see if any time window is available to it for compliance with the law. Thereafter, only ERNET India will initiate recovery proceedings.
137	20	5.3 Goods and Services Tax (GST)	Along with the invoice; Bidder/Contractor would be required to submit relevant documentary evidence to the effect that invoice submitted was issued either through e-Invoice system of GST or has been updated on GSTN portal using Invoice Furnishing Facility (IFF).	GSTR 1 filing screenshot would be provided as documentary evidence	We agree.
138	21	5.3 Goods and Services Tax (GST)	In case, in future any GST liability is required to be borne by ERNET India; which was the responsibility of the Bidder/Contractor, then the same shall be claimed from the Bidder/Contractor by way of raising debit notes.	ERNET should intimate any such GST liability before raising any debit note in this regard	We agree.
139	21	5.3 Goods and Services Tax (GST)	ERNET India reserves the right to ask the Bidder/Contractor to submit relevant documents to ensure that they are GST compliant and in such a case Bidder/Contractor shall forthwith provide all such documents as may be required by ERNET India.	Relevant documents as prescribed under GST legislation would be shared subject to necessary internal approvals.	No Change

140	30	12.1.1 Right to Vary Quantities	Right to Vary Quantities: i. ERNET India reserves the right to increase/decrease the quantities to be ordered up to 25 % of sum total of final bid value; at the time of placement of contract. ii. Keeping in the view of the fact that the project requirements are dynamic and ever changing therefore ERNET India reserves the right to increase the ordered value by up to 25% of sum total of final bid value; till the completion of O&M activities, without any reference to the intial ordered quantities. iii. Successful Bidder/ Contractor is bound to accept the orders accordingly, failing which; ERNET India may declare this as an event of default and consequences for event of default will be applicable.	Right to Vary Quantities: ERNET India reserves the right to decrease the quantity to be ordered up to 25 percent of final bid value at the time of placement of contract. The ERNET India also reserves the right to increase the ordered quantity by up to 25% of the final bid value at the time of placement of contract or within one (1) year period from the issuance of the contract. It may be noted by the bidder that the prices of SFPs and Patch cords quoted in the bid shall remain valid for the complete duration of contract period. Successful Bidder/ Contractor is bound to accept the orders accordingly failing which; ERNET India may declare this as an event of default and consequences for event of default will be applicable.	No Change
141	40	5.5 Indemnities for breach of IPR Rights or from other issues	Indemnities for breach of IPR Rights or from other issues: 1) the contractor shall indemnify and hold harmless, free of costs, the ERNET India and its employees and officers from and against all suits, actions or administrative proceedings, claims, demands, losses, damages, costs, and expenses of any nature, including attorney's fees and expenses, which may arise in respect of the Equipment provided by the contractor under this Contract, as a result of any infringement or alleged infringement of any patent, utility model, registered design, copyright, or other Intellectual Proprietary Rights (IPR) or trademarks, registered or otherwise existing on the date of the contract arising out of or in connection with:	Indemnities for breach of IPR Rights or from other issues: 1) the contractor shall indemnify and hold harmless, free of costs, the ERNET India ~~and its employees and officers~~ from and against all direct suits, actions or administrative proceedings, claims, demands, losses, damages, costs, and expenses of any nature, including attorney's fees and expenses, which may arise in respect of the Equipment provided by the contractor under this Contract, as a result of any infringement or alleged infringement of any patent, utility model, registered design, copyright, or other Intellectual Proprietary Rights (IPR) or trademarks, registered or otherwise existing on the date of the contract arising out of or in connection with:	No Change
142	41	5.5 Indemnities for breach of IPR Rights or from other issues	4) The contractor shall be solely responsible for any damage, loss or injury which may occur to any property or to any person by or arising out the execution of the works or temporary works or in carrying out of the contract otherwise than due to the matters referred to in this agreement hereinbefore. The bidder would ensure for observance of all labour and other laws applicable in the matter and shall indemnify and keep indemnified the ERNET India, end users/ its customers against the effect of non-observance of any such laws.	4) The Contractor shall be solely responsible for any direct damage, loss or injury which may occur to any property or to any person by or arising out the execution of the works or temporary works or in carrying out of the contract otherwise than due to the matters referred to in this agreement hereinbefore . The contractor would ensure for observance of all labour and other laws applicable in the matter and shall indemnify and keep indemnified the ERNET India, end users/ its customers against the effect of nonobservance of any such laws.	No Change

143	46	6.4 Warranty for equipments/solutions procured via this tender at New DC-DR & remote sites	Warranty The Contractor shall arrange for free Onsite comprehensive maintenance for a period of warranty from the date/dates of acceptance of the project milestone wise with regard to rectification/removal of defects if any observed during this period . If the Contractor does not arrange to rectify the defects observed during the maintenance period within a reasonable time (5 days) the ERNET India/End user shall be at liberty to get such defects rectified at the cost and risk of the Contractor in addition to levying of penalties.	11) The Contractor shall arrange for free Onsite comprehensive maintenance for a period of warranty from the date/dates of acceptance of the project milestone wise with regard to rectification/removal of defects if any observed during this period. If the Contractor does not arrange to rectify the defects observed during the maintenance period within a reasonable time (10 days). the ERNET/End user shall be at liberty to get such defects rectified at the cost and risk of the Contractor in addition to levying of penalties. In no event should such cost or liability of the Contractor will exceed the amount or value of the defected portion of Contract.	No Change
144	55	9.5 Extension of Delivery Period and Liquidated Damages:	2) Liquidated Damages (LD): a. If the Contractor fails to meet the prescribed timelines for respective milestones due to any reason whatsoever then in such a case ERNET India would be entitled to impose the Liquidated Damages for the delay: i. Delay in Delivery of the Equipments (only for DC & DR): @ 0.5 % of the value of delayed equipments (of the respective milestones); per week or part of the week of delayed period. ii. Delay in Commissioning & offering for acceptance (for DC, DR & Remote Sites): @ 0.5 % of the sum total value of all the equipments for respective milestone; per week or part of the week of delayed period. Note: Overall Liquidated Damages shall be restricted to 10% of the total contract value. While calculating LD; GST will be excluded from the value on which LD is calculated; thereafter GST may be charged (if applicable) on the LD value as per S.No. 4 clause 5.3 of Section II of this document. In case, delay beyond 20 weeks, ERNET India may initiate termination for default and take remedial action(s) accordingly as per GCC Clause 12.1.	2) Liquidated Damages (LD): If the Contractor fails to complete delivery, installation, testing, commissioning, training, acceptance etc. of equipment(s) as per timelines specified in the contract, then in such a case ERNET India would be entitled to impose the Liquidated Damages for the delay @ 0.5% of the value of the delayed deliverables ~~value of total equipment(s)~~ at non-commissioned sites per week or part of the week of delayed period. Liquidated Damages shall not exceed 10% of the value of the delayed deliverables ~~total contract value~~. In case, delay beyond 20 weeks, ERNET India may initiate termination for default and take remedial action(s) accordingly as per GCC Clause 12.1.	Kindly refer to respective updated clause in Annexure-B
145	59	12.1.2 Notice for Default:	Notice for Default: As soon as a breach of contract is noticed, a show-cause 'Notice of Default' shall be issued to the contractor, giving two weeks ' notice, reserving the right to invoke contractual remedies. After such a show-cause notice, all payments to the contractor would be temporarily withheld to safeguard needed recoveries that may become due on invoking contractual remedies.	Notice for Default: As soon as a breach of contract is noticed, a show-cause 'Notice of Default' shall be issued to the contractor, giving thirty (30) days ~~two weeks~~ ' notice, reserving the right to invoke contractual remedies. ~~After such a show-cause notice, all payments to the contractor would be temporarily withheld to safeguard needed recoveries that may become due on invoking contractual remedies.~~	No Change

146	60	12.1.2 Notice for Default:	1) Notice for Termination for Default: Notice for Termination for Default: In the event of unsatisfactory resolution of 'Notice of Default' within two weeks of its issue as per sub-clause above, the ERNET India, if so decided, shall by written Notice of Termination for Default sent to the contractor, terminate the contract in whole or in part, without compensation to the contractor.	1) Notice for Termination for Default: In the event of unsatisfactory resolution of 'Notice of Default' within thirty (30) days ~~two weeks~~ of its issue as per sub-clause above, the ERNET India, if so decided, shall by written Notice of Termination for Default sent to the contractor, terminate the contract in whole or in part, ~~without compensation to the contractor.~~	No Change
147	60	12.1.4 Contractual Remedies for Breaches/Defaults or Termination for Default	If there is an unsatisfactory resolution of the issues raised in the 'Notice of Default' within the period specified in the notice, then ERNET India may take any one; or more of the following contractual remedies. 1) Temporary withhold payments due to the contractor till recoveries due to invocation of other contractual remedies are complete. 2) Recover liquidated damages for delays. 3) Encash and/ or Forfeit performance or other contractual securities. 4) Debar the contractor from participation in future procurements as follows: 5) ERNET India may debar the contractor or any of its successors from participating in any Tender Process undertaken by it for a period not exceeding two years commencing from the date of debarment. Terminate contract for default, fully or partially including its right for Risk-and-Cost Procurement as per following sub-clause. 6) Risk and Cost Procurement: In addition to termination for default, the ERNET India shall be entitled, and it shall be lawful on its part, to procure Equipment and services similar to those terminated, with such terms and conditions and in such manner as it deems fit at the "Risk and Cost" of the contractor. Such 'Risk and Cost Procurement' will be contracted within nine months from the breach of Contract. The Contractor shall be liable for any loss which the ERNET India may sustain on	If there is an unsatisfactory resolution of the issues raised in the 'Notice of Default' within the period specified in the notice, then ERNET India may take any one; or more of the following contractual remedies. 1) Temporary withhold payments due to the contractor till recoveries due to invocation of other contractual remedies are complete. 2) Recover liquidated damages for delays. 3) Encash and/ or Forfeit performance or other contractual securities. ~~4) Debar the contractor from participation in future procurements as follows:~~ ~~5) ERNET India may debar the contractor or any of its successors from participating in any Tender Process undertaken by it for a period not exceeding two years commencing from the date of debarment.Terminate contract for default, fully or partially including its right for Risk-and-Cost Procurement as per following sub-clause.~~ 6) Risk and Cost Procurement: In addition to termination for default, the ERNET India shall be entitled, and it shall be lawful on its part, to procure Equipment and services similar to those terminated, with such terms and conditions and in such manner as it deems	No Change
148		.....	Limitation of Liability: Except in cases of criminal negligence or wilful misconduct, the aggregate liability of the contractor to the ERNET India, whether under the contract, in tort or otherwise, shall not exceed the total Contract value, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment, or to any obligation of the contractor to indemnify the ERNET India concerning IPR infringement.	Limitation of Liability: Except in cases of criminal negligence or wilful misconduct, the aggregate liability of the contractor to the ERNET India, whether under the contract, in tort or otherwise, shall be limited to the applicable purchase order /invoice / statement of work ~~not exceed the total Contract value~~, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment, or to any obligation of the contractor to indemnify the ERNET India concerning IPR infringement.	No Change

149	61	12.2.1 Notice for Determination of Contract	12.2.1 Notice for Determination of Contract 1) The ERNET India reserves the right to terminate the contract, in whole or in part for its (the ERNET India's) convenience, by serving written 'Notice for Determination of Contract' on the contractor by giving sixty (60) days prior notice during the currency of the contract. The notice shall specify that the termination is for the convenience of the ERNET India of the contract. The notice shall also indicate inter-alia, the extent to which the contractor's performance under the contract is terminated, and the date with effect from which such termination shall become effective.	12.2.1 Notice for Determination of Contract: 1) The ERNET India reserves the right to terminate the contract, in whole or in part for its (the ERNET India's) convenience, by serving written 'Notice for Determination of Contract' on the contractor by giving sixty (60) days prior written notice ~~at any time~~ during the currency of the contract. The notice shall specify that the termination is for the convenience of the ERNET India of the contract. The notice shall also indicate inter-alia, the extent to which the contractor's performance under the contract is terminated, and the date with effect from which such termination shall become effective.	No Change
150		.....	** Termination right was not provided to Contractor in case of material breach by ERNET. We suggest incorporation of said clause.**	Termination for Material Breach: In the event ERNET materially breaches any term of the Contract, which breach is not cured within 30 thirty (30) days after written notice specifying the breach is given to the ERNET, Contractor may (i) terminate the Contract by giving written notice to the other party and (ii) pursue any and all remedies available subject to the provisions of the Contract.	No Change
151		.....	**Termination right was not provided to Contractor in case ERNET goes inslovent/bankrupt. We suggest incorporation of said clause.**	Termination for Insolvency: Contractor may terminate this Contract immediately with notice to the ERNET if, ERNET becomes insolvent or bankrupt, makes a general assignment for the benefit of, or enters into any arrangement with, creditors, files a voluntary petition under any bankruptcy, insolvency, or similar law, or has proceedings initiated under any such laws.	No Change
152	57	6. The payment term	In respect of DC and DR equipment (s), 50% of the value of equipment(s) delivered at DC and similarly 50% of the value of equipment(s) delivered at DR shall be released only after submission of BG equivalent to the amount which is to be released. The BG should be valid for a minimum period of 6 months (with a claim period of additional 3 months). BG must be extendable till the successful completion of rack mounting & Power On Self Test (POST) of active equipments	Please amend the clause to: In respect of DC and DR equipment (s), 75% of the value of equipment(s) delivered at DC and similarly 75% of the value of equipment(s) delivered at DR shall be released only after submission of BG equivalent to the amount which is to be released. The BG should be valid for a minimum period of 6 months (with a claim period of additional 3 months). BG must be extendable till the successful completion of rack mounting & Power On Self Test (POST) of active equipments	No Change
153	57	6. The payment term	d. In respect of equipment at remote sites, 80% of the total value of items will be made after successful delivery, installation, integration, commissioning and acceptance of the individual remote sites.	Please amend the clause to: d. In respect of equipment at remote sites, 70% of the total value of items will be made after successful delivery and 10 % on installation, integration, commissioning and acceptance of the individual remote sites.	No Change
154	57	6. The payment term	c. In respect of equipment (s) at DC and DR, additional 30% of the total value of items will be made after successful installation, integration, commissioning and acceptance as per the respective milestone(s).	Please amend the clause to: c. In respect of equipment (s) at DC and DR, additional 10% of the total value of items will be made after successful installation, integration, commissioning and acceptance as per the respective milestone(s).	No Change

155	49	14) SLA during warranty period and penalties for breach thereof:	The overall Penalties for non-adherence with the SLA of warranty support (during 3rd , 4th & 5th year of warranty period) per quarter shall be capped at a maximum of 25% of the respective Quarterly payment (CAPEX). In case penalty imposed on the contractor consecutively for two quarters reaches the maximum Penalty (i.e 25%) then in such an eventuality ERNET India reserves the right to terminate the Contract as per Clause 12.1 & 12.2.	We request to cap the maximum penalty to 5% of the respective quarterly payment for relevant component/software as 25% is very high.	No Change
156	125	1 Service Level during Operation & Maintenance period for Equipment: A. For Equipment at DC & DR and Remote Sites (procured via this bid):	1) At Data Center (New DC & New DR) and remote sites, for faults in any of the equipment, SLA penalty @ 0.25 % of the equipment(s) cost per day or part thereof will be deducted beyond 24 hours from the reporting time of fault, then penalty @ 0.5 % of equipment cost per day will be deducted. SLA penalty of Rs. 2000/- per day beyond 24 hours will be charged for equipment(s) (active and passive component) whose price could not be derived (e.g Intelligent Cables) from the price bid. 2) In case of downtime caused due to core networking equipment* failure supplied by bidder, a penalty of Rs. 1,00,000/- for every six hour or part thereof will be imposed. This penalty will be over and above any other applicable penalties. 3) Bidder may keep spare equipment/ parts etc. to keep the services running and minimize the fault duration & penalties. 4) No penalty will be imposed for downtime asked by the bidder for preventive maintenance, schedule maintenance, patch upgradation etc. However, any of these activity shall be done only in off peak hours and with due permission from ERNET India/CERT-In. 5) In case, SLA breach happens due to the technical dependency on the ERNET India/CERT-In, the penalties would not be applicable on Contractor. 6) During O&M, bidder must do preventive maintenance (PM) in every quarter for DC & DR and yearly for remote sites. If PM is missed as per	Please amend the clause to: 1) At Data Center (New DC & New DR) and remote sites, for faults in any of the equipment, SLA penalty @ 0.10 % of the equipment(s) cost per day or part thereof will be deducted beyond 24 hours from the reporting time of fault, then penalty @ 0.5 % of equipment cost per day will be deducted. SLA penalty of Rs. 1000/- per day beyond 24 hours will be charged for equipment(s) (active and passive component) whose price could not be derived (e.g Intelligent Cables) from the price bid. 2) In case of downtime caused due to core networking equipment* failure supplied by bidder, a penalty of Rs. 50,000/- for every six hour or part thereof will be imposed. This penalty will be over and above any other applicable penalties. 3) Bidder may keep spare equipment/ parts etc. to keep the services running and minimize the fault duration & penalties. 4) No penalty will be imposed for downtime asked by the bidder for preventive maintenance, schedule maintenance, patch upgradation etc. However, any of these activity shall be done only in off peak hours and with due permission from ERNET India/CERT-In. 5) In case, SLA breach happens due to the technical dependency on the ERNET India/CERT-In, the penalties would not be applicable on Contractor. 6) During O&M, bidder must do preventive maintenance (PM) in every quarter for DC & DR and yearly for remote sites. If PM is missed as per defined frequency, the same	No Change
157	83	Sec VI, Clause A.2	The minimum average annual audited financial turnover of the bidder during the last three years (FY 21-22,22-23,23-24), should not be less than Rs.700 Crore.	We request you to allow Parent company turnover to be considered for qualification	**Not Allowed**
158	83	Sec VI, Clause A.3	Bidder should have experience of successful implementation of similar project(s) in Central/State Government/ Govt. undertakings/ UT's/Autonomous Bodies/Public listed companies/reputed Private organisation in India as: Single order of Rs. Rs.500 Crore or more; OR Two orders each having minimum of Rs. 250Crore of estimated cost or more; OR Three orders each having minimum of Rs. 200Crore of estimated cost or more	We request you to allow Parent experience credentials to be considered for qualification.	**Not Allowed**

159	83	Sec VI, Clause A.4	Bidder should have experience of successful implementation of data center with leaf and spine architecture in Central/State Government/ Govt. undertakings/ UT's/Autonomous Bodies/Public listed companies/reputed Private organisation in India as Single order of Rs. 100 Crore or more; OR Implemented 50 Rack with leaf and spine architecture or more;	We request you to allow Parent experience credentials to be considered for qualification.	**Not Allowed**
160	51	Sec III, Clause 9.1	The effective date of the contract shall be the date on which it has been issued by ERNET India on GeM Portal. The dates of deliveries shall be counted from the date of contract	We undertand that T is a mutually signed date of contract agreement signed between ERNET n Bidder . Kindly explain	T is date of issue of contract on GeM portal.
161	52	Sec III, Clause 9.3.6	Delivery of the Equipments at DC : T +8 weeks	As per our understanding, the OEMs require a minimum of 16 weeks for the delivery of the equipment. We kindly request an extension of the delivery timeline to accommodate this.	Kindly refer to respective updated clause in Annexure-B
162	53	Sec III, Clause 9.3.6 , Point No. 10	O&M of Existing DC, DR and Remote sites: To begin within 3 months from date of instructions issued by ERNET India/CERT-In in this regard	O&M of Existing DC, DR and Remote sites shall begin from the date of acceptance(FAT) issued by ERNET India/CERT-In. Request to amend the clause accordingly.	No Change
163	55	Sec III, Clause 9.5 , Point No. 2 (i)	Delay in Delivery of the Equipment's (only for DC & DR): @ 0.5 % of the value of delayed equipments (of the respective milestones); per week or part of the week of delayed period.	As this is a high value project, request to amend the Liquidated damages (LD) @ 0.25% of the value of delayed equipments (of the respective milestones); per week or part of the week of delayed period.	Kindly refer to respective updated clause in Annexure-B
164	55	Sec III, Clause 9.5 , Point No. 2 (ii)	Overall Liquidated Damages shall be restricted to 10% of the total contract value.	As this is a high value project, request to restrict overall Liquidated damages to a maximum of 10 % of delayed equipments (of the respective milestones); per week or part of the week of delayed period.	Kindly refer to respective updated clause in Annexure-B
165	57	Sec III, Clause No. 10, Point No. 6.b	Payment Terms : In respect of DC and DR equipment (s), 50% of the value of equipment(s) delivered at DC and similarly 50% of the value of equipment(s) delivered at DR shall be released only after submission of BG equivalent to the amount which is to be released. The BG should be valid for a minimum period of 6 months (with a claim period of additional 3 months). BG must be extendable till the successful completion of rack mounting & Power On Self Test (POST) of active equipments	We request you to release the 50% payent of the delivered items at the time of delivery wo any submission of BG for equivalent value. Bidder is already submiiting PBG for the performance of contract. Hence an additional BG requirement becomes extra burden.	No Change
166	71	Sec IV, BoM: PART-C(OPEX)	Manpower at contractor Premises, Point No. 45 to Databases GeoIP, VPN Services, Point No. 59	We understand that O&M is for a period of 2 years i.e 24 months. Kindly clarify 36 months mentioned for PART-C(OPEX)\, Point No. 45 to 59	Few of the members are required from Implementation Phase hence its 36 months for them.
167	72	Sec IV, BoM: PART-C(OPEX)	O&M costs for exisisting remote sites, Point No. 50	Kindly clarify if bidder needs to provide O&M for existing 380 remote sites aswell ?	O&M will be required for all 380 existing sites and 34 new remote sites
168	72	Sec IV, BoM: PART-C(OPEX)	O&M costs for New remote sites, Point No. 51	We undertand that the number of new Remote sites is 100 as per the RFP. Please clarify the count for 34 nos.	New Remote Sites are 34 in this project , however 380 remote sites will be there from existing project. So for better clarity - O&M for 380 & 34 remote sites is required.
169	84	Sec VI, Clause No. A, Point No. 5	Note i.r.o clause 4,5&6- Bidder shall provide relevant copies of the customer purchase orders in support of scope of work, deliverables, project value and satisfactory work completion certificate from client. Bidder shall also provide Name, Address, email and contact no. of organization whose Purchase orders are submitted by Bidder. Order Completion date/date(s) should fall between 01/11/2019 to 31/10/2024.	Kindly allow the bidder to submit a CA certificate w.r.t. timely delivery of delivered portion, support quality and technical expertise of manpower deployed. Wherever completion certificate is not available kindly consider CA certified letter for completion.	Kindly refer to respective updated clause in Annexure-B

170	60	Sec III, Clause No. 12.1.3, Point No. 1	Notice for Termination for Default: Default: In the event of unsatisfactory resolution of 'Notice of Default' within two weeks of its issue as per sub-clause above, the ERNET India, if so decided, shall by written Notice of Termination for Default sent to the contractor, terminate the contract in whole or in part, without compensation to the contractor.	Kindly amend the Notice for Termination for Default as 60 days i.e. In the event of unsatisfactory resolution of 'Notice of Default' within 60 days of its issue as per sub-clause above, the ERNET India, if so decided, shall by written Notice of Termination for Default sent to the contractor, terminate the contract in whole or in part, without compensation to the contractor.	No Change
171	61	Sec III, Clause No. 12.1.5	12.1.5 Limitation of Liability Except in cases of criminal negligence or wilful misconduct, the aggregate liability of the contractor to the ERNET India, whether under the contract, in tort or otherwise, shall not exceed the total Contract value, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment, or to any obligation of the contractor to indemnify the ERNET India concerning IPR infringement.	As this is high value contract , so limitation of liability should be limited to undelivered portions only for the remaining duration of contract and neither party shall be liable to the other party for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits, interest costs.	No Change
172	61	Sec III, Clause No. 12.2.1, Point No. 1 - 4	Termination for Default/ Convenience of ERNET India: Notice for Determination of Contract	We request to remove this clause from RFP TnCs as termination basis convenience is not pro business. This project require heavy investments and should see its complete tenure. Such clause is not applicable in current business scenario.	No Change
173	89	Scope of Work of Contractor	The overall scope of the Contractor/System Integrator (SI) to be selected under this tender is as follows	Please confirm if these three names (Bidder, Contractor and System Integrator) refers to same entity ?	Yes. The bidder who wins the bid ; to whom the contract is awarded will be termed as Contractor/SI
174	91	High level Role and Responsibilities of contractor at New Data Centers	ERNET India is in the process of finalizing Data Center operator for Co-location services and expected to be finalize soon. Thereafter, contractor shall perform following activities	1. Please clarify that colocation sites, including rack space, power, and cooling etc. are out of scope for the bidder/contractor. 2. Please specify the scope of services regarding the selection of a colocation operator, as we understand this is also out of the scope of bidder.	Clause is self explanatory
175	89	Scope of Work	Note: It may be noted that the Operating System and other core software applications in servers to be supplied under this tender	We have noted that details regarding Operating System licensing details/types are not included in the RFP. Please specify whether these should be included as separate line items in the Commercial Bill of Quantities (BoQ).	Clause is self explanatory
176	102	Scope of Work for Operation and Maintenance	Operations, maintenance and management of all IT components (Hardware and software) and related services for the equipment installed as per BoM at DC, DR & Remote sites.	Please clarify that operations and maintenance (0&M) responsibilities pertain only to the equipment listed in the BoQ, and that any application related operations and maintenance (0&M) are out of scope for the bidder.	Clause and self explanatory, Further application (not supplied by the bidder) related software based operations and maintenance (O&M) are out of scope for the bidder.
177	124	Service Level Agreement during Operation & Maintenance	Service Level during Operation & Maintenance period for Equipment:	Please provide SLA details for each service included in the proposal.	Clause is self explanatory
178	168	Form 12 Financial Bid (BoQ)	Refers to Intelligent Cabling for 100 Racks at DC and 50 Racks at DR .	Please clarify, Will you be providing rack specifications (dimensions, power ratings, etc.), or should the bidder account for these in their proposal?	Rack & iPDU will be provided as a part of Colocation services provided by ERNET India/CERT-In
179	90	Sect VII-4-vi	Contractor needs to plan, co-ordinate with various stakeholders and execute DC-DR drills .	Please clarify the number of Disaster Recovery drills required and this involves only New DC and New DR sites ?	Needs to be planned in advance along with ERNET India & CERT-In with selected bidder for New DC & DR only.
180	107	12.8	All the critical applications of DC shall be setup and configured in the Disaster Recovery (DR).	Please clarify how many critical applications will be involved in this project.	Critical applications include all services running in DC and DR supplied as a part of this bid.
181	104	12.2 Preventive Maintenance Services	The Contractor shall ensure preventive maintenance (PM) services for all the IT equipment installed at the DC & DR at least once in every six months and for Remote Sites on per year basis.	Please clarify if PMS is only for new DC and new DR sites only and it excludes all remote sites(new and existing) and existing infrastructure.	PMS will be required for new & exsisting (DC,DR & Remote Sites)

182	48	Sect 6.4-14-ii	After completion of O&M of 2 years (during the warranty period), 6 resident engineers needs to be deployed at DC and 6 resident engineers needs to be deployed at DR (2 in each shift and total there will be 3 shifts of 8 hours each).	Please clarify any discrepancies between resource requirements indicated on pages 172-175 of the RFP.	No Change ; "Manpower cost to maintain 3rd, 4th, 5th Yr of warranty services at New-DC, NewDR - Manpower for only warranty services" is 12 ; which is inline to 2 per shift per DC/DR , having 3 shifts.
183	90	Sect VII-4-vi	Contractor needs to plan, co-ordinate with various stakeholders and execute DC-DR drills .	Kindly, share clarification on Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) requirements.	Will be decided along with the contractor
184	89	Sect VII-1-i	To setup , commission and integrate IT Infrastructure/equipment(s) & solutions of DC, DR and 100+ remote locations.	There appears to be a difference in scope details mentioned in Section VII-2-ii regarding Operations and Maintenance (O&M) of existing IT infrastructure and solutions for new DC, DR, and 300+ remote sites. Please provide clarification.	100 may be read as 34; refer revised clause for same.
185	165	Form 12 Financial Bid (BoQ)	Utility server* (Category 05)	Will the utility server function as a management server to host applications required for managing the BoQ/infrastructure?	These Utility servers are for only hosting CERT-In's applications. Bidder's should not plan to make use of these servers.
186	91	High level Role and Responsibilities of contractor at New Data Centers (DC and DR)	Contractor is required to prepare various SoPs including BCP , DRP & other documents related to operations & as required for ISO27001 certification.	Since the contractor is responsible solely for IT hardware deployment—excluding OS and virtualization—please confirm that creating Standard Operating Procedures (SOPs) will be a joint responsibility involving the contractor, ERNET, and other ERNET partners managing OS, virtualization, and applications.	This will be contractor's responsibility to prepare SoPs,BCP,DRP & other docs required for ISO certification sought. These artifacts will be prepared by contractor for review of ERNET India & CERT-In. For any OS/Virtualization/Application specific processes / documentation information will be provided by CERT-In's third party agency.
187	91	High level Role and Responsibilities of contractor at New Data Centers (DC and DR)	If required, for specific use cases integrate the existing IT infrastructure with the equipment(s) planned in this tender.	Please clarify, since Contractor/Bidder will be responsible only from Hardware perspective only in integrating in this case.	Clause is self explanatory
188	96	7. Role and Responsibilities of Contractor i.e. AAA,AD,EMS and related software applications:	It is responsibility of contractor to maintain the backup of EMS for at least one year which includes data, configuration, alarms, performance etc. Assets data must be maintained throughout	Please confirm if any third party backup solution (e.g. Commvault/NetBackup/Veeam) need to be factored as part of the solution. Also please confirm the amount of data to be backed up to factor the required backup licenses and Backup target Storage.	Based on scope of work, items in BoQ, etc, the data requirements may be calculated and required solution if required by bidder may be factored in.
189	58	Section 10.6. Payment terms	O&M Charges (OPEX Charges) during Operation & Maintenance for Data Centers (DC & DR) and Remote Sites will be released on quarterly basis after completion of each quarter from the date of acceptance of respective milestone.	Days payable post the submission of involve to be specified. For instance, 30 days payment cycle post the submission of respective invoice for Capex and Opex items.	No Change
190	69	Part B (CAPEX II)	EMS: For monitoring of MPLS Link of 250 locations	Please confirm if Monitoring of MPLS link of all 350+ location or only 250 locations	The clause may be read as : For monitoring of MPLS Link of 150 locations
191	89	Section 1	Project Overview: Migration of 80 Links from existing DC & DR to New DC & DR	Please confirm Are these 80 links is only MPLS or any requirement of any P2P link from any remote location to DC/DR ?	These are 80 Remote Locations over MPLS which are being currently connected with exsisting DC-DR ; Contractor needs to migrate these to new DC & new DR by making repective changes in configuration or any other coordination with bandwidth provider.
192	91	Section 4	Contractor shall submit DC-DR Rack layouts for Racking/Stacking of each equipment planned	Request you to confirm number of Rack at DC and DR locations. Existing DC has 100 Rack and DR has 50, it will be similar or different ?	1. New DC , New DR locations are yet to be finalized & will be in Tier-I/Tier-II cities of India. 2. 100 Racks at Exisiting DC and 50 Racks at Exisiting DR
193	91	Section 4	If required, for specific use cases integrate the existing IT infrastructure with the equipment(s) planned in this tender.	Request you to confirm, Is this for requirement of connectivity existing DC/DR with new DC/DR ?	Clause is self explanatory
194	91	Section 4	Integration of all remote sites through IPSec over MPLS Links.	Please confirm this is only for 80 remotes sites, as mentioned in other section.	34 new remote sites ; 80 sites upon migration
195	94	Section 6	Configuring/Integrating the Management and Monitoring software at new DC and new DR with all remote sites.	Please confirm Is this only for 80 remotes sites which will be migrated to new DC/DR ? or all existing remote sites ?	114 Sites and new sites in future that may come.

196	107	Section 12.8	The Contractor shall be responsible for setting up Network services at disaster recovery site for Auto/Manual switch over to run the critical applications from DR in case of any unforeseen disaster at Main DC or as per the directions of ERNET India/ CERT-In.	Please confirm, As per BoQ, DR BoQ is less than of DC. In this case, expectation is not for full recovery in case of entire DC goes down, right ? Need to have more understanding on expectation of Disaster Recovery	This is per application design.
197	64	Bill of Material (BoM)	Part A (Capex-I)	Please clarify, Is there any server commissioning /decommisiong required at the remote sites?	At Remote Sites, only Remote Firewall(s) need(s) to be commissioned
198	90	Project Overview	Migration of 80 Links from existing DC & DR to New DC & DR.	Please clarify, What is the scope of migration and what are the components involved?	These are 80 Remote Locations over MPLS which are being currently connected with exsisting DC-DR ; Contractor needs to migrate these to new DC & new DR by making repective changes in configuration or any other cordinaton with bandwidth provider.
199	72	Part C (Opex)	O&M costs for existing remote sites - Existing - 380	Please clarify, Is this 380 referring to manpower required to support existing remote sites or number of remote sites?	This is number of remote sites
200	93	Scope of Work	Existing IT infrastructure housed at DC, Bengaluru & DR, Mohali which are having IT solutions,	Please clarify, In any migration expected to be done from existing DC/DR to new DC/DR.	No. There is not any migration plan for IT equipmenet. However link migration plan is there from old DC/DR to New DC/DR
201	94	Scope of Work for Operation and Maintenance	Comprehensive On Site maintenance of equipment installed in New DC, DR & remote Sites.	Please clarify, Is 24/7 support required on both new and old DC/DR as well as all remote sites or resources will travel from base location whenever required?	Clause is self explanatory.
202	85	Bidder's Qualification Criteria	Valid certificate(s) of above professional to be submitted along with the bid with covering letter of Director HR of bidder's organization	Please clarify, Can the certificate number be Masked as its confidential or can it be shared at a later stage after qualification.	No Change
203	40	2.1 Assignment and Sub-contracting	All the manpower to be deployed in project for delivery, installation, testing & commissioning and operation & maintenance including onsite support should be on the payroll of the Contractor or OEM whose equipment(s) are offered. Outsourcing of manpower will not be allowed.	Please clarify, Can an outsource resource be deployed in Non-Metro location.	No Change
204	90	Scope of Work of Contractor	To configure ILL, P2P , MPLS WAN links & respective IPSec Tunnels for all remote sites & Data Centre(s) under this bid. The ERNET India empaneled service provider will be providing the ILL, P2P , MPLS WAN links at remote locations	Please confirm ILL, P2P , MPLS WAN links & respective IPSec Tunnels for New DC , New DR and existing DC, DR and all remote sites will also be provided by ERNET ?	Yes links will be provided by ERNET India
205	90	Scope of Work of Contractor	Supply of competent & dedicated manpower for a period of two years respectively at Mumbai, Chennai, Kolkata , Delhi/NCR, Bangalore working in Project from contractor's premises	Please confirm if all resources can work from bidder premises.	For Mumbai and Kolkata, Bidder's premises is allowed. For rest other location, manpower will sit in ERNET India's office.
206	90	High Level Roles and Responsibilities of Contractor	Coordination with Colocation Contractor of existing DC, DR	Please share the details of contractor .	Will be shared with successful bidder
207	88	ction VII Scope of wo	xvii. Perform the security audit (including VAPT) and fix all security issues at the time of acceptance. VAPT should be performed once per year	Request ERNET to share number of assets for which VAPT is to be performed. Also request ERNET to share if they have some existing VAPT tools/licenses which bidder can leverage or if tools have to be procured by the bidder. It tools/licenses are to be procured by the bidder, request ERNET to include the same in the bill of quantity.	Asset details of existing hardware shared in Annexure. Further it is duty of contractor to bring desried tool/equipment to perform VAPT of new/existing DC-DR and remote sites.
208	91	Section VII Scope of work	Contractor must perform continuous & mandatory security audits, of various applicable artifacts (such as security review of DC-DR-Remote Site architecture/design, security review of integration of various components/solutions & other security reviews.), at the all stages of the project beginning from the conceptualizing the bid response, project planning, design and implementation stages.	Request ERNET to specify the number of assets/applications for which VA is to be conducted. Request ERNET to include this in BOQ.	Asset details of existing hardware shared in Annexure. Further it is duty of contractor to bring desried tool/equipment to perform VAPT of new/existing DC-DR and remote sites.

209	91	Section VII Scope of work	Contractor needs to submit the details of two CERT-In empaneled agencies as the security auditor(s) of the project in the Bid for ensuring the security of the overall project including remote sites.	Would ERNET be responsible for clearing the invoices raised by these CERT-In empaneled vendors? Requesting clarification to ensure correct scoping of the bid.	Revised Clause: Sucessful bidder needs to submit the details of two CERT-In empaneled agencies as the security auditor(s) of the project for ensuring the security of the overall project including remote sites with in 4 months from the date of contract. Further payment to these agencies will be made by Successful bidder only. ERNET India will not bear any expenditure in this regard.
210	92	Section VII Scope of work	Contractor needs to provide an independent cyber security expert consultant who will be available within 30 days from the date of issue of contract (available till end of project) & responsible for designing and implementing the security of the project & support in knowledge sharing reviews of Change requests etc.	Request ERNET to share the desired qualification/certifications of this cybersecurity consultant. Also request ERNET to include this consultant in manpower BOQ.	Kindly refer manpower specification in this regard.
211	92	Section VII Scope of work	Contractor also needs to support, facilitate the integration of additional planned security solutions (such as AntiAPT Solutions, HIDS/HIPS, ZTA etc. – this list is yet to be finalized, & procured via another bid) with the currently planned infrastructure in this bid. In order for successful integration of additional security solutions contractor shall perform the required, approved changes in the supplied IT Infrastructure/equipment's/solutions.	Bidder would require details regarding the make and model of the procured items and solutions to ensure compatibility of bidder supplied components with the same.	These equipment(s) are yet to be procured.
212	92	Section VII Scope of work	Contractor shall configure all the components and sub-components for end-to-end user access to all applications/services. It is clarified that, it is a contractor's responsibility to change the configurations (if required) for DC equipment's which are already installed to integrate with equipment procured through this bid.	Responsibility of changes of configurations of existing equipment should lie with the incumbent vendors and OEMs as bidder may not have any expertise in the existing solutions and equipment. Request ERNET to let this responsibility lie with the existing vendor or to specify the expertise which would be required to carry out this activity and include the same in the manpower BOQ.	O&M of existing DC-DR will be provided by successful bidder. Manpower already planned in BoQ for this activity. Proper Handoff from existing to new contractor will be planned by ERNET India.
213	84	A. Bidder's Qualification Criteria	The bidder on the date of publishing of this bid; should already have in-house capabilities to discharge the roles & responsibilities as a System Integrator. Therefore, the bidder is not allowed to float any EoI or Tender against this Tender requirement for identifying any system integrator, consultant, empanelment, sub-contractor or a partner or a teaming partner etc. by whatever name called; for discharging/sharing its responsibilities as a System Integrator. Further, it may also be noted that consortium, arrangements, joint-ventures, teaming, subletting, sub-contracting is strictly prohibited in this bid. In case, at any stage of the project, if its identified that any kind of above mentioned prohibitions were violated, ERNET India reserves the right to take suitable actions such as mentioned in Section III Clause 12. The bidder needs to submit an undertaking in this regard	We would like to confirm whether the experience of a subsidiary company can be considered to meet the requirements related to the successful implementation of Supply, Installation, or Operation and Maintenance of WAN setups. Our subsidiary company, has successfully completed the implementation of WAN setups across 50 customer office locations. Request to allow subsidiary company experience also.	No Change
214	98	Section VII Scope of work	It may be noted by bidder that VAPT to be done for entire setup .	Request ERNET to share number of assets for which VAPT is to be performed. Also request ERNET to share if they have some existing VAPT tools/licenses which bidder can leverage or if tools have to be procured by the bidder. It tools/licenses are to be procured by the bidder, request ERNET to include the same in the bill of quantity.	Asset details of existing hardware shared in Annexure. Further it is duty of contractor to bring desried tool/equipment to perform VAPT of new/existing DC-DR and remote sites.

215	107	12.7 Security Administration and Management Services	Addressing the ongoing needs of security management including, but not limited to, monitoring, configuration/reconfiguration, troubleshooting of various devices/ tools such as firewall, IPS/IDS, through implementation of proper patches, procedures and rules.	ERNET to clearly specify the ongoing needs of security management. This would require clear outlining of the current security solutions being used at ERNET. This will help bidder in identifying the scope and expertise required to fulfill RFP conditions.	Asset details of existing hardware shared in Annexure , accordingly bidders will be able to access the required details in identifying the scope and expertise required to fulfill RFP conditions.
216	107	12.7 Security Administration and Management Services	Respond to security breaches or other security incidents by taking corrective measures, providing guidelines to users and coordinate with respective OEM in case a new threat is observed to ensure that workaround /patch is made available for the same	Responding to breaches would require access to logs and would also need a SOC setup by the bidder. Request ERNET to specify if an SIEM tools exists or needs to be procured by the bidder. if the tool is to be procured by the bidder, request ERNET to include the same in the BOQ.	Logs will be made available with permissions from CERT-In when required. Bidder needs to ensure the security breaches don't occur and accordingly needs to establish the right SoP/Updates/Upgrades/Policies/Configurations etc.
217	127	E. Security and Incident Management Service Levels for all DC and DR	There will not be any penalty capping for this sectio	Request ERNET to add quarterly capping of 5%.	No Change
218	127	E. Security and Incident Management Service Levels for all DC and DR	For every Virus attack reported and not resolved within 36 hrs. from the time of attack	Bidder should not be held responsible and penalized for any virus attack resulting from the vulnerabilities in the existing equipment which has not been supplied by the bidder. Request ERNET to modify these conditions. Also, overall security can only be monitored if a SOC is operated by the bidder which has not been specified in the scope. Request ERNET to clarify on the same.	No Change
219	127	E. Security and Incident Management Service Levels for all DC and DR	For every instance of Data Theft, the bidder is subject to penalty and/or punishment applicable under the IT act/ ERNET India/CERT-In data theft policy or any other prevailing laws of the State/Country at that point of time, which shall be over and above the stated penalty.	Bidder should not be held responsible and penalized for any data theft resulting from the vulnerabilities in the existing equipment which has not been supplied by the bidder. Request ERNET to modify these conditions. Also, overall security can only be monitored if a SOC is operated by the bidder which has not been specified in the scope. Request ERNET to clarify on the same.	No Change
220	66	Bill of Material (BoM)	54 Forensic workstations 2 no. 55 Forensic laptops	Request ERNET to specify if any forensic tools/ solutions have to be procured by the bidder.	Pls refer to the specifications of item. Relevant details are available in specs.
221	40	Sec-3	5.3. Consequences of a breach of Obligations	Should the contractor commit a default or breach of GCC-clause 5.1 to 5.6, the Contractor shall remedy such breaches within 21 days, keeping the ERNET India informed. However, at its discretion, the ERNET India shall be entitled, and it shall be lawful on its part, to treat it as a breach of contract and avail any or all remedies thereunder. The decision of the ERNET India as to any matter or thing concerning or arising out of GCC-clause 5.1 to 5.6 or on any question whether the contractor has committed a default or breach of any of the conditions shall be final and binding on the contractor.	No Change
222	38	Sec-3	2.5.2	5.3 Consequences of a breach of Obligations Should the contractor commit a default or breach of GCC-clause 5.1 to 5.6, the Contractor shall remedy such breaches within 21 days, keeping the ERNET India informed. However, at its discretion, the ERNET India shall be entitled, and it shall be lawful on its part, to treat it as a breach of contract and avail any or all remedies thereunder. ~~The decision of the ERNET India as to any matter or thing concerning or arising out of GCC-clause 5.1 to 5.6 or on any question whether the contractor has committed a default or breach of any of the conditions shall be final and binding on the contractor.~~	No Change

223	40	Sec-3	5.5.	5.6 Confidentiality and IPR Rights 5.6.1 IPR Rights All deliverables, outputs, plans, drawings, specifications, designs, reports, and other documents and software submitted by the Parties ~~contractor under this Contract shall become and remain the property of the ERNET India/ CERT-In and~~ must not be shared with third parties or reproduced, whether in whole or part, without either Party's ~~the ERNET India/ CERT-In's~~ prior written consent. The contractor shall, not later than upon termination or expiration of this Contract, deliver all such documents and software to the ERNET India/ CERT-In, together with a detailed inventory thereof.	No Change
224	49	Sec-3	7 (7.1)	9.5 Extension of Delivery Period and Liquidated Damages: ERNET India may, on the request of the bidder or otherwise, extend the delivery date suitably subject to the following conditions: 1) The original Delivery Period may be re-scheduled by the ERNET India without any Liquidated damages if such reschedule is warranted due to Force Majeure conditions mentioned below and also on the ground/reasons of delay attributable to the ERNET India. However, the said re-schedule delivery period shall be provided in the Purchase Order issued to sucessful bidder. In all other cases, if any extension is given then same shall also attract LD as given in clause 9.5.2 below. 2) Liquidated Damages (LD): a. If the Contractor fails to meet the prescribed timelines for respective milestones due to any reason whatsoever, except due to Force Majeure conditions, then in such a case ERNET India would be entitled to impose the Liquidated Damages for the delay: i. Delay in Delivery of the Equipments (only for DC & DR): @ 0.5 % of the value of delayed equipments (of the respective milestones); per week or part of the week of delayed period. ii. Delay in Commissioning & offering for acceptance (for DC, DR & Remote Sites): @ 0.5 % of the sum total value of all the equipments for respective milestone; per week or part of the week of delayed period. Note: Overall Liquidated Damages shall be restricted to 10% of the total contract value. While calculating LD; GST will be excluded from the value on which LD is calculated; thereafter GST may be charged (if applicable) on the LD	No Change
225	56	Sec-3	9.6	What is Non-Contractual claims?	Examples of non-contractual claims include tresspasing, assault, fraud, breach of confidentiality, negligence.
226	59	Sec-3	12	What is the indemnity for in this clause?	Clauses are self explanatory
227	179	Annexure-1 (Technical Specifications)	All the solutions proposed to be supplied with this bid mandatorily should work in as an on-premises solution & not as a cloud based solution.	Please confirm, our understanding that the Request for Proposal (RFP) specifies only hardware requirements and no Cloud software required, application software are not within the scope of the bidder/contractor.	No Cloud based solutions are required ; Only the solutions/Applications sought in the Bid are required to be supplied. The applications planned to be installed on server are out of scope of bidder
228	1	Section V: Technical Specifications / Annexure-1 (Technical Specifications)	l. Only the Manpower on OEM payrolls shall perform network planning, designing, implementation, integration and testing/validation for all Networking equipment(s) i.e. **only direct OEM payroll manpower would be allowed to work on the project's designing, implementation & testing phase.** An undertaking for same shall be provided.	We understand that OEM payroll employee will be required to perform network planning, designing and validation along with the bidder. However for integration & testing for all networking equipments, OEM authorized service partner OR OEM product certified resource would be allowed to work undee OEM supervision.	No Change

229	2	GEM NIT	EMD EXEMPTION: The bidder seeking EMD exemption, must submit the valid supporting document for the relevant category as per GeM GTC with the bid. Under MSE category, only manufacturers for goods and Service Providers for Services are eligible for exemption from EMD. Traders are excluded from the purview of this Policy.	As per the Notice Inviting Tender (NIT), it is specified that the bidder seeking EMD exemption must submit valid supporting documents for the relevant category, as per GeM GTC. However, in the General Conditions of Contract (GCC) - Section III of the tender document, it is mentioned that in case of any conflict between the provisions of the GCC and the GeM GTC, the provisions of the GCC will prevail, and in case of a conflict with the GeM GTC, the provisions of the tender document shall govern. Given that the NIT allows EMD exemption under GeM GTC, but the GCC mandates the EMD submission, there appears to be a contradiction between the two clauses. This could lead to confusion regarding the submission requirements for bidders who are exempted from EMD as per GeM GTC. In this regard, could you kindly provide clarification on the following points: 1. Confirmation on EMD Exemption: 2. Clarification on Conflict Resolution: In case of a conflict between the GeM GTC and the provisions of the GCC regarding the EMD requirement, which of the two documents should be considered binding? 3. Action on Additional Terms and Conditions (ATCs): As per the disclaimer in the NIT, if any clause(s) are incorporated in contradiction with GeM GTC, the resulting contract may be declared null and void. How does this affect the applicability of EMD provisions in this tender?	Kindly refer to respective updated clause in Annexure-B
230	9	2.3. Earnest Money Deposit (EMD)	- EMD is to be submitted along with the bid by the bidders. Therefore, the last date of submission of EMD will be the same as last date of submission of the bids. - Bids received without Earnest Money Deposit are liable to be rejected.		Kindly refer to respective updated clause in Annexure-B
231	15	1.4.4	1.4.4 Section III: General Conditions of Contract (GCC) Section III – General Conditions of Contract (GCC) describe the conditions that shall govern the resulting contract. In case of any conflict, provisions of GCC shall prevail over those in ITB and in case of any conflict of this tender document from GeM GTC, provisions of this tender document shall prevail over those in GeM GTC		Kindly refer to respective updated clause in Annexure-B
232	5	GEM NIT	**Disclaimer** The additional terms and conditions have been incorporated by the Buyer after approval of the Competent Authority in Buyer Organization, whereby Buyer organization is solely responsible for the impact of these clauses on the bidding process, its outcome, and consequences thereof including any eccentricity / restriction arising in the bidding process due to these ATCs and due to modification of technical specifications and / or terms and conditions governing the bid. If any clause(s) is / are incorporated by the Buyer regarding following, the bid and resultant contracts shall be treated as null and void and such bids may be cancelled by GeM at any stage of bidding process without any notice:- 2. Seeking EMD submission from bidder(s), including via Additional Terms & Conditions, in contravention to exemption provided to such sellers under GeM GTC.		Kindly refer to respective updated clause in Annexure-B

233	General	GEM NIT	Document required from seller 1. Experience Criteria, 2. Past Performance, 3. Bidder Turnover, 4. Certificate (Requested in ATC), 5. OEM Authorization Certificate, 6. OEM Annual Turnover, 7. Additional Doc 1 (Requested in ATC), 8. Additional Doc 2 (Requested in ATC), 9. Additional Doc 3 (Requested in ATC), 10. Additional Doc 4 (Requested in ATC), 11. Compliance of BoQ specification and supporting document	As per GEM portal only 11 slots are available for uploading bid documents, with a maximum of 10 MB per slot and 100 pages per slot. This limitation restricts bidders from submitting comprehensive bids, as multiple OEM documents, technical specifications, and other required documents are essential for a complete submission. Given the complexity and volume of documentation involved in the bidding process, it would be greatly beneficial if the number of available upload slots could be increased, along with an expansion of the file size limit, to ensure that all necessary documents can be uploaded without any issues. We kindly request your support in making these adjustments to facilitate smoother and more efficient bid submissions for all parties involved.	ERNET India will request GeM to enhance MB per slot.
234	42	Section III: General Conditions of Contract(GCC) : 5.7 (1)	Performance Bond/ Security The successful bidder shall submit a Performance Security @ 5% of total value of Contract (including GST)within 14 days from the date of issuance of contract. The Performance Security if submitted in the form of Bank Guarantee, Fixed Deposit and Insurance Surety bond should be valid for a minimum period of 75 months (Implementation period+ Warranty Period+ Claim Period of 3 months).	Request to amend the clause as mentioned below:- The successful bidder shall submit a Performance Security @ 3% of total value of Contract (including GST)within 14 days from the date of issuance of contract in the form of Bank Guarantee, Fixed Deposit and Insurance Surety bond should be valid for a minimum period of 75 months (Implementation period+ Warranty Period+ Claim Period of 3 months).	No Change
235	47	Section III: General Conditions of Contract(GCC): Clause 14 viii	The overall Penalties for non-adherence with the SLA of warranty support (during 3rd , 4th & 5th year of warranty period) per quarter shall be capped at a maximum of 25% of the respective Quarterly payment (CAPEX).	Request to reduce the limit up to 10% for smooth execution of the project.	No Change
236	57	Section III: General Conditions of Contract(GCC): Clause 10.6b	50% of the value of equipment(s) delivered at DC and similarly 50% of the value of equipment(s) delivered at DR shall be released only after submission of BG equivalent to the amount which is to be released. The BG should be valid for a minimum period of 6 months (with a claim period of additional 3 months). BG must be extendable till the successful completion of rack mounting & Power On Self Test (POST) of active equipments	Request to reduce the limit up to 10% for smooth execution of the project.	No Change
237	57	Section III: General Conditions of Contract(GCC) : Cluase No. 10.6e Prices and Payments Terms:	ERNET India may give an option to contractor to claim Balance 20% payment against submission of Bank Guarantee.	Request to replace the word "may" from "will" for determining the better cashflow for smooth execution of project.	No Change
238	72	Section IV: Bill of Material : BOM-Part C (OPEX),	59, Databases GeoIP, VPN Services	The exact requirement of the scope may be detailed further for this clause.	Pls refer to the revised specifications

239	73	Section IV: Bill of Material :BOM-Part C (OPEX), Minimum Qualification, Relevant Experience & Certifications at DC/DR & Shastri Park, Delhi	Role- **Data center IT networking & architecture expert-** B.E./B.Tech/MCA with 10 Years relevant experience in IT/ITeS + CCIE-ENT	Data Center Expert should have DC Networking Experience & certification wrt DC. Request you to change the certificate requirement from CCIE-Ent to CCNP-DC/JNCIP-DC	The clause may be read as : **Data center IT networking & architecture expert** B.E./B.Tech/MCA with 10 Years relevant experience in IT/ITeS + CCNP-DC/JNCIP-DC
240	85	Section VI: Qualification Criteria : A9. Bidder's Qualification Criteria	9. The bidder must be an authorised representative of the products/Equipment(s) offered. The authorisation letter from the OEM must be submitted along with the bid Authorisation must be issued by OEMs Authorised signatory. OEMs' MAF should contain mainly the following points in its MAF (Manufacturer Authorisation Form) while issuing to bidder: c) Offered equipment(s)/solutions (s) are IPv6 ready	Kindly clarify that IPv6 clause will be applicable for the Active equipment only and will be not apply for the non IT (Passive) equipment OEMs.	Yes; Its sought for Active Equipments
241	86	Section VI: Qualification Criteria : B1. Original Equipment Manufacturer (OEM)'s Criteria	1. Following equipment(s) OEMs whose products have been offered in the bid shall have Technical Assistance Centre (TAC) in India. OEM shall have dedicated/Toll Free Number for TAC to support the equipment. OEM(s) should have direct presence with their own office in India. Relevant documentary proof (i.e. Registration/Incorporation Certificate, Self-certification of TAC availability and Dedicated/Toll free number) should be submitted. Note: ERNET India/CERT-In/Contractor's representative should be able to log complaints on OEM TAC directly.	Kindly provide the list of the equipment as mentioned for the " **Following equipment(s) OEMs**" as per clause.	Clause is self explanatory.
242	90	Section Section VII: Scope of Work Clause No. 2.Scope of Work of Contractor	xvii.Any other electric/networking accessories related work required for installation/commissioning of equipment(s)/software. xviii.Any other activity essential or incidental for successfully accomplishing the objectives & outcomes of this project.	Pl clarify further on the bidder's scope of electric/networking/integration requirements not covered in SOR	Clause is self explanatory
243	90	Section Section VII: Scope of Work Clause No. 2.Scope of Work of Contractor	xix.Contractor needs to support, faciliatate the integration of additional planned security solutions / devices (to be procured via another bid) with the currently planned infrastructure in this bid.	We understand that the security solutions provided in this bid may need to be integrated with security solutions to be procured by another bid, the type of devices and scope of such integration may be elaborated further	Clause is self explanatory
244	90	Section Section VII: Scope of Work Clause No. 2.Scope of Work of Contractor	xv.Supply of competent & dedicated manpower for a period of two years respectively at Mumbai, Chennai, Kolkata , Delhi/NCR, Bangalore working in Project from contractor's premsies. In addition, supply of competent & dedicated contractor's manpower including OEM's manpower at ERNET India / CERT-In & at new DC, DR locations as per the required manpower criteria(s) defined in respective manpower section.	We understand that the resources deployement at contractor premises Mumbai, Chennai, Kolkata , Delhi/NCR, Bangalore other than new DC, DR to be deployed primarily for project in 1st year and rest 2 year they will be part of O&M. Pl clarify	This manpower shall remain deployed as per their designated locations only throughout the complete duration as defined in "PART-C(OPEX)"

245	90	Section VII: Scope of Work 2. Scope of Work of Contractor	viii. Integration of supplied IT infrastructure & solutions, equipment(s) at DC, DR and remote locations as per finally accepted & audited HLD & LLD.	As per our understanding Cooling, Power cabling and earthings will be provided by the customer and Distribution Board to rack PDU power cable & earthing extension will be taken care by the bidder. Kindly confirm if our understanding is correct **or else kindly provide the details and scope for the Power cabling and earthings.**	Power uptil PDU at DC& DR will be responsibility of ERNET India/CERT-In.
246	92	Section VII: Scope of Work, Clause 4 High level Role and Responsibilities of contractor at New Data Centers (DC and DR), a	a. Contractor needs to provide an independent cyber security expert consultant who will be available within 30 days from the date of issue of contract (available till end of project) & responsible for designing and implementing the security of the project & support in knowledge sharing reviews of Change requests etc. b. Contractor needs to provide an independent data center IT networking & architecture expert consultant at within 30 days from the date of issue of contract (available till end of DC-DR project commissioning) & will be responsible for: i. Designing (HLD, LLD) and implementing the data center networking, compute & other solutions .	Is this role of cybersecurity & DC Expert which is part of the dimensioned manpower or Additional 3rd party consultants to be considered? Pls clarify	This should be a regular manpower on Payrolls of Contractor
247	92	Section Section VII: Scope of Work Clause No. 4.High level Role and Responsibilities of contractor at New Data Centers (DC and DR)	xiv.Contractor also needs to support, faciliatate the integration of additional planned security solutions (such as AntiAPT Solutions, HIDS/HIPS, ZTA etc. – this list is yet to be finalized, & procured via another bid) with the currently planned infrastructure in this bid. In order for successful integration of additional security solutions contractor shall perform the required, approved changes in the supplied IT Infrastructure/equipments/solutions.	We understand that the security solutions provided in this bid may need to be integrated with security solutions to be procured by another bid, the type of devices and scope of such integration may be elaborated further	Clause is self explanatory;
248	94	Section VII: Scope of Work / 7. Role and Responsibilities of Contractor i.r.o AAA,AD,EMS and related software applications:	1) Setting up, configuring and integrating requested software modules such as AAA, Active Directory, EMS, PATS, IT Helpdesk, Asset Management etc. (its complete list as per BoM & specifications) **in a High Availability (HA) mode** for administration, monitoring and management of infrastructure and established Network. EMS OEM holds the responsibility to perform integration of overall EMS solution & PATS (with all their respective sought modules).	Contractor assumes that the high availability is required between DC and DR and standalone implementation to be carried out at individual site i.e. DC/DR. Kindly confirm if the understanding is correct.	Refer to tender specs w.r.t Enterprise Management System with NMS in HA
249	95	Section VII: Scope of Work / 7. Role and Responsibilities of Contractor i.r.o AAA,AD,EMS and related software applications:	13) Integration with Email Gateways/servers, SMS Gateways. Please note that Supplied EMS must have the capability to get integrated with standard solutions available in market w.r.t Email Gateways/servers, SMS Gateways.	Contractor assumes that the integration with Email Gateways/servers, SMS Gateways to be done by supplied EMS; however the **mail Gateways/servers, SMS Gateways including their charges will be provided by ERNET**. Kindly confirm it.	Email/SMS gateway will be procured by ERNET India separately

250	97	Section VII: Scope of Work / 8. General Activities to be performed by Contractor for the project: -	12) The bid should include **OEM professional services** for the successful implementation of project. The OEM professional services shall include but not limited to solution architecture, design, installation, preparation of acceptance test plan & procedure with expected results and end user training leading to OEM Certification. The above activities should be jointly done by the Contractor and the OEM, as per the best security practices for the final acceptance.	Contractor request the ERNET India to clarify which all components should include OEM professional services. Please clarify it.	Clause is self explanatory
251	127	Section VIII: Service Level Agreement during Operation & Maintenance	The overall Penalties (for Clause 1-A,B,C,D in Section-VIII) per quarter shall be capped at a maximum of 25% of the respective Quarterly payment of Grand Total Value.	Please reduce the penalty capping to 10% of respective quarterly payment.	No Change
252	127	Section VIII: Service Level Agreement during Operation & Maintenance (Security and Incident Management Service Levels for all DC and DR)	There will not be any penalty capping for security incidents. Rs.5,00,000 per instance. For every instance of Data Theft, the bidder is subject to penalty and/or punishment applicable under the IT act/ ERNET India/CERT-In data theft policy or any other prevailing laws of the State/Country at that point of time, which shall be over and above the stated penalty.	Please include security incidents penalty as well in overall capping of penalty.	No Change
253	128	Section VIII: Service Level Agreement during Operation & Maintenance (Manpower Service Level Agreement)	If the employee is found responsible for disobedience/ misconduct.Immediate replacement of resource within 3 days as decided by ERNET India depending on the gravity of the act	Please increase the time duration for replacement of employee to 45 days.	No Change
254	20	Section II: Instructions to Bidders (ITB) -5.2.1	Prices quoted by Bidder shall remain firm and fixed during the currency of the contract and not subject to variation on higher side on any account.	Prices quoted by Bidder shall remain firm for one time work order/Purchase order of the contract.	No Change
255	30	Section II: Instructions to Bidders (ITB) - 12.1.1 ii	ERNET India reserves the right to increase the ordered value by up to 25% of sum total of final bid value; till the completion of O&M activities, without any reference to the intial ordered quantities.	It is requested to change the clause as "ERNET India reserves the right to increase the ordered value by up to 25% of sum total of final bid value **at the time of one time work order/ Purchase order".**	No Change
256	52	Section III: General Conditions of Contract(GCC) : Clause 9.3.6	Timeline for Delivery, Installation, testing, commissioning & Acceptance:	It is requested to change the clause as "Start of Milestone 1 - T+12 Weeks Completion of milestone 1 - T +36 weeks Start of milestone 2 - T + 12 weeks Completion of milestone 2 - T + 38 weeks Start of milestone 3 - T + 40 weeks completion of milestone 3 - T + 44 weeks	Kindly refer to respective updated clause in Annexure-B
257	38	2.5.1.1	"......At any time during the currency of the contract, the ERNET India may suo-moto or, on request from the contractor, by written order, amend the contract by making alterations and modifications within the general scope of the Contract."	It is requested that any change or amendment in the contract shall be on mutual agreement basis.	No Change

258	124	Sec VIII -1.A.(2)	In case of downtime caused due to core networking equipment* failure supplied by bidder, a penalty of Rs. 1,00,000/- for every six hour or part thereof will be imposed. This penalty will be over and above any other applicable penalties	Kindly confirm capping on this SLA is restyricted to overall SLA capping at 25%	Clause is self explanatory
259	126	Sec VIII - E & F	There has been no capping for the SLA for Security & Incident Management Services levela for all DC and DR alongwith Manpower deployment	It is requested that the penalty for said SLAs be capped to 25% as defined for all other SLAs during O&M.	No Change
260	58	10-7	It may be noted that the payment to the contractor are subject to making sufficient funds available by CERT-In to ERNET India . Contractor agrees and accepts that there can be delays in releasing the payment due to non-availability of funds.	It is requested that the payment shall be made on submission of Invoices by customer and shall not be linked to fund availability from CERT-In	CERT-In is the funding agency of this project, accordingly , release of payments to contractor will be made upon receipt of funds .
261	40	05-Jan	Indemnities for breach of IPR Rights or from other issues	It is requested to modify this clause by adding the following: The Contractor's indemnification shall not extend to any such liability which arises as a result (a) use of Contractor's deliverables or services in a manner inconsistent with instructions or documentation provided by the Contractor; (b) combination of Contractor deliverables or services with software or other programs not provided by the Contractor.	No Change
262	59	12-Jan	Defaults, Breaches, Termination and closure of Contract	Two weeks is a very short time to cure the defect hence the contractor would like to suggest to increase the defect cure notice period to 2 months as a defect cure notice period for the contractor to cure the breaches if any and only upon its failure to do so, ERNET may terminate the affected portion of the scope of work and not the entire contract.	No Change
263	60	06-Jan	Risk and Cost Procurement	The condition that ERNET reserves the right to remedied the defects at the risk and cost of the defaulting contractor actually puts the contractor in UNLIMITED/UNCAPPED RISK which is unreasonable, more due to the fact that there are multiple penalties already applicable. Hence, this provision may be deleted.	No Change
264	61	12.1.5	Except in cases of criminal negligence or wilful misconduct, the aggregate liability of the contractor to the ERNET India, whether under the contract, in tort or otherwise, shall not exceed the total Contract value, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment, or to any obligation of the contractor to indemnify the ERNET India concerning IPR infringement.	The exception towards the liability cap must be modified to the extent that the overall liability of the bidder is capped to a certain amount. Please include the following provision within the tender "The contractor’s aggregate liability arising out of or in connection with the contract, whether based on contract, tort, statutory warranty or otherwise, shall be limited to an aggregate of most recent 12 months of the charges collected by the contractor under the affected order. The contractor shall not be liable for any special, indirect, incidental or consequential damages of any kind including but not limited to loss of use, data, profit, income, business, anticipated savings, reputation, and more generally, any loss of an economic or financial nature, whether these may be deemed as consequential or arising directly and naturally from the incident giving rise to the claim".	No Change

265	61	12	12.2.1 Termination for Default/ Convenience of ERNET India	ERNET has reserved the right to terminate the contract for convenience. It is requested to either delete this clause or modify it by adding the following: ERNET shall pay the Contractor the following amounts: (a) The Contract Price, attributable to the parts of the Equipment(s)/Work(s) executed including goods and services delivered (including also the Work in Progress) by the Contractor up to the date of termination. In respect of capital items deployed in the Project, ERNET must purchase at the Written Down Value (WDV) from the Contractor all IT & non-IT infrastructure and the hardware and software deployed. The costs reasonably incurred by Contractor in the ramp down / disengagement of Contractor's and its subcontractors' personnel; (c) Any amount to be paid by Contractor to its subcontractors in connection with the termination of any subcontracts, including any cancellation charges; (d) Costs incurred by Contractor in protecting the Equipment(s)/ Work(s) and leaving the site in a clean and safe condition pursuant to this clause; and (e) The cost of satisfying all other obligations, commitments, and claims that Contractor may in good faith have undertaken with third parties in connection with the contract. Work in progress. The term "work in progress" shall include but not limited to the value of goods and services meant for delivery to ERNET India (i) for which manufacturing process was initiated by Contractor; or (ii) order was placed by Contractor on its vendors, prior to the date of termination.	No Change
266	83	Section VI: Qualification Criteria / A(3)	Bidder should have experience of successful implementation of similar project(s) in Central/State Government/ Govt. undertakings/UT's/Autonomous Bodies/Public listed companies/reputed Private organisation in India as: Single order of Rs. Rs.500 Crore or more; OR Two orders each having minimum of Rs. 250Crore of estimated cost or more; OR Three orders each having minimum of Rs. 200Crore of estimated cost or more Similar Projects: - Setting up of Data Centre (including computing, storage & networking Infrastructure) / Ongoing Operation & Maintenance of Data Centres (done for minimum of two years)/ Completed or ongoing AMC of Data Center (done for minimum of two years)/ Network Operation Centres/ Security operation centres/ Smart City Projects/ Large IT networking.	It is understood that the term "single order" refers to the bidder's experience in the implementation, ongoing operation, and maintenance (O&M) or Annual Maintenance Contract (AMC) of a data center under one project. Furthermore, the purchase order may either be a single order covering the entire scope, or separate purchase orders for the implementation phase and for the ongoing operation and maintenance/AMC of the same project. This is in line with industry practice, where the O&M/AMC contract may be awarded upon the successful completion of the implementation phase of the project.	For the project which has been implemented by the bidder concerned, any O&M/AMC being an integral part of the same project, even if awarded by way of separate work orders will be considered, provided the separate work order(s) for O&M/AMC were not bagged by way of participating in competetive bidding. An undertaking in this regard shall be submitted by the bidder in relevant cases.
267	84	Section VI: Qualification Criteria / A(4)	Bidder should have experience of successful implementation of Supply & Installation or operation and maintenance at 50 locations, of WAN setup in customer office premises in single or multiple orders in Central/State Government/ Govt. undertakings / UT's /Autonomous Bodies/Public listed companies.	It is understood that if the bidder has successfully supplied and installed user equipment or provided operation and maintenance services at 50 user locations with access to data center/ centalized applications in customer office premises, either in single or multiple orders, for Central/State Government, Government Undertakings, Union Territories (UTs), Autonomous Bodies, or Public Listed Companies, this will be considered.	Kindly refer to respective updated clause in Annexure-B

268	84	Section VI: Qualification Criteria / Note i.r.o clause 4,5&6-	Bidder shall provide relevant copies of the customer purchase orders in support of scope of work, deliverables, project value and satisfactory work completion certificate from client. Bidder shall also provide Name, Address, email and contact no. of organization whose Purchase orders are submitted by Bidder. Order Completion date/date(s) should fall between 01/11/2019 to 31/10/2024.	It is requested that the order completion date(s) should fall between 01/11/2017 and 30/11/2024, as the scope of the project and the required experience pertain to a turnkey project with a duration of 6 to 9 years. Alternatively, a consortium may be allowed. Further, due to the lockdown period, projects may have been either short-closed or extended, and therefore, the lockdown period should be considered.	Kindly refer to respective updated clause in Annexure-B
269	84	Section VI: Qualification Criteria / A(7)	The bidder must have following professional* working on its payroll: a. Prince-2/ PMP - 5 numbers b. CISA/CISSP/CISM - 2 numbers c. CDCP - 2 numbers d. CCIE-Sec/JNCIE-Sec - 1 numbers e. CCIE-ENT/JNCIE-ENT - 1 numbers f. CCIE-DC/CCNP-DC/JNCIE-DC/JNCIP-DC - 2 numbers g. CCNP-Sec/ JNCIP-Sec/Fortigate NSE-4/PCNSE - 3 numbers h. CCNP-ENT/ JNCIP-ENT - 3 numbers *Professionals must be regular employee of bidder as on date of submission of this bid. Fixed term contract/contractual employee will not be accepted. Valid certificate(s) of above professional to be submitted along with the bid with covering letter of Director HR of bidder's organisation.	This may be deleted as it violates GeM conditions, as outlined below, and also restricts the bidder's participation: "**Mandating foreign / international certifications even in case of existence of Indian Standards without specifying equivalent Indian Certification / standards**" and "**Seeking experience from specific organization / department / institute only or from foreign / export experience**"	Kindly refer to respective updated clause in Annexure-B
270	84	Additional Clause	Similar work under NDA	The bidder may have implemented similar work under a Non-Disclosure Agreement (NDA) and may not be able to provide specific details. In such cases, can the work details be certified by the Company Secretary as acceptable?	Kindly refer to respective updated clause in Annexure-B
271	83	Section VI: Qualification Criteria	A. Bidder's Qualification Criteria 3. Bidder should have experience of successful implementation of similar project(s) in Central/State Government/ Govt. undertakings/ UT's/Autonomous Bodies/Public listed companies/reputed Private organisation in India as: Single order of Rs. Rs.500 Crore or more; OR Two orders each having minimum of Rs. 250Crore of estimated cost or more; OR Three orders each having minimum of Rs. 200Crore of estimated cost or more Similar Projects: - Setting up of Data Centre (including computing, storage & networking Infrastructure) / Ongoing Operation & Maintenance of Data Centres (done for minimum of two years)/ Completed or ongoing AMC of Data Center (done for minimum of two years)/ Network Operation Centres/ Security operation centres/ Smart City Projects/ Large IT networking.	As some of the projects are under NDA, it is not feasible to share the customer artifacts as they are confidential. Hence the bidder requests the following 1. Please allow to submit the anonymize project citations. 2. Please accept self-certificate signed by authorized signatory / Company Secretary stating the relevant experience details as a documentary evidence.	Kindly refer to respective updated clause in Annexure-B

272	83	Section VI: Qualification Criteria	A. Bidder’s Qualification Criteria 4. Bidder should have experience of successful implementation of data center with leaf and spine architecture in Central/State Government/ Govt. undertakings/ UT’s/Autonomous Bodies/Public listed companies/reputed Private organisation in India as: Single order of Rs. 100 Crore or more; OR Implemented 50 Rack with leaf and spine architecture or more; Note: This clause (4) is not applicable for those bidder(s), who are having experience of setting up of data center along with leaf and spine architecture as per clause no.3 above.	As some of the projects are under NDA, it is not feasible to share the customer artifacts (Customer purchase orders, Work order or Go-Live / Completion certificate from client / /Agreement/LOA/LOI). Similarly Name, Address, email and contact no. of organization whose Purchase orders are submitted by Bidder. Hence the bidder requests the following 1. Please allow to submit the anonymize project citations. 2. Please accept self-certificate signed by authorized signatory / Company Secretary stating the relevant experience details as a documentary evidence.	Kindly refer to respective updated clause in Annexure-B
273	83	Section VI: Qualification Criteria	A. Bidder’s Qualification Criteria 2. The minimum average annual audited financial turnover of the bidder during the last three years (FY 21-22,22-23,23-24), should not be less than Rs.700 Crore. The bidder should also have Positive Net Worth as on 31/03/2024. A certificate from a practicing Chartered Accountant (with UDIN) on its letter head confirming annual turnover, average turnover for 3 years as specified above and confirming positive net worth as on 31/03/2024 is to be provided along with the technical bid.	Please accept a certificate from Company Secretary instead of Chartered Accountant certificate.	No Change
274	84	Section VI: Qualification Criteria	A. Bidder’s Qualification Criteria 5. Bidder should have experience of successful implementation of Supply & Installation or operation and maintenance at 50 locations, of WAN setup in customer office premises in single or multiple orders in Central/State Government/ Govt. undertakings / UT’s /Autonomous Bodies/Public listed companies. Note i.r.o clause 4,5&6- Bidder shall provide relevant copies of the customer purchase orders in support of scope of work, deliverables, project value and satisfactory work completion certificate from client. Bidder shall also provide Name, Address, email and contact no. of organization whose Purchase orders are submitted by Bidder. Order Completion date/date(s) should fall between 01/11/2019 to 31/10/2024.	As some of the projects are under NDA, it is not feasible to share the customer artifacts (Customer purchase orders, Work order or Go-Live / Completion certificate from client / /Agreement/LOA/LOI). Similarly Name, Address, email and contact no. of organization whose Purchase orders are submitted by Bidder. Hence the bidder requests the following 1. Please allow to submit the anonymize project citations. 2. Please accept self-certificate signed by authorized signatory / Company Secretary stating the relevant experience details as a documentary evidence.	Kindly refer to respective updated clause in Annexure-B
275	91	4. High level Role and Responsibilities of contractor at New Data Centers (DC and DR)	xvii. Perform the security audit (including VAPT) and fix all security issues at the time of acceptance. VAPT should be performed once per yea	Please provide the cost for appointing the two Cert-in empaneled auditor will be borne by department?	Clause is self explanatory ; Additionally Cost for Auditor will be borne by the contractor ;

276	96	7. Role and Responsibilities of Contractor i.r.o AAA,AD,EMS and related software applications:	16) Contractor must provide & configure CA certificates from Verified CA store to allow both Internet and Intranet Access to software web based modules (such as EMS etc.) which are valid for the total duration of work on all applicable devices/servers to support SSL based encryption. The default access to EMS and other management modules provided should be via only Intranet, whereas in certain special cases, internet access to specific modules may be provided upon authorized requests& approvals in system (Helpdesk). **(Bidder is required to provide the CA certificates as per the applications provided for the overall RFP (including the applications sought in BoM))**	Please accept a certificate from Company Secretary instead of Chartered Accountant certificate.	Here CA means "Certifying Authority"
277	111	12.14 Dash boarding and Reporting	Half-Yearly reports 1) DC, DR & remote sites Security Audit Report. 2) IT infrastructure Upgrade / Obsolescence Report.	a. Kindly confirm, the half yearly audit will be conducted internally by bidder?	Refer Scope of Work
278	127	E. Security and Incident Management Service Levels for all DC	1 For every Virus attack reported and not resolved within 36 hrs from the time of attack	a. Kindly provide the scope of endpoints/servers in scope which bidder need to manage? B. Request clarification that solution like HIPS and Antivirus for servers will be provided by department?	Clause is self explanatory
279	127	E. Security and Incident Management Service Levels for all DC	For every instance of Data Theft, the bidder is subject to penalty and/or punishment applicable under the IT act/ ERNET India/CERT-In data theft policy or any other prevailing laws of the State/Country at that point of time, which shall be over and above the stated penalty.	The bidders will only be responsible for securing the infrastructure and software supplied by the bidder. Whereas, the data which will be part of the third party applications will be managed by the respective application owners.	Clause is self explanatory
280	61	12.1.5 Limitation of Liability	Except in cases of criminal negligence or wilful misconduct, the aggregate liability of the contractor to the ERNET India, whether under the contract, in tort or otherwise, shall not exceed the total Contract value, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment, or to any obligation of the contractor to indemnify the ERNET India concerning IPR infringement.	Consequential and Indirect liability should be excluded	No Change
281	124	Section VIII: Service Level Agreement during Operation & Maintenance		SLA Penalty is not capped for first 2 years	Incomplete Query

282	83	Section VI: Qualification Criteria	A. Bidder’s Qualification Criteria 3. Bidder should have experience of successful implementation of similar project(s) in Central/State Government/ Govt. undertakings/ UT’s/Autonomous Bodies/Public listed companies/reputed Private organisation in India as: Single order of Rs. Rs.500 Crore or more; OR Two orders each having minimum of Rs. 250Crore of estimated cost or more; OR Three orders each having minimum of Rs. 200Crore of estimated cost or more Similar Projects: - Setting up of Data Centre (including computing, storage & networking Infrastructure) / Ongoing Operation & Maintenance of Data Centres (done for minimum of two years)/ Completed or ongoing AMC of Data Center (done for minimum of two years)/ Network Operation Centres/ Security operation centres/ Smart City Projects/ Large IT networking.	As some of the projects are under NDA, it is not feasible to share the customer artifacts as they are confidential. Hence the bidder requests the following 1. Please allow to submit the anonymize project citations. 2. Please accept self-certificate signed by authorized signatory / Company Secretary stating the relevant experience details as a documentary evidence.	Kindly refer to respective updated clause in Annexure-B
283	83	Section VI: Qualification Criteria	A. Bidder’s Qualification Criteria 4. Bidder should have experience of successful implementation of data center with leaf and spine architecture in Central/State Government/ Govt. undertakings/ UT’s/Autonomous Bodies/Public listed companies/reputed Private organisation in India as: Single order of Rs. 100 Crore or more; OR Implemented 50 Rack with leaf and spine architecture or more; Note: This clause (4) is not applicable for those bidder(s), who are having experience of setting up of data center along with leaf and spine architecture as per clause no.3 above.	As some of the projects are under NDA, it is not feasible to share the customer artifacts (Customer purchase orders, Work order or Go-Live / Completion certificate from client / /Agreement/LOA/LOI). Similarly Name, Address, email and contact no. of organization whose Purchase orders are submitted by Bidder. Hence the bidder requests the following 1. Please allow to submit the anonymize project citations. 2. Please accept self-certificate signed by authorized signatory / Company Secretary stating the relevant experience details as a documentary evidence.	Kindly refer to respective updated clause in Annexure-B
284	83	Section VI: Qualification Criteria	A. Bidder’s Qualification Criteria 2. The minimum average annual audited financial turnover of the bidder during the last three years (FY 21-22,22-23,23-24), should not be less than Rs.700 Crore. The bidder should also have Positive Net Worth as on 31/03/2024. A certificate from a practicing Chartered Accountant (with UDIN) on its letter head confirming annual turnover, average turnover for 3 years as specified above and confirming positive net worth as on 31/03/2024 is to be provided along with the technical bid.	Please accept a certificate from Company Secretary instead of Chartered Accountant certificate.	No Change

285	84	Section VI: Qualification Criteria	A. Bidder’s Qualification Criteria 5. Bidder should have experience of successful implementation of Supply & Installation or operation and maintenance at 50 locations, of WAN setup in customer office premises in single or multiple orders in Central/State Government/ Govt. undertakings / UT’s /Autonomous Bodies/Public listed companies. Note i.r.o clause 4,5&6- Bidder shall provide relevant copies of the customer purchase orders in support of scope of work, deliverables, project value and satisfactory work completion certificate from client. Bidder shall also provide Name, Address, email and contact no. of organization whose Purchase orders are submitted by Bidder. Order Completion date/date(s) should fall between 01/11/2019 to 31/10/2024.	As some of the projects are under NDA, it is not feasible to share the customer artifacts (Customer purchase orders, Work order or Go-Live / Completion certificate from client / /Agreement/LOA/LOI). Similarly Name, Address, email and contact no. of organization whose Purchase orders are submitted by Bidder. Hence the bidder requests the following 1. Please allow to submit the anonymize project citations. 2. Please accept self-certificate signed by authorized signatory / Company Secretary stating the relevant experience details as a documentary evidence.	Kindly refer to respective updated clause in Annexure-B
286	91	4. High level Role and Responsibilities of contractor at New Data Centers (DC and DR)	xvii. Perform the security audit (including VAPT) and fix all security issues at the time of acceptance. VAPT should be performed once per yea	Please provide the cost for appointing the two Cert-in empaneled auditor will be borne by department?	Clause is self explanatory ; Additionally Cost for Auditor will be borne by the contractor ;
287	96	7. Role and Responsibilities of Contractor i.r.o AAA,AD,EMS and related software applications:	16) Contractor must provide & configure CA certificates from Verified CA store to allow both Internet and Intranet Access to software web based modules (such as EMS etc.) which are valid for the total duration of work on all applicable devices/servers to support SSL based encryption. The default access to EMS and other management modules provided should be via only Intranet, whereas in certain special cases, internet access to specific modules may be provided upon authorized requests& approvals in system (Helpdesk). **(Bidder is required to provide the CA certificates as per the applications provided for the overall RFP (including the applications sought in BoM))**	Please accept a certificate from Company Secretary instead of Chartered Accountant certificate.	CA referred here means "Certifying Authority" & not Chartered Accountant
288	111	12.14 Dash boarding and Reporting	Half-Yearly reports 1) DC, DR & remote sites Security Audit Report. 2) IT infrastructure Upgrade / Obsolescence Report.	a. Kindly confirm, the half yearly audit will be conducted internally by bidder?	Refer Scope of Work
289	127	E. Security and Incident Management Service Levels for all DC	1 For every Virus attack reported and not resolved within 36 hrs from the time of attack	a. Kindly provide the scope of endpoints/servers in scope which bidder need to manage? B. Request clarification that solution like HIPS and Antivirus for servers will be provided by department?	All services running in DC supplied as a part of this bid shall also commissioned in DR by contractor. Moreover , w.r.t All third party Applications at DC will be configured at DR as well.
290	127	E. Security and Incident Management Service Levels for all DC	For every instance of Data Theft, the bidder is subject to penalty and/or punishment applicable under the IT act/ ERNET India/CERT-In data theft policy or any other prevailing laws of the State/Country at that point of time, which shall be over and above the stated penalty.	The bidders will only be responsible for securing the infrastructure and software supplied by the bidder. Whereas, the data which will be part of the third party applications will be managed by the respective application owners.	Clause is self explanatory

291	25	.....	v. The EMD may be forfeited: ____________a) If the bid is withdrawn during the validity period or any extension ____________thereof agreed to by the bidder. ____________b) If the successful bidder fails to execute the contract or defaults on any ____________of its obligations. c) If the successful bidder fails to sign the contract and submit ____________Performance Bank Guarantee within the stipulated period. d) If the bid is varied or modified in a manner not acceptable to ERNET ____________India after opening of the bid during the validity period or any extension thereof. ____________e) Any violation/default by the bidders in respect of tender terms & ____________conditions may lead to rejection of the bid & forfeiture of EMD. vi. If the Bidder attempts to influence the evaluation process. ____________vii. EMD is to be submitted along with the bid by the bidders. Therefore, the ____________last date of submission of EMD will be the same as last date of submission ____________of the bids.	v. The EMD may be forfeited: ____________a) If the bid is withdrawn during the validity period or any extension thereof agreed to by the bidder. ____________b) If the successful bidder fails to execute the mutually agreed contract or defaults on any ____________of its obligations. ____________c) If the successful bidder fails to sign the mutually agreed contract and submit Performance Bank Guarantee within the stipulated period. ~~d) If the bid is varied or modified in a manner not acceptable to ERNET ____________India after opening of the bid during the validity period or any extension thereof. ____________e) Any violation/default by the bidders in respect of tender terms & conditions may lead to rejection of the bid & forfeiture of EMD.~~ ____________vi. If the Bidder attempts to influence the evaluation process. ____________vii. EMD is to be submitted along with the bid by the bidders. Therefore, the last date of submission of EMD will be the same as last date of submission ____________of the bids.	No Change
292	40	.....	5.5 Indemnities for breach of IPR Rights or from other issues ____________1) the contractor shall indemnify and hold harmless, free of costs, the ERNET India and ____________its employees and officers from and against all suits, actions or administrative proceedings, claims, demands, losses, damages, costs, and expenses of any nature, including attorney's fees and expenses, which may arise in respect of the Equipment provided by the contractor under this Contract, as a result of any infringement or alleged infringement of any patent, utility model, registered design, copyright, or other Intellectual Proprietary Rights (IPR) or trademarks, registered or otherwise existing on the date of the contract arising out of or in connection with: ____________a) any design, data, drawing, specification, or other documents or Equipment ____________provided or designed by the contractor for or on behalf of the ERNET India. ____________b) The installation of the Equipment by the contractor or the use of the Equipment at the ERNET India's / CERT-In/ other end user Sites. ____________2) If any proceedings are brought, or any claim is made against the ERNET India arising out of the matters referred above, the ERNET India shall promptly give the contractor a notice thereof. At its own expense and in the ERNET India's name, the contractor	5.5 Indemnities for breach of IPR Rights or from other issues ____________1) the contractor shall indemnify and hold harmless, free of costs, the ERNET India and its employees and officers from and against all suits, actions or administrative proceedings, claims, demands, losses, damages, costs, and expenses of any nature, including attorney's fees and expenses, which may arise in respect of the Equipment ____________provided by the contractor under this Contract, as a result of any infringement or ____________alleged infringement of any patent, utility model, registered design, copyright, or other Intellectual Proprietary Rights (IPR) or trademarks, registered or otherwise ____________existing on the date of the contract arising out of or in connection with: a) any design, data, drawing, specification, or other documents or Equipment ____________provided or designed by the contractor for or on behalf of the ERNET India. ____________b) The installation of the Equipment by the contractor or the use of the Equipment at the ERNET India's / CERT-In/ other end user Sites. ____________2) If any proceedings are brought, or any claim is made against the ERNET India arising out of the matters referred above, the ERNET India shall promptly give the contractor ____________a notice thereof. At its own expense and in the ERNET India's name, the contractor ____________may conduct such proceedings and negotiations to settle any such proceedings or ____________claim, keeping the ERNET India informed. ____________3) If the contractor fails to notify the ERNET India within twenty-eight (28) days after	No Change

293	41	.....	5.6.1 IPR Rights ____________All deliverables, outputs, plans, drawings, specifications, designs, reports, and other documents ____________and software submitted by the contractor under this Contract shall become and remain the property of the ERNET India/ CERT-In and must not be shared with third parties or reproduced, whether in whole or part, without the ERNET India/ CERT-In's prior written consent. The contractor shall, not later than upon termination or expiration of this Contract, deliver all such documents and software to the ERNET India/ CERT-In, together with a detailed inventory thereof.	5.6.1 IPR Rights ____________Subject to the provisions of this claue ~~A~~all deliverables, outputs, plans, drawings, specifications, designs, reports, and other documents and software submitted by the contractor under this Contract shall become and remain the property of the ERNET India/ CERT-In and must not be shared with third parties or reproduced, whether in whole or part, without the ERNET India/ CERT-In's prior written consent. The ____________contractor shall, not later than upon termination or expiration of this Contract, deliver all such ____________documents and software to the ERNET India/ CERT-In, together with a detailed inventory ____________thereof. ERNET acknowledges and agrees that this is a professional services agreement and this agreement is not intended to be used for licensing of any Bidder's proprietary software or tools. If Bidder and ERNET mutually agree that the Bidder provides to ERNET any proprietary software or tools of Bidder or of a third party, the parties shall negotiate and set forth the applicable terms and conditions in a separate license agreement and the provisions of this Section shall not apply to any deliverables related to customization or implementation of any such proprietary software or products of Bidder or of a third party. Further, ERNET acknowledges that in performing Services under this Agreement Bidder may use Bidder's proprietary materials including without limitation any software (or any part or component thereof), tools, methodology, processes, ideas, know-how and technology that are or were developed or owned by Bidder prior to or independent of the Services	No Change
294	49	.....	viii. The overall Penalties for non-adherence with the SLA of warranty support (during 3rd , 4th & 5th year of warranty period) per quarter shall be capped at a maximum of 25% of the respective Quarterly payment (CAPEX). In case penalty imposed on the contractor consecutively for two quarters reaches the maximum Penalty (i.e 25%) then in such an eventuality ERNET India reserves the right to terminate the Contract as per Clause 12.1 & 12.2.	viii. The overall Penalties for non-adherence with the SLA of warranty support (during ____________3rd , 4th & 5th year of warranty period) per quarter shall be capped at a maximum ____________of ~~2~~5% of the respective Quarterly payment (CAPEX). In case penalty imposed on the contractor consecutively for two quarters reaches the maximum Penalty (i.e ____________~~2~~5%) then in such an eventuality ERNET India reserves the right to terminate the Contract as per Clause 12.1 & 12.2. Notwithstanding anything contained in this Agreement the maximum aggregate penalty including LD shall not exceed five (5) percent of the value of the delayed or undelivered services and can be levied for reasons that are solely attributable to the Bidder.	No Change
295	55	.....	Note: Overall Liquidated Damages shall be restricted to 10% of the total contract value. While calculating LD; GST will be excluded from the value on ____________which LD is calculated; thereafter GST may be charged (if applicable) on the ____________LD value as per S.No. 4 clause 5.3 of Section II of this document. In case, delay ____________beyond 20 weeks, ERNET India may initiate termination for default and take ____________remedial action(s) accordingly as per GCC Clause 12.1. 3) ERNET India will serve a notice duly accompanied by a preliminary ca	Note: Overall Liquidated Damages shall be restricted to 1.0% of the total ____________contract value. While calculating LD; GST will be excluded from the value on which LD is calculated; thereafter GST may be charged (if applicable) on the ____________LD value as per S.No. 4 clause 5.3 of Section II of this document. In case, delay beyond 20 weeks, ERNET India may initiate termination for default and take ____________remedial action(s) accordingly as per GCC Clause 12.1. ____________3) ERNET India will serve a notice duly accompanied by a preliminary ca	Kindly refer to respective updated clause in Annexure-B

296	56	.....	10Prices and Payments Terms:	10Prices and Payments Terms: All payments due for more than thirty (30) days will attract an interest at the rate of 2 percent per month on the invoice amount calculated from the date the payment became due until the recovery is made in full with interest. Without prejudice to the other rights available, Bidder also reserves the right to withhold the provision of services till such time all the payments due to it under this Agreement have been made by ERNET and any such withholding by the Bidder shall not be treated as breach by it of the provisions of this Agreement.	No Change
297	60	.....	12.1.4 Contractual Remedies for Breaches/Defaults or Termination for Default ____________If there is an unsatisfactory resolution of the issues raised in the 'Notice of Default' within the period specified in the notice, then ERNET India may take any one; or more of the following contractual remedies. ____________1) Temporary withhold payments due to the contractor till recoveries due to invocation of other contractual remedies are complete. 2) Recover liquidated damages for delays. 3) Encash and/ or Forfeit performance or other contractual securities. ____________4) Debar the contractor from participation in future procurements as follows: ____________5) ERNET India may debar the contractor or any of its successors from participating in any Tender Process undertaken by it for a period not exceeding two years commencing from the date of debarment. Terminate contract for default, fully or partially including its right for Risk-and-Cost Procurement as per following sub-clau	12.1.4 Contractual Remedies for Breaches/Defaults or Termination for Default ____________If there is an unsatisfactory resolution of the issues raised in the 'Notice of Default' within the ____________period specified in the notice, then ERNET India may take any one; or more of the following ____________contractual remedies. 1) Temporary withhold payments due to the contractor till recoveries due to invocation of ____________other contractual remedies are complete. ____________2) Recover liquidated damages for delays. ____________3) Encash and/ or Forfeit performance or other contractual securities. ____________~~4) Debar the contractor from participation in future procurements as follows:~~ ~~5) ERNET India may debar the contractor or any of its successors from participating in any~~ ____________~~Tender Process undertaken by it for a period not exceeding two years commencing from~~ ____________~~the date of debarment. Terminate contract for default, fully or partially including its right~~ ____________~~for Risk-and-Cost Procurement as per following sub-clau~~ Bidder shall also have all such rights of termination which shall apply mutatis-mutandis apply on ERNET also.	No Change
298	60	.....	6) Risk and Cost Procurement: In addition to termination for default, the ERNET India shall be entitled, and it shall be lawful on its part, to procure Equipment and services similar to those terminated, with such terms and conditions and in such manner as it deems fit at the "Risk and Cost" of the contractor. Such 'Risk and Cost Procurement' will be contracted within nine months from the breach of Contract. The Contractor shall be liable for any loss which the ERNET India may sustain on that account provided the procurement, or, if there is an agreement to procure, such agreement is made. The Contractor shall not be entitled to any gain on such procurement, and the manner and method of such procurement shall be in the entire discretion of the ERNET India. It shall not be necessary for the ERNET India to notify the contractor of such procurement. It shall, however, be at the discretion of the ERNET India to collect or not the security deposit from the firm/ firms on whom the contract is placed at the risk and cost of the defaulted firm.	6) Risk and Cost Procurement: In addition to termination for default, the ERNET India ____________shall be entitled, and it shall be lawful on its part, to procure Equipment and services ____________similar to those terminated, with such terms and conditions and in such manner as it ____________deems fit at the "Risk and Cost" of the contractor. Such 'Risk and Cost Procurement' will be contracted within nine months from the breach of Contract. The Contractor shall be ____________liable for any loss which the ERNET India may sustain on that account provided the ____________procurement, or, if there is an agreement to procure, such agreement is made which loss shall be capped to two (2) percent of the value of such delayed services. The ____________Contractor shall not be entitled to any gain on such procurement, and the manner and ____________method of such procurement shall be in the entire discretion of the ERNET India. It shall not be necessary for the ERNET India to notify the contractor of such procurement. It ____________shall, however, be at the discretion of the ERNET India to collect or not the security ____________deposit from the firm/ firms on whom the contract is placed at the risk and cost of the ____________defaulted firm.	No Change

299	61	.....	12.1.5 Limitation of Liability Except in cases of criminal negligence or wilful misconduct, the aggregate liability of the contractor to the ERNET India, whether under the contract, in tort or otherwise, shall not exceed the total Contract value, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment, or to any obligation of the contractor to indemnify the ERNET India concerning IPR infringement.	12.1.5 Limitation of Liability Except in cases of criminal negligence or wilful misconduct, the aggregate liability of the ~~contractor~~Bidder to the ERNET India, whether under the contract, in tort or otherwise, shall not exceed the total amount paid to Bidder by the ERNET in the preceding twelve months under that applicable work that gives rise to such liability (as of the date the liability arose~~Contract value~~, provided that this limitation shall not apply to ~~the cost of repairing or replacing defective equipment, or to~~ any obligation of the ~~contractor~~Bidder to indemnify the ERNET India concerning IPR infringement. Bidder shall be excused and not be liable or responsible for any delay or failure to perform the services or failure of the services or a deliverable under this Agreement, to the extent that such delay or failure has arisen as a result of any delay or failure by the ERNET or its employees or agents or third party service providers to perform any of its duties and obligations as set out in this Agreement. In the event that Bidder is delayed or prevented from performing its obligations due to such failure or delay on the part of or on behalf of the ERNET, then Bidder shall be allowed an additional period of time to perform its obligations and unless otherwise agreed the additional period shall be equal to the amount of time for which Bidder is delayed or prevented from performing its obligations due to such failure or delay on the part of or on behalf of the ERNET. Such failures or delays shall be brought to the notice of the ERNET and subject to mutual agreement with the ERNET.	No Change
300	88	.....	Section VII: Scope of Work	Section VII: Scope of Work	Incomplete Query
301	144	.....	Subject: Terms & Conditions- Compliance 1) With reference to our Bid submitted against the above referred Tender no…………, we hereby confirm that we comply with all terms, conditions and specifications of the Tender Documents read in conjunction with Amendment(s)/Corrigendum(s) / Clarification(s) (if any) issued by ERNET India prior to last date of submission of bids and the same has been taken into consideration while submitting our bid and we declare that we have not taken any deviation in this regard. 2) We further confirm that any deviation, variation or additional conditions etc. or any mention, contrary to Bidding Documents and its Amendment(s)/Corrigendum(s) / Clarification(s) (if any) as mentioned at 1.0 above found anywhere in our bid, implicit or explicit, shall stand unconditionally withdrawn, without any cost implication whatsoever to ERNET India.	Subject: Terms & Conditions- Compliance 1) With reference to our Bid submitted against the above referred Tender no…………, we hereby confirm that subject to deviations we comply with ~~all~~ terms, conditions and specifications of the Tender Documents read in conjunction with Amendment(s)/Corrigendum(s) / Clarification(s) (if any) issued by ERNET India prior to last date of submission of bids and the same has been taken into consideration while submitting our bid and we declare that we have not taken any deviation in this regard. ~~2) We further confirm that any deviation, variation or additional conditions etc. or any mention, contrary to Bidding Documents and its Amendment(s)/Corrigendum(s) / Clarification(s) (if any) as mentioned at 1.0 above found anywhere in our bid, implicit or explicit, shall stand unconditionally withdrawn, without any cost implication whatsoever to ERNET India.~~	No Change
302	147	.....	MODEL BANK GUARANTEE FORMAT FOR FURNISHING EMD	MODEL BANK GUARANTEE FORMAT FOR FURNISHING EMD	Incomplete Query

303	151	.....	• If the Bidder(s)/Contractor(s), before award or during execution has committed a transgression through a violation of Section 2, above or in any other form such as to put his reliability or credibility in question, ERNET is entitled to disqualify the Bidder(s)/Contractor(s) from the tender process or take action as per the Government/ERNET India's procedure on banning of the business dealings/bidders/contractors, etc.	~~• If the Bidder(s)/Contractor(s), before award or during execution has committed a transgression through a violation of Section 2, above or in any other form such as to put his reliability or credibility in question, ERNET is entitled to disqualify the Bidder(s)/Contractor(s) from the tender process or take action as per the Government/ERNET India's procedure on banning of the business dealings/bidders/contractors, etc.~~	No Change
304	155	.....	1. This Agreement will apply to all confidential and proprietary information disclosed, owned or collected by one party to the other party, including information generated under this project, which the disclosing party identifies in writing or otherwise as confidential to the receiving party ("Confidential information"). Information consists of certain specifications, designs, plans, drawings and /or technical information, software, data etc, and all copies and derivatives containing such information, that may be disclosed to one another for and during the purpose, which a party considers proprietary or confidential ("Information"). Information may be in any form or medium, tangible or intangible, and may be communicated/disclosed in writing, orally, or through visual observation or by any other means to one party (hereinafter referred to as the receiving party) by the other party (hereinafter referred to as one disclosing party). Information shall be subject to this Agreement, if it is in tangible form, only if clearly marked as proprietary or confidential as the case may be, when disclosed to the receiving party or, if not in tangible form, its proprietary	1. This Agreement will apply to all confidential and proprietary information disclosed, owned or collected by one party to the other party, including information generated under this project, which the disclosing party identifies in writing or otherwise as confidential to the receiving party ("Confidential information"). Information consists of certain specifications, designs, plans, drawings and /or technical information, software, data etc, and all copies and derivatives containing such information, that may be disclosed to one another for and during the purpose, which a party considers proprietary or confidential ("Information"). Information may be in any form or medium, tangible or intangible, and may be communicated/disclosed in writing, ~~orally, or through visual observation or by any other means to one party~~ (hereinafter referred to as the receiving party) by the other party (hereinafter referred to as one disclosing party). Information shall be subject to this Agreement, if it is in tangible form, only if clearly marked as proprietary or confidential as the case may be, when disclosed to the receiving party or, if not in tangible form, its proprietary	No Change
305	157	.....	11. That in case of any dispute or differences, breach & violation relating to the terms of this agreement, the said matter or dispute, difference shall be referred to Director General, ERNET India for his decision in this regard. The decision of the Director General, ERNET India will be final and binding on both the parties.	~~11. That in case of any dispute or differences, breach & violation relating to the terms of this agreement, the said matter or dispute, difference shall be referred to Director General, ERNET India for his decision in this regard. The decision of the Director General, ERNET India will be final and binding on both the parties.~~	No Change
306	158	.....	14. This Agreement will remain in effect during the currency of agreement & shall survive even after expiry of the agreement or project.	14. This Agreement will remain in effect during the currency of agreement & shall survive for a period of two years even after expiry of the agreement or project.	No Change

307	160	.....	Format 1.1: Bank Guarantee Format for Performance Security	Format 1.1: Bank Guarantee Format for Performance Security ________ ________ This Bank Guarantee issued by ________ Bank, on behalf of the Contractor in favor of Purchaser is in respect of the Contract/agreement dated ________. As communicated by Contractor on the date of execution of this Bank Guarantee an amount of Rupees ________ (Rupees ________ only) is outstanding and payable to Contractor by Purchaser, in respect of pervious contracts between Contractor and Purchaser. As communicated by Contractor on the date of execution of this Bank Guarantee, there are no outstanding disputes related to any pervious contracts between Contractor and Purchaser. Notwithstanding anything contained hereinabove: a) Our liability under this Bank Guarantee shall not exceed and is restricted to Rs. ________ (Rupees ________ only) ________ b) This Guarantee shall remain in force up to and including ________ (including claim period of three months) ________ c) Unless the demand/claim under this guarantee is served upon us in writing before ________ all the rights of Purchaser under this guarantee shall stand automatically forfeited and we shall be relieved and discharged from all liabilities mentioned hereinabove.	No Change
308		Additional Clause	Additional Clause	**Following clauses needs to be submitted with the prebid queries/ deviations /proposal.** **Execution Infrastructure** The ERNET will provide necessary and adequate infrastructure to enable Bidder to fulfill its commitment for the assignment. This will be applicable for each Bidder Consultant associated with the project and will be arranged for and provided at no cost to Bidder. The infrastructure will include: i. Office space; ii. Hardware and software; iii. Computer consumable including stationery, printer ribbons/toner, magnetic storage media such as floppy disks, tapes, cartridges, DATs; iv. Office stationery and consumable; v. Secretarial assistance, if necessary at site; vi. Telephone, e-mail and fax facilities at site; vii. Photocopying assistance; viii. Meeting Room facilities including room equipped with a writing board, seating arrangements, computers/ terminals, overhead projector and consumables. (pl. mention if any additional infrastructure is to be provided). The above-mentioned infrastructure will be required for work to be carried out at the site of ERNET during regular working hours. ERNET shall make arrangements to provide for the same beyond these hours such as after regular	No Change; Sitting Facility at DC & DR and ERNET India office, Delhi will be provided by ERNET India
309	124	Section VIII: Service Level Agreement during Operation & Maintenance		SLA Penalty is not capped for first 2 years	No Change

310	97	Section VII: Scope of Work 8. General Activities to be performed by Contractor for the project:, 12	The bid should include OEM professional services for the successful implementation of project. The OEM professional services shall include but not limited to solution architecture, design, installation, preparation of acceptance test plan & procedure with expected results and end user training leading to OEM Certification. The above activities should be jointly done by the Contractor and the OEM, as per the best security practices for the final acceptance.	Installation of the passive structured cabling and AIM system is implemented by OEM certified system integrators for most OEMs if not all. Therefore passive OEMs do not provide professional services as part of their offerings. OEMs can help and offer technical guidance to the system integrators. It is requested that Passive Structured Cabling and AIM OEMs be exempted from this clause. The clause should be amended to the following: The bid should include OEM professional services (except for Passive Structured Cabling and AIM) for the successful implementation of project. The OEM professional services shall include but not limited to solution architecture, design, installation, preparation of acceptance test plan & procedure with expected results and end user training leading to OEM Certification. The above activities should be jointly done by the Contractor and the OEM, as per the best security practices for the final acceptance. For Passive OEMs, Site audit monthly will be mandatory	No Change
311	83	Section VI (A) (3) Bidder's Qualification Criteria	Bidder should have experience of successful implementation of similar project(s) in Central/State Government/ Govt. undertakings/ UT's/Autonomous Bodies/Public listed companies/reputed Private organisation in India as: Single order of Rs. Rs.500 Crore or more; OR Two orders each having minimum of Rs. 250Crore of estimated cost or more; OR Three orders each having minimum of Rs. 200Crore of estimated cost or more	Bidder should have experience of successul implementation of similar project(s) in Central/State Government/Govt. undertaking/UT's/ Autonomous Bodies/Public listed companies/reputed Private organization in India as: **Single order of Rs. 400 Crore or more.**	Kindly refer to respective updated clause in Annexure-B
312	84	Section VI (A)(5) Bidder's Qualification Criteria	Bidder should have experience of successful implementation of Supply & Installation or operation and maintenance at 50 locations, of WAN setup in customer office premises in single or multiple orders in Central/State Government/ Govt. undertakings / UT's /Autonomous Bodies/Public listed companies.	Bidder should have experience of successful implementation of Supply & Installation or operation and maintenance at **25 locations**, of WAN setup in customer office premises in single or multiple orders in Central/State Government/ Govt. undertakings / UT's /Autonomous Bodies/Public listed companies.	Kindly refer to respective updated clause in Annexure-B
313	83	A. Bidder's Qualificat	3. Bidder should have experience of successful implementation of similar project(s) in Central/State Government/ Govt. undertakings/ UT's/Autonomous Bodies/Public listed companies/reputed Private organisation in India as: Single order of Rs. Rs.500 Crore or more; OR Two orders each having minimum of Rs. 250Crore of estimated cost or more; OR Three orders each having minimum of Rs. 200Crore of estimated cost or more	We request you to kindly ammend clause as: Bidder should have experience of successful implementation/ **Maintenance** of similar project(s) in Central/State Government/ Govt. undertakings/ UT's/Autonomous Bodies/Public listed companies/reputed Private organisation in India as: Single order of Rs. Rs.350 Crore or more; OR Two orders each having minimum of Rs. 150Crore of estimated cost or more; OR Three orders each having minimum of Rs. 100Crore of estimated cost or more	Kindly refer to respective updated clause in Annexure-B

314	83	A. Bidder’s Qualificat	Bidder should have experience of successful implementation of data center with leaf and spine architecture in Central/State Government/ Govt. undertakings/ UT’s/Autonomous Bodies/Public listed companies/reputed Private organisation in India as: Single order of Rs. 100 Crore or more; OR Implemented 50 Rack with leaf and spine architecture or more;	We request you to kindly ammend clause as: Bidder should have experience of successful implementation/ **Maintenance** of data center with leaf and spine architecture in Central/State Government/ Govt. undertakings/ UT’s/Autonomous Bodies/Public listed companies/reputed Private organisation in India as: Single order of Rs. 100 Crore or more; OR Implemented 50 Rack with leaf and spine architecture or more.	Kindly refer to respective updated clause in Annexure-B
315	84	A. Bidder’s Qualificat	Bidder should have experience of successful implementation of Supply & Installation or operation and maintenance at 50 locations, of WAN setup in customer office premises in single or multiple orders in Central/State Government/ Govt. undertakings / UT’s /Autonomous Bodies/Public listed companies.	We request you to kindly ammend clause as: Bidder should have experience of successful implementation of Supply & Installation or operation and maintenance at 50 locations, of WAN/**LAN** setup in customer office premises in single or multiple orders in Central/State Government/ Govt. undertakings / UT’s /Autonomous Bodies/Public listed companies.	Kindly refer to respective updated clause in Annexure-B
316	84	A. Bidder’s Qualificat	The bidder must have following professional* working on its payroll: a. Prince-2/ PMP - 5 numbers b. CISA/CISSP/CISM - 2 numbers c. CDCP - 2 numbers d. CCIE-Sec/JNCIE-Sec - 1 numbers e. CCIE-ENT/JNCIE-ENT - 1 numbers f. CCIE-DC/CCNP-DC/JNCIE-DC/JNCIP-DC - 2 numbers g. CCNP-Sec/ JNCIP-Sec/Fortigate NSE-4/PCNSE - 3 numbers h. CCNP-ENT/ JNCIP-ENT - 3 numbers	We request you to kindly ammend clause as: The bidder must have following professional* working on its payroll: a. Prince-2/ PMP - 2 **numbers** b. CISA/CISSP/CISM - 4 numbers c. CCIE-DC/CCNP-DC/JNCIE-DC/JNCIP-DC/**CCNP-Routing Switching - 1 number**s d. CCNP-ENT/ JNCIP-ENT/**CEH** - 3 numbers	Kindly refer to respective updated clause in Annexure-B
317	85	Clause 8 of Bidder’s Qualification Criteria	The bidder on the date of publishing of this bid; should already have in-house capabilities to discharge the roles & responsibilities as a System Integrator. Therefore, the bidder is not allowed to float any EoI or Tender against this Tender requirement for identifying any system integrator, consultant, empanelment, sub-contractor or a partner or a teaming partner etc by whatever name called; for discharging/sharing its responsibilities as a System Integrator. Further, it may also be noted that consortium, arrangements, joint- ventures, teaming, subletting, sub- contracting is strictly prohibited in this bid. In case, at any stage of the project, if its identified that any kind of above mentioned prohibitions were violated, ERNET India reserves the right to take suitable actions such as mentioned in Section III Clause 12. The bidder needs to submit an undertaking in this regard.	RailTel is a Navratna PSU. We own and manage two Tier – III Certified Data Centres for more than 5 (Five) Years. RailTel has the requisite skillset and capability to execute such Data Centre infrastructure projects. RailTel has undertaken and executed such Data Centre Projects and also maintaining the same, however for arranging the material from MNCs, petty work like cabling, RailTel engages supply chain vendors following the due process. Considering the above, may kindly exempt PSUs having owned Data Centres and currently being used for commercial purpose.	No Change; Refer to Clause "5.4 Assignment and Sub-contracting" .

318	40	Point 5.4 of Clause 5 of Contractor's Obligations and restrictions on its Rights	All the manpower to be deployed in project for delivery, installation, testing & commissioning and operation & maintenance including onsite support should be on the payroll of the Contractor or OEM whose equipment(s) are offered. Outsourcing of manpower will not be allowed.	Attrition of skilled tech resources is high. PSUs have to follow due process for onboarding/replacement of these resources which is a time taking process. This may adversely affect day-to-day critical DC operations Considering the above, may kindly revise the clause to ”should be on the payroll of the Contractor or authorised partner of the contractor or OEM whose equipment(s) are offered.”	No Change
319	83	Clause 3 of Bidders Qualification Criteria	Bidder should have experience of successful implementation of similar project(s) in Central/ State Government/ Govt. undertakings/ UT's/ Autonomous Bodies/ Public listed companies/ reputed Private organisation in India as: Single order of Rs. 500 Crore or more; OR Two orders each having minimum of Rs. 250 Crore of estimated cost or more;OR Three orders each having minimum of Rs. 200 Crore of estimated cost or more	Bidder should have experience of successful implementation of similar project(s) in Central/State Government/ Govt. undertakings/ UT's/Autonomous Bodies/Public listed companies/reputed Private organisation in India as: Single order of Rs. Rs.500 Crore or more; OR Two orders each having minimum of Rs. 250 Crore of estimated cost or more;OR Three orders each having minimum of Rs. 150 Crore of estimated cost or more	Kindly refer to respective updated clause in Annexure-B
320	57	b. of Point 6 of Clause 10 of GCC	In respect of DC and DR equipment (s), 50% of the value of equipment(s) delivered at DC and similarly 50% of the value of equipment(s) delivered at DR shall be released only after submission of BG equivalent to the amount which is to be released. The BG should be valid for a minimum period of 6 months (with a claim period of additional 3 months). BG must be extendable till the successful completion of rack mounting & Power On Self-Test (POST) of active equipment.	In respect of DC and DR equipment (s), 50% of the value of equipment(s) delivered at DC and similarly **70%** of the value of equipment(s) delivered at DR shall be released only after submission of BG equivalent to the amount which is to be released. The BG should be valid for a minimum period of 6 months (with a claim period of additional 3 months). BG must be extendable till the successful completion of rack mounting & Power On Self-Test (POST) of active equipment.	No Change
321	57	c. of Point 6 of Clause 10 of GCC	In respect of equipment (s) at DC and DR, additional 30% of the total value of items will be made after successful installation, integration, commissioning and acceptance as per the respective milestone(s).	In respect of equipment (s) at DC and DR, additional **10%** of the total value of items will be made after successful installation, integration, commissioning and acceptance as per the respective milestone(s).	No Change
322	84	Clause 5 of Bidders Qualification Criteria	Note i.r.o clause 4, 5 & 6 – Bidder shall provide relevant copies of the customer purchase orders in support of scope of work, deliverables, project value and satisfactory work completion certificate from client. Bidder shall also provide Name, Address, email and contact no. of organization whose Purchase orders are submitted by Bidder. Order Completion date/date(s) should fall between 01/11/2019 to 31/10/2024.	Kindly clarify if the work orders required under Clause 3 of Bidders Qualification Criteria falls under order completion period of 01/11/2019 to 31/10/2024 as mentioned here.	Kindly refer to respective updated clause in Annexure-B
323	51	Point 9.2 of Clause 9 of Terms of Delivery and Delays	DC and DR location is under finalisation and remote sites are spread across India where the Equipment are to be delivered have been stipulated in the Section IV – Bill of Material.	If the locations for New DC and New DR are finalised kindly communicate the same.	DC & DR location is yet to be finalised. However DC/DR location will be tier-I/II cities of India. Further Remote locations are spreaded across India

324	168	Form 12 Financial Bid (BoQ)	In case a bidder quotes a solution of higher specifcations than sought specifications , bidder needs to ensure that all specifications / features / functionality/ relevant hardware/SFPs must be delivered , installed & commissioned. E.g instead of 24 port switch , a 48 port switch is quoted by a bidder, he needs to populate SFPs for 48 ports before offering the milestone for delivery	Requesting to remove this clause as the minumum qualifying criteria in terms of feature , interfaces and SFP is already mentioned in the respective section. In case a bidder is quoting 48 port switch to meet the 24 port requirement due to model limitation, then this cluase will increase the overall commercials of the quoted product.	This clause stands deleted
325		Add New Clause	Add New Clause	Request to Add New Clause **Sub-contracting:** **Prime Bidder may be allowed to sub-contract the work to any other System Integrator. However, Ownership of the project will be remain with the Prime Bidder**.	No Change
326	83	A. Bidder's Qualification Criteria | Clause No: 2 Bidder's Average Turnover	The minimum average annual audited financial turnover of the bidder during the last three years (FY 21-22,22-23,23-24), should not be less than Rs.700 Crore. The bidder should also have Positive Net Worth as on 31/03/2024. A certificate from a practicing Chartered Accountant (with UDIN) on its letter head confirming annual turnover, average turnover for 3 years as specified above and confirming positive net worth as on 31/03/2024 is to be provided along with the technical bid.	We kindly request you to reconsider the minimum average annual audited financial turnover requirement of ₹700 Crores and revise it to ₹250 Crores. This request is in alignment with the General Financial Rules (GFR), which recommend that the financial capability criteria for bidders should not exceed 30% of the estimated project value.	No Change
327	83	A. Bidder's Qualification Criteria | Clause No: 3 Bidder's Experience	Bidder should have experience of successful implementation of similar project(s) in Central/State Government/ Govt. undertakings/ UT's/Autonomous Bodies/Public listed companies/reputed Private organisation in India as: Single order of Rs. Rs.500 Crore or more; OR Two orders each having minimum of Rs. 250Crore of estimated cost or more; OR Three orders each having minimum of Rs. 200Crore of estimated cost or more	We kindly request you to consider relaxing the requirements as follows: Single project: ₹400 Crores (instead of ₹500 Crores) Two projects: ₹200 Crores each (instead of ₹250 Crores each) Three projects: ₹150 Crores each (instead of ₹200 Crores each) This will increase and encourage the broader participation.	Kindly refer to respective updated clause in Annexure-B
328	83	Generic	Consortium Participation	Considering the scope, scale, and sanctity of this project, we respectfully request you to allow consortium participation for the tender. Justification for Allowing Consortium: • Enhancement capability and expertise • Alignment with project scale • Encouraging participation • Risk Mitigation	No Change
329	83	A. Bidder's Qualification Criteria | Clause No: 2 Bidder's Average Turnover	The minimum average annual audited financial turnover of the bidder during the last three years (FY 21-22,22-23,23-24), should not be less than Rs.700 Crore. The bidder should also have Positive Net Worth as on 31/03/2024. A certificate from a practicing Chartered Accountant (with UDIN) on its letter head confirming annual turnover, average turnover for 3 years as specified above and confirming positive net worth as on 31/03/2024 is to be provided along with the technical bid.	We kindly request you to reconsider the minimum average annual audited financial turnover requirement of ₹700 Crores and revise it to ₹250 Crores. This request is in alignment with the General Financial Rules (GFR), which recommend that the financial capability criteria for bidders should not exceed 30% of the estimated project value.	No Change

330	83	A. Bidder's Qualification Criteria | Clause No: 3 Bidder's Experience	Bidder should have experience of successful implementation of similar project(s) in Central/State Government/ Govt. undertakings/ UT's/Autonomous Bodies/Public listed companies/reputed Private organisation in India as: Single order of Rs. Rs.500 Crore or more; OR Two orders each having minimum of Rs. 250Crore of estimated cost or more; OR Three orders each having minimum of Rs. 200Crore of estimated cost or more	We kindly request you to consider relaxing the requirements as follows: Single project: ₹400 Crores (instead of ₹500 Crores) Two projects: ₹200 Crores each (instead of ₹250 Crores each) Three projects: ₹150 Crores each (instead of ₹200 Crores each) This will increase and encourage the broader participation.	Kindly refer to respective updated clause in Annexure-B
331	83	Generic	Consortium Participation	Considering the scope, scale, and sanctity of this project, we respectfully request you to allow consortium participation for the tender. Justification for Allowing Consortium: • Enhancement capability and expertise • Alignment with project scale • Encouraging participation • Risk Mitigation	No Change
332	89	Section VII: Scope of Work	To configure and establish MPLS/ P2P / ILL Links connectivity at DC, DR and 100+ remote locations & configure the sought P2P & ILL Links. Please note that ERNET India will arrange MPLS P2P & ILL service provider, however, integration of supplied hardware with MPLS, P2P & ILL links will be the responsibility of contractor.	According to clause, we have to only configure and managed the Links not supply.	Clause is self explanatory ; Supply of Links is bandwidth service provider's responsibility.
333	89	Section VII: Scope of Work	ii. Operation and maintenance of existing IT infrastructure* for two years.	Please clarify if ERNET has direct OEM service support for the existing infrastructure to facilitate its operation and maintenance for the same duration.	Warranty of existing IT infrastructure is in place.
334	87	Section VI: Qualification Criteria : B. Original Equipment Manufacturer (OEM)'s Criteria: Point No:2	The annual average financial turnover of the Server OEM; during the last three years (FY 21-22, 22-23, 23-24), on standalone basis ;should not be less than Rs.350 Cr. A certificate from a practicing Chartered Accountant (with UDIN of the CA) on its letter head confirming annual turnover and average annual turnover have to be provided along with the bid. In case the OEM has been incorporated in a country outside India then specified financial detail needs to be provided in INR by converting the foreign currency with INR.	The annual average financial turnover of the Server OEM; during the last three years (FY 21-22, 22-23, 23-24), on standalone basis ;**should not be less than Rs.200 Cr.** A certificate from a practicing Chartered Accountant (with UDIN of the CA) on its letter head confirming annual turnover and average annual turnover have to be provided along with the bid. In case the OEM has been incorporated in a country outside India then specified financial detail needs to be provided in INR by converting the foreign currency with INR.	No Change
335	300	42.Technical Requirements - Support & Services	The OEM is responsible for driving an onsite quarterly audit of the deployment to ensure that system is functional and used optimally.	Generally OEM are doing audits twice in a year for reviewing the sizing and utility. Please review agiant and confirm if we should do quarterly or once in a six month.	No Change
336	179	Annexure-1 (Technical Specifications)	l. Only the Manpower on OEM payrolls shall perform network planning, designing, implementation, integration and testing/validation for all Networking equipment(s) i.e. only direct OEM payroll manpower would be allowed to work on the project's designing, implementation & testing phase. An undertaking for same shall be provided.	our understaning of this clause is OEM will be responsible for network planning, designing, implementation, integration and testing/validation for all Networking equipment(s).Is it for Only Network Equipment or all project component.	These activities needs to accomplished only by networking OEM Manpower , in consultations with all other OEMs in the project , ERNET India , CERT-In & other experts.

337	179	Annexure-1 (Technical Specifications)	The hardware equipment proposed to be supplied in this bid should be compatible, stackable i.e. rack mountable inside a standard sized 42-U rack.	The server specifications mention Rail Kits to be supplied. Please confirm if bidder needs to supply racks as well for the proposed hardware, or if racks would be made available by ERNET.	In survey, if it is found that at any remote location, rack is not availbale to keep equipment then Racks will beprovisioned at such location. At DC &DR , Racks will be provided by ERNET India.
338	97	Bill of Material, Part(D)	Training with Certification from Authorized Certification Bodies	1.What will be the mode of training Classroom or Virtual? 2.If Classroom, training location / city for the training? 3.Will ERNET provide training venue with all teaching aids including desktop/pc/laptop for all participants? 4.What will be minimum and maximum batch size for each training session? 5.With regards to GIAC Certifications (GCIH/ GMON/ GSOC /GCFA/GDSA /GNFA/ GDSA /GCTI, etc): All these certifications required for 25 participants each training or total of 25 participants spread across these trainings? 6.With regards to EC Council/COMPTIA Trainings and Certification (CPENT, CEH, CHFI, Certified SOC Analyst, CCISO,CASP+, CYSA+ etc): All these certifications required for 50 participants each training or total of 50 participants spread across these trainings?	Instructor led Classroom Trainings in Delhi during the duration of the contract scheduled as per convience of ERNET India /CERT-In; Refer to the clause for specific number. The total number of such(GIAC Certifications (GCIH/ GMON/ GSOC /GCFA/GDSA /GNFA/ GDSA /GCTI, etc) trainings will be 25 i.e. total of 25 participants spread across these trainings The total number of such (EC Council/COMPTIA Trainings and Certification (CPENT,CEH,CHFI,Certified SOC Analyst, CCISO,CASP+,CYSA+ etc) trainings will be 50 i.e. total of 50 participants spread across these trainings .
339	89	Section VII,Scope of Work of contractor, (1) Project overview, Pt IV	Migration of 80 Links from existing DC & DR to New DC & DR	1. Please specify mapping of links which are getting migrated. 2. Are the 80 remote sites connecting to these existing DC, DR to be decommissioned and integrated to new DC, DR . Is this 80 count is coming out of 380 remote sites already integrated ? 3. Mention location of 80 remote sites to be disintegrated and moved to new DC DR ?	1. Details will be shared with successful bidder. Yes these 80 remote sites will be connected to exisiting DC&DR. 2. Yes count is coming out of 380. 3. The movement doesn't require any hardware movement. It will be logically moved from old dc-dr to new dc-dr.
340	89	Section VII,Scope of Work of contractor, (1) Project overview, Pt Vi	Provisioning of Co-Location Services w.r.t New DC and DR.	1. Specify the location details for colocation of new DC, DR ? 2. For this project, this is not expansion in existing DC, DR. we need location of new DC, DR ? 3. is it collocation for this new DC, DR ? As per our understanding , ERNET will provide Rack in new DC/DR. Is this understanding correct ?	Locations for the new DC,DR are not yet finalized, but these will be in Tier-I & Tier-II; This is not expansion of existing DC-DR. ERNET India is looking for Colo Services ; which will include Racks,Power,Cooling.
341	89	Section VII,Scope of Work of contractor, (1) Project overview, Pt IV , Pt I	To setup , commission and integrate IT Infrastructure/equipment(s) & solutions of DC, DR and 100+ remote locations.	1. Specify the location details of each site 2. is it 100+ new sites Or as per pricing table is it 34 new sites ?	Locations for the new remote sites will be in Tier-I & Tier-II; Pls refer to the updated clause ; 100 may be read as 34.
342	89	Section VII,Scope of Work of contractor, (1) Project overview, Pt Vi, Pt II	To configure and establish MPLS/ P2P / ILL Links connectivity at DC, DR and 100+ remote locations & configure the sought P2P & ILL Links. Please note that ERNET India will arrange MPLS P2P & ILL service provider, however, integration of supplied hardware with MPLS, P2P & ILL links will be the responsibility of contractor	Please clarify as Price format is not having line items for remote 100 + branches	Presently in the Bidder's scope is to connect 34 sites. Other sites will fall in O&M scope of bidder.
343	91	4. High level Role and Responsibilities of contractor at New Data Centers (DC and DR), Pt VII	If required, for specific use cases integrate the existing IT infrastructure with the equipment(s) planned in this tender.	specify the integration scope for existing infrastructure to new DC, DR	Clause is self explanatory

344	92	4. High level Role and Responsibilities of contractor at New Data Centers (DC and DR), Pt XI	Installation, Commissioning and Integration of AIM, EMS, PATS, & other relevant software solutions with complete IT infra.	Do we need to onboard existing devices as well to new EMS, IPAM being supplied ?	No ; Only REST APIs need to be consumed in new EMS for integrating the old EMS with new EMS to show Single Dashboard view for oldDC,oldDR,new DC, new DR & old& new remote sites.
345	91	4High level Role and Responsibilities of contractor at New Data Centers (DC and DR), PT (viii)	Contractor to provide the necessary support & facilitate the installation of the OS on the supplied servers.	The specifications of servers to be supplied ask for certifications for different OS / Virtualization platforms etc. but do not require any such licenses to be supplied along with the servers. Please confirm if bidder needs to supply any licenses for OS etc., or if the mentioned OS licenses would be supplied by ERNET. Compatibility with the supplied hardware will also need to be verified before OS can be installed on them.	Bidder doesn't need to provide any Licenses. Compatability has been sought in this bid ; Bidders need to take care of it with respective OEMs.
346	89	Section VII,Scope of Work of contractor, (1) Project overview, Pt(i)	To setup , commission and integrate IT Infrastructure/equipment(s) & solutions of DC, DR and 100+ remote locations	Is count of remote site is 100+ as per "PART-C(OPEX)" of RFP new sites count is 34	Refer to the revised clause ; 100 may be read as 34
347	102	12 : Scope of Work for Operation and Maintenance	Scope of Work for Operation and Maintenance	So can we consider handover date as Live date for operations for which Bidder would be starting invoicing against the resources.	Refer to Tender Clauses ; A Successful Acceptance testing will lead to start date of O&M.
348	115	13.2 Minimum Manpower to be deployed for two year(s) from the start of Operation and maintenance	Manpower At Existing Data Center (DC)	As per asked in table, resources are not being required for 24 x7 for some roles i.e. Security specialist, Network specialist & server maintenance specialist. So please confirm if 24x7 is not required for the mentioned roles and therefore requried as in mentioned time slot/slots.	Manpower is required as per the requirements mentioned in the tender clause
349	115	13.2 Minimum Manpower to be deployed for two year(s) from the start of Operation and maintenance	Manpower At Existing Disaster recovery Data Center (DR)	As per asked in table, resources are not being required for 24 x7 for some roles i.e. Security specialist, Network specialist, server maintenance specialist, EMS Engineer and Help desk support staff resp. So please confirm if 24x7 is not required for the mentioned roles and therefore requried as in mentioned time slot/slots.	Manpower is required as per the requirements mentioned in the tender clause
350	116	13.2 Minimum Manpower to be deployed for two year(s) from the start of Operation and maintenance	Manpower At New Data Center (DC)	As per asked in table, resources are not being required for 24 x7 for some roles i.e. OEM Security specialist,Security specialist, Network specialist and OEM server maintenance specialist. So please confirm if 24x7 is not required for the mentioned roles and therefore requried as in mentioned time slot/slots.	Manpower is required as per the requirements mentioned in the tender clause
351	116	13.2 Minimum Manpower to be deployed for two year(s) from the start of Operation and maintenance	Manpower At New Disaster recovery Data Center (DR)	As per asked in table, resources are not being required for 24 x7 for some roles i.e. OEM Security specialist,Security specialist, Network specialist and OEM server maintenance specialist. So please confirm if 24x7 is not required for the mentioned roles and therefore requried as in mentioned time slot/slots.	Manpower is required as per the requirements mentioned in the tender clause
352	128	Sec VIII Service Level Agreement during Operation & Maintenance PT (F)	Manpower Service Level Agreement	Operation and Maintenance billing will be started only after minimum 75% deployment (atleast 1 manpower of each line item) - Can this criteria be lower to 50% deployment to start the Operation and Maintenance billing.	No Change
353	109	12.12 Change management Services	Change Management :Plan for changes to be made - draw up a task list, decide on responsibilities, coordinate with all the affected parties, establish and maintain communication between parties to identify and mitigate risks, manage the schedule, execute the change, ensure and manage the port change tests and regular updates w.r.t changes should be documented in knowledge bank.	Please confirm the number of change request per month which are dependent on Applications/Security/Infrastruture/EMS/DCIM etc.	Contractor will not be responsible for change requests in the application s/w . Contractor's responsibility will be to ensure the required IT Infra is available 24x7 to run these applications (being supplied by CERT-In). Accordingly the total CRs will depend primarily upon the performance of IT infra supplied & Configuration Change requests .

354	49	14 (VIII):SLA during warranty period and penalties for breach thereof:	The overall Penalties for non-adherence with the SLA of warranty support (during 3rd , 4th & 5th year of warranty period) per quarter shall be capped at a maximum of 25% of the respective Quarterly payment (CAPEX). In case penalty imposed on the contractor consecutively for two quarters reaches the maximum Penalty (i.e 25%) then in such an eventuality ERNET India reserves the right to terminate the Contract as per Clause 12.1 & 12.2.	As per industry standard and customer's other tenders, the maximum cap of penalty is 10%. Please change it to 10%.	No Change
355	187	Form 12 Financial Bid,Web Server (Category 03)	Power Supply: Redundant, maximum rated power upto 1600 W	It should be max. 2400W, The consumed power requirement will increase as per configuration. Hence requesting the change.	No Change
356	89	Section VII: Scope of Work, 2. Scope of Work of Contractor	xvi. Migration of 80 remote sites connected from existing DC, DR to new DC, DR	Please specify, Counts of VMs to be migrated and total capacity of storage to be migrated, Any P2V is also required, Also please specify Is there any Live migration is required or Downtime/maintance window will be provided at that time.	Migration of 80 remote sites from existing DC, DR to new DC, DR will require the configuration changes only at DC & DR equipments. VM/Storage migration during this activity will not be performed by contractor & instead facilitation w.r.t networking configruations & asset inventory level changes etc. will be required to be done by contractor .
357	108	12.9 Network Managed Service including security Incident lifecycle Management	vi 24x7x365 monitoring of the network to spot the problems immediately.	Bidder shall also factor monitoring tool for all links/b/w or tool will be provided by the Ernet. Also if there is any API Bonding done between the monitoring tool and ISP for auto ticket logging.	Clause is self explanatory ; Tools are being procured via this bid & other tools will also be procured in future to help quicker response/actions by contractor's manpower. Contractor's manpower needs to ensure all best practices & SoPs also to avoid problems. As of now , No Bonding exisits between the exisiting monitoring tool and ISP for auto ticket logging.
358	109	12.10 Remote site support	Any shifting of site till the time of completion of O&M will be done by Contractor, if required	Bidder need to be provided with details of shifting till the time O&M will be done by Contractor	Clause is self explanatory
359	109	12.10 Remote site support	Further , this is clarified that once equipment are installed and accepted by ERNET India thereafter, Intracity shifting will be the bidder's responsibility and Intercity shifting will be the end user's responsibility.	For Intra City shifting, how many times the shifting will done and what all devices bidder need to shift. Will logistic support also provided by Bidder?	It may be applicable for 5 to 10 sites only
360	108	12.9 Network Managed Service including security Incident lifecycle Management	MIS and SLA reports shall be provided by Contractor via automated tool in dashboard.	ERNET to confirm if the automated tool to factored by bidder or not?	Refer BoQ & Technical Specifications EMS & Other Solutions being sought via this bid will be used for generating different reports including MIS and SLA reports .
361	112	13 Manpower required at DC , DR, Delhi & other loca	The bidder needs to provide Project management Tool such as JIRA/Microsoft's Project Plan etc for planning, tracking / monitoring the project status , issues , dependencies etc. The tool shall be installed on-Premises allowing different projects to tracked & shall allow atleast 50 simultaneous user.	Please confirm if ERNET will provide with required infratsructure for deployment of tool like JIRA/Mircrosoft Project Plan.	Contractor need to provide the IT infrastructure
362	127	Section VIII: Service Level Agreement during Operation & Maintenance	The overall Penalties (for Clause 1-A,B,C,D in Section-VIII) per quarter shall be capped at a maximum of 25% of the respective Quarterly payment of Grand Total Value. In case penalty imposed on the contractor consecutively for two quarters reaches the maximum Penalty (i.e 25%) then in such an eventuality ERNET India reserves the right to terminate the Contract as per Clause 12.1 & 12.2 of Section-III	Request ERNET to cap penalty at 5 % insteaf of 25 % of the respective quarterly Payment.	No Change
363	166	Form 12 Financial Bid, Intelligent cabling	Intelligent cabling	1. Please provide the cabling length and type of the cables required for passive supply. 2. Also who will do all intra and inter-rack cabling for passive services 3. Do we need to supply new racks for new DC DR ?	Racks including Power, Cooling etc for new DC and DR will be provided by Colo Services Contractor. The bidder's need to consider the effort & resources for laying of Intelligent Cabling across the DC & DR .

364	96	7. Role and Responsibilities of Contractor i.r.o AAA,AD,EMS and related software applications	Backup	Backup and recovery is mentioned at multiple places in the tender document. However it is not clear if the backup solution along with the infrastructure & licenses will be provided by ERNET or if it needs to be proposed by bidder. Please confirm. In case bidder needs to provide backup solution, please share the details of size of data to be backed up, backup window, backup and retention policy, data to be backed up to disk/tape, etc. for each application, so that the backup solution can be proposed accordingly.	Backup period requirement is 01 Year. Bidders need to consider the required infra to support this requirement. Refer to the Scope of work , Specs & Tender Clauses for the size details.
365	88	Section VII,Scope of Work of contractor	iii Security Audited HLD , Security Audited LLD & Acceptance test plan (ATP) with detailed test procedure for review and approval by ERNET India /CERT-In.	Please ellobrate the "Security Audited HLD, Security Audited LLD & Acceptance test plan (ATP)	HLD,LLD audited from security prespective by stakeholders mentioned in Scope of work. ATP contains detailed acceptance test procedures for acceptance test plan.
366	79	Minimum Qualification, Relevant Experience & Certifications at DC/DR & Shastri Park, Delhi, Training	Training with Certification from Authorized Certifica	The understandsting is the Bidder need to provide training with certification vouchers. The certifciation needs to be taken by the attendees in authourized center. Kindly confirm the understanding	It may be noted that expenses pertaining to training & certification vouchers & its facilitation will be borne by bidder.
367	91	Section VII: Scope of Work	The Contractor is required to prepare detailed deployment plan along with Security Audited HLD, Security Audited LLD along with the detailed Acceptance Test Plan and shall submit the same for approval within Ten (10) weeks from the issuance of the contract Agreement	Kindly clarify what is meant by Security Audited HLD & LLD	HLD,LLD audited from security prespective by stakeholders mentioned in Scope of work.
368	127	E. Security and Incident Management Service Levels for all DC and DR	For every instance of Data Theft, the bidder is subject to penalty and/or punishment applicable under the IT act/ ERNET India/CERT-In data theft policy or any other prevailing laws of the State/Country at that point of time, which shall be over and above the stated penalty	Since the bidder doesn't have the control or visibility of the data or the policy which are getting configured based onconfirmation given by ERNET Request ERNET to remove this SLA	The contractor's manpower's role is work on creation/configuring/changing policies , maintaining the 24x7 safe operations across the complete IT Infra supplied. Accordingly , contractor needs to use its manpower's expertise to ensure the data is safely maintained. Hence this clause from SLA cannot be removed.
369	344	Form 12 Financial Bid (BoQ),55 Forensic Laptops	Additional	Kindlly confirm the warranty duration of the Forensic Laptop?	Refer to Specs for warranty Duration
370	349	Form 12 Financial Bid (BoQ),59 Heavy Duty Workstation	Additional	Kindlly confirm the warranty duration of the Forensic Laptop?	3 years, Refer revised specs too.
371	89	Section VII: Scope of Work,Scope of Work of Contractor	Additional	Will all workstation, Laptop and printer be deployed in domain controlled system? Please kindly define the scope of configurations?	Yes; Scope of configurations will be decided with contractor.
372	98	8. General Activities to be performed by Contractor for the project:	The bidder has to do the VA & PT for the Solutions including Applications that are procured as part of in this tender.	Does Earnet want to do VAPT of Desktop also? Kindly confirm..	Yes
373	124	Sec VIII (A)(1)1 Service Level during Operation & Maintenance period for Equipment:	At Data Center (New DC & New DR) and remote sites, for faults in any of the equipment, SLA penalty @ 0.25 % of the equipment(s) cost per day or part thereof will be deducted beyond 24 hours from the reporting time of fault, then penalty @ 0.5 % of equipment cost per day will be deducted. SLA penalty of Rs. 2000/- per day beyond 24 hours will be charged for equipment(s) (active and passive component) whose price could not be derived (e.g Intelligent Cables) from the price bid.	There is no capping here. Can we expect some maximum capping over Penalty.	No Change

374	99	Form3A: Unpriced Make & Model Details-Compliance,10 (Training)	Training for 20 Persons (in batches) shall be provided onsite by the OEM experts/OEM representatives for equipment of respective OEMs for installation and operations of installed equipment(s) per equipment supplied.	We understand that 20 persons batch training will be required. However please confirm the maximum number of person to be trainined and for which particular Component/OEM. It will helpful in making appropriate arrangement for the required training accordingly.	A maximum of 3 such batches; Clause is self explanatory
375	112	13 Manpower required at DC , DR, Delhi & other locations	Manpower required at DC , DR, Delhi & other locations	Please confirm whether Ernet would be providing laptop/desktop for the required Manpower or Bidder need to provide them from their side.	Laptops for NoC Team will be brought by Contractor; All the laptops need to be hardened before the use in DC/DR area. However final decision in this regard will be taken during the project implementation
376	125	Section(VIII)C(vi)C. Help Desk support during O&M period for services:	Should provision for all necessary channels for reporting issues to onsite technical team. The incident reporting channels will be the following : SMS	As SMS alerts will be required while using different tools , please confirm that ERNET will be providing SMS gateway Service i.e. to be taken from any ISP	SMS Gateway will be provided by ERNET India /CERT-In
377	45	6.2 Project Planning & Management	Contractor must ensure that Project Managers as asked in Manpower section will handle all activities of project (i.e. for implementation and Operation & Maintenance) till its completion.	As per our understanding, ERNET would be haivng no issue while we would deploy different PM for implementation phase and a different PM for operation (maintenance) phase. Please share your consent.	It is suggested to have same PM for both phases. However, if Bidder feels, project can be managed better with different PM, ERNET India has no objection.
378	90	2.(xv)	Supply of competent & dedicated manpower for a period of two years respectively at Mumbai, Chennai, Kolkata , Delhi/NCR, Bangalore working in Project from contractor's premsies.	Please confirm from where these deployed Manpower will work. It should be ERNET location instead of "Contractor's premises".	No Change; Refer "Section Minimum Manpower required w.r.t Implementation"
379	102	12(VI)	Contractor shall carry out Vulnerability assessment (VA)	Please confirm the frequency as well for the Vulnerability assessment (VA)	Refer Scope Of Work , Tender Clause & Section Acceptance Testing (AT) for required information
380	102	12(VII)	During the O&M period, the Contractor shall provide all product(s) and documentation updates, patches/fixes, and version upgrades within 15 days of their availability/release and should carry out installation and make operational	We are confirming that all products updates and patches will be n-1. However if any patches or upgrades will be released then it will be updated within 30 days of their availability. Please allow 30 days for the same.	The clause may be read as : During the O&M period, the Contractor shall provide all product(s) and documentation updates, patches/fixes, and version upgrades within 30 days of their availability/release and should carry out installation and make operational the same at no additional cost to ERNET India/CERT-In. Contractor must ensure that permission has been taken from ERNET India/CERT-In before any updates, patches/fixes, and version upgrades.
381	105	12.4NMS (VI)	Coordination with defined agencies for WAN links .	Our understanding is that new WAN links's project/documentation part will not be responsibility. Any cordination with ISPs on documentation will not be part of responsibility. Please confirm.	Coordination with defined agencies for WAN links is one of the critical responsibilties of the O&M manpower. Relevant documentation required by ISP / bandwidth provider will be provided
382	109	12.13(vi)	The request would be made on help desk by the user by dedicated help line number	Our understanding is that ERNET would be take care of considered help line (telecom services) as mentioned in stated clause.	Yes
383	52	9.3 Terms of Delivery, Installation, testing, commissioning & Acceptance	6.2. Delivery of the Equipments at DC	Request to extend the timeline from by 8 weeks, total 16 weeks required to deliver equipment at respective locations.	Kindly refer to respective updated clause in Annexure-B
384	52	9.3 Terms of Delivery, Installation, testing, commissioning & Acceptance	6.3. Installation, Testing & Commissioning of Complete Equipments at DC Offering of this infrastructure under Milestone-1 for Acceptance Testing (AT) to ERNET India as per Acceptance Testing Plan (ATP).	28 weeks are required to post delivery	No Change
385	52	9.3 Terms of Delivery, Installation, testing, commissioning & Acceptance	6.4. Acceptance by ERNET India for Complete Milestone 1 and issuance of acceptance certificate subject to completion of complete work as per tender.	40 weeks are required to completion of milestone 1	No Change
386	52	9.3 Terms of Delivery, Installation, testing, commissioning & Acceptance	6.5. Delivery of the Equipments at DR	Start of Milestone 2 - T + 16 Weeks is required	Kindly refer to respective updated clause in Annexure-B

387	52	9.3 Terms of Delivery, Installation, testing, commissioning & Acceptance	6.6. Installation, Testing & Commissioning of Complete Equipments at DR Offering of this infrastructure under Milestone-2 for Acceptance Testing (AT) to ERNET India as per Acceptance Testing Plan (ATP).	24 weeks are required to post delivery	No Change
388	52	9.3 Terms of Delivery, Installation, testing, commissioning & Acceptance	6.7. Acceptance by ERNET India for Complete Milestone 2 and issuance of acceptance certificate subject to completion of complete work as per tender.	48 weeks are required to completion of milestone 2	No Change
389	52	9.3 Terms of Delivery, Installation, testing, commissioning & Acceptance	6.8. Site Survey (if required), Delivery, Installation, Testing & Commissioning of Complete equipments at Remote Sites and their integration with DC. Offering of this infrastructure for AT to ERNET India as per ATP.	Start of Milestone 3 - T + 48 Weeks is required	No Change
390	53	9.3 Terms of Delivery, Installation, testing, commissioning & Acceptance	6.9. Acceptance by ERNET India for Complete Milestone 3 and issuance of acceptance certificate subject to completion of complete work as per tender.	56 weeks are required to completion of milestone 3	No Change
391	53	9.3 Terms of Delivery, Installation, testing, commissioning & Acceptance	6.10. O&M of Existing DC, DR and Remote sites	requesting to amend this clause to 2 month.	no Change; And Remote Sites Document
392	55	9.5.2	2. Liquidated Damages (LD):	Request to amend this clause to reduce penalty 0.25% per week for undelivered portion.	Kindly refer to respective updated clause in Annexure-B
393	55	9.5.2	2. Liquidated Damages (LD):	Request to amend this clause to reduce the maximum cap upto 5 %.	Kindly refer to respective updated clause in Annexure-B
394	2	EMD EXEMPTION:(a)	EMD EXEMPTION: The bidder seeking EMD exemption, must submit the valid supporting document for the relevant category as per GeM GTC with the bid. Under MSE category, only manufacturers for goods and Service Providers for Services are eligible for exemption from EMD. Traders are excluded from the purview of this Policy./	We are exempted from EMD submission as per GeM T&C. GTC Clause: Following categories of Sellers shall however, be exempted from furnishing Bid Security: Sellers / Service Provider having annual turnover of INR 500 Crore or more, at least in one of the past three completed financial year(s) Kindly confirm GeM Exemption is applicable for this opportunity.	Kindly refer to respective updated clause in Annexure-B
395	41	5.6.1-IPR Rights	All deliverables, outputs, plans, drawings, specifications, designs, reports, and other documents and software submitted by the contractor under this Contract shall become and remain the property of the ERNET India/ CERT-In and must not be shared with third parties or reproduced, whether in whole or part, without the ERNET India/ CERT-In’s prior written consent. The contractor shall, not later than upon termination or expiration of this Contract, deliver all such documents and software to the ERNET India/ CERT-In, together with a detailed inventory thereof.	SInce there is no exlcusivity in the services/software provided, and also the fact that the bidder is not a manufacturer of any software, there cannot be an IPR transfer in favour of ERNET India. Accordingly, we request a revision in the clause, to be read as follows: "Neither party will gain by virtue of this Agreement any rights of ownership of copyrights, patents, trade secrets, trademarks or any other intellectual property rights owned by the other. All copyrights patents, trade secrets, trademarks and any other intellectual property rights existing prior to the Effective Date or developed independent of this Agreement shall belong to the party that owned such rights immediately prior to the Effective Date or has developed such intellectual property right. Contractor will own all intellectual property rights, title and interest in any ideas, concepts, know how, documentation or techniques developed under this Agreement and provides ERNET a non-exclusive, non-transferable, royalty-free license for its internal use only during the term of the contract."	No Change

396	50	8.1-Transfer of Assets	The ownership of the supplied Equipment along with its warranty and all other associated rights shall be transferred within 90 days to CERT-In, ; after successful Commissioning and Acceptance of each milestone by ERNET India. All the risks, responsibilities, liabilities thereof in respect of all equipment shall remain with contractor till acceptance of each milestone. All licenses are to be provided in the name of Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology Government of India. Contact details including email id of Cert-In will be provided to L-1 bidder. Contractor shall provide following documents during handover of assets as per milestones: 1)Invoices with serial no of devices 2)Bill of Material 3)OEM Warranty certificates 4)Duly received Delivery challan at all locations 5)Software license detail, if any 6)Final Acceptance report 7)Any other document specified by ERNET India	We request a revision in the clause, to be read as follows: "Ownership of the supplied Equipment along with its warranty and all other associated rights shall stand transferred in the name of ERNET India immediately upon delivery of such equipment." We are unable to accept the clause in its current form.	No Change
397	56	9.6-Force Majeure	1)On the occurrence of any unforeseen event, beyond the control of either Party, directly interfering with the delivery of Equipment(s) and Services arising during the currency of the contract, such as war, hostilities, acts of the public enemy, civil commotion, sabotage, fires, floods, explosions, epidemics, pandemic, quarantine restrictions, strikes, lockouts, or acts of God, or any other defined by government, the affected Party shall, within a week from the commencement thereof, notify the same in writing to the other Party with reasonable evidence thereof. Unless otherwise directed by ERNET India in writing, the contractor shall continue to perform its obligations under the contract as far as reasonably practicable and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event. If the force majeure condition(s) mentioned above be in force for 90 days or more at any time, then in such a case either party shall have the option to terminate the contract on expiry of 90 days of commencement of such force majeure by giving 14 days' notice to the other party in writing. In case of such termination, no damages shall be claimed by either party against the other, save and except those which had occurred under any other clause of this contract before such termination. 2)Notwithstanding the remedial provisions contained in GCC-clause9.6 (2) or 12.1.1, none of the Party shall seek any such remedies or damages	It may not be possible for the bidder to perform the services if a force majeure event occurs, since equipment to be delivered will come from third party OEMs.A force majeure event like a pandemic might affect delivery timelines. In view of the above, we request a revision in the clause, to be read as follows: "1)On the occurrence of any unforeseen event, beyond the control of either Party, directly interfering with the delivery of Equipment(s) and Services arising during the currency of the contract, such as war, hostilities, acts of the public enemy, civil commotion, sabotage, fires, floods, explosions, epidemics, pandemic, quarantine restrictions, strikes, lockouts, or acts of God, or any other defined by government, the affected Party shall, within a week from the commencement thereof, notify the same in writing to the other Party with reasonable evidence thereof. In case of any delay in performance of the Services and delivery of Equipment due to Force Majeure event including of any pandemics, the timeline for such work shall automatically get extended for such period affected due to Force Majeure event. If the force majeure condition(s) mentioned above be in force for 90 days or more at any time, then in such a case either party shall have the option to terminate the contract on expiry of 90 days of commencement of such force majeure by giving 14 days' notice to the other party in writing. In case of such termination, no damages shall be claimed by either party against the other, save and except those which had occurred under any other clause of this contract before such termination.	No Change

398	59	12.1.2-Notice for Default	As soon as a breach of contract is noticed, 'Notice of Default' shall be issued to the contractor, giving two weeks' time to resolve the issues mentioned in the notice. Despite serving NFD, ERNET India would be having right to invoke contractual remedies to safeguard its interest.	1. We request that a notice period of atleast 30 days to cure any breach on our part. Accordingly, we request a revision in the clause, to be read as follows: "As soon as a breach of contract is noticed, 'Notice of Default' shall be issued to the contractor, giving thirty days' time to resolve the issues mentioned in the notice." 2. Further, in the event of termination, ERNET shall pay the contractor for work done successfully till the date of payment. Further, ERNET shall also pay the the contractor for orders already placed with OEMs/Software Licensors, which Orders cannot be cancelled with the OEMs/Software Licensors or pay cancellation costs, if any, levied by the OEMs/Software Licensors. Further, if the contractor is providing licenses or products on opex model or on lease, then in case of termination, ERNET will have to pay for the entire pre-agreed duration of the contract.	No Change
399	60	12.1.4 (1)-Contractual Remedies for Breaches/Defaults	If there is an unsatisfactory resolution of the issues raised in the 'Notice of Default' within the period specified in the notice, then ERNET India may take any one; or more of the following contractual remedies. 1)Temporary withhold payments due to the contractor till recoveries due to invocation of other contractual remedies are complete..........	We request a clarification that ERNET will not withhold any payments due to the contractor for the services which have already been provided successfully.	No Change
400	61	12.2.1-Notice for determination of contract	The ERNET India reserves the right to terminate the contract, in whole or in part for its (the ERNET India's) convenience, by serving written 'Notice for Determination of Contract' on the contractor by giving sixty (60) days prior notice during the currency of the contract. The notice shall specify that the termination is for the convenience of the ERNET India of the contract. The notice shall also indicate inter-alia, the extent to which the contractor's performance under the contract is terminated, and the date with effect from which such termination shall become effective.	We requst that a notice period of atleast 90 days be given to the bidder in the event of termination for convenience. Further, in the event of termination, ERNET shall pay the contractor for work done successfully till the date of payment. Further, ERNET shall also pay the the contractor for orders already placed with OEMs/Software Licensors, which Orders cannot be cancelled with the OEMs/Software Licensors or pay cancellation costs, if any, levied by the OEMs/Software Licensors. Further, if the contractor is providing licenses or products on opex model or on lease, then in case of termination, ERNET will have to pay for the entire pre-agreed duration of the contract.	No Change
401	20	5.2.1	Firm Price	The prices are dependant on Taxes, Duties (including Custom Duty), Levies, USD-INR exchange rate, OEM List Price, OEM Discounting etc. These factors are not within bidder's control and hence please request ERNET to allow price revision for additional quantity as per the prevailing business conditions during order placement. The revised prices will be applicable only on the subsequent orders after 1st PO.	No Change

402	30	12.1.1	Right to Vary Quantities i. ERNET India reserves the right to increase/decrease the quantities to be ordered up to 25 % of sum total of final bid value; at the time of placement of contract. ii. Keeping in the view of the fact that the project requirements are dynamic and ever changing therefore ERNET India reserves the right to increase the ordered value by up to 25% of sum total of final bid value; till the completion of O&M activities, without any reference to the intial ordered quantities. iii. Successful Bidder/ Contractor is bound to accept the orders accordingly, failing which; ERNET India may declare this as an event of default and consequences for event of default will be applicable.	The prices are dependant on Taxes, Duties (including Custom Duty), Levies, USD-INR exchange rate, OEM List Price, OEM Discounting etc. These factors are not within bidder's control and hence please request ERNET to allow price revision for additional quantity as per the prevailing business conditions during order placement. The revised prices will be applicable only on the subsequent orders after 1st PO.	No Change
403	50	8.1	Transfer of Assets : After successful Commissioning and Acceptance of each milestone;the ownership of the supplied Equipment along with its warranty and all other associated rights is planned to be transferred within 90 days to CERT-In by ERNET India ; after successful Commissioning and Acceptance of each milestone by ERNET India. All the risks, responsibilities, liabilities thereof in respect of all equipment shall remain with contractor till 90 days ; from the effective date of such acceptance of each milestone.	Request ERNET to revise the clause as below: The ownership of the supplied Equipment along with its warranty and all other associated rights shall be transferred to CERT-In on delivery of equipments to ERNET India. All the risks, responsibilities, liabilities thereof in respect of all equipment shall remain with ERNET India. All licenses are to be provided in the name of Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology Government of India."""	No Change
404	50	8.2	Insurance The Bidders shall also arrange to get all the supplied equipments (including additional equipements ordered using right to vary quantities clause) insured to cover loss/damage due to theft, burglary, fire, or any natural disaster for the period of 03 (three) years from the date of issue of the contract. Bidder shall be required to extend the insurance period in case, there is delay in commissioning & acceptance of project. The insurance shall not be for an amount less than 100 percent of the value of the equipment(s) as mentioned in the contract. Bidder may include cost of insurance in the unit price of equipment(s) quoted in the price bid. Note: It is also clarified that it is contractor’s responsibility to manage the insurance of delivered equipment at Data Centers, remote sites throughout the process till acceptance of milestones, also.	Request ERNET India to revise the Insurance clause upto delivery of equipments at designated premise. Post delivery Insurance of the supplied equipments has to be covered under ERNET's Insurance policy.	No Change

405	56	10	Prices and Payments Terms: b. In respect of DC and DR equipment (s), 50% of the value of equipment(s) delivered at DC and similarly 50% of the value of equipment(s) delivered at DR shall be released only after submission of BG equivalent to the amount which is to be released. The BG should be valid for a minimum period of 6 months (with a claim period of additional 3 months). BG must be extendable till the successful completion of rack mounting & Power On Self Test (POST) of active equipments. c. In respect of equipment (s) at DC and DR, additional 30% of the total value of items will be made after successful installation, integration, commissioning and acceptance as per the respective milestone(s). d. In respect of equipment at remote sites, 80% of the total value of items will be made after successful delivery, installation, integration, commissioning and acceptance of the individual remote sites. e. Thereafter, based on successful performance during warranty period, balance 20% value of the respective milestone shall be released in twenty (20) equal instalments on a quarterly basis after completion of every quarter. It would be duty of contractor to get the satisfactory	Request ERNET to consider following payment terms for CAPEX : For equipment at DC and DR and remote location 60% payment on delivery,30% on installation and commissioning, and based on successful performance during warranty period, balance 10% value of the respective milestone in twenty (20) equalinstalments on a quarterly basis after completion of every quarter. Request ERNET to remove following clause : It may be noted that the payment to the contractor are subject to making sufficient funds available by CERT-In to ERNET India . Contractor agrees and accepts that there can be delays in releasing the payment due to non-availability of funds	No Change
406	59	12.1.3	Terminations for Default	We requst that a notice period of atleast 90 days be given to the bidder in the event of termination for convenience. Further, in the event of termination, ERNET shall pay the contractor for work done successfully till the date of payment. Further, ERNET shall also pay the the contractor for orders already placed with OEMs/Software Licensors, which Orders cannot be cancelled with the OEMs/Software Licensors or pay cancellation costs, if any, levied by the OEMs/Software Licensors.	No Change
407	61	12.2	Termination for Default/ Convenience of ERNET Inc	We request that a notice period of atleast 90 days be given to the bidder in the event of termination for convenience. Further, in the event of termination, ERNET shall pay the contractor for work done successfully till the date of payment. Further, ERNET shall also pay the the contractor for orders already placed with OEMs/Software Licensors, which Orders cannot be cancelled with the OEMs/Software Licensors or pay cancellation costs, if any, levied by the OEMs/Software Licensors.	No Change

408	124	Section VIII	Service Level Agreement during Operation & Maintenance The overall Penalties (for Clause 1-A,B,C,D in Section-VIII) per quarter shall be capped at a maximum of 25% of the respective Quarterly payment of Grand Total Value. In case penalty imposed on the contractor consecutively for two quarters reaches the maximum Penalty (i.e 25%) then in such an eventuality ERNET India reserves the right to terminate the Contract as per Clause 12.1 & 12.2 of Section-III	Please request ERNET to revise the SLA penalty capping at 5% of quarterly payment value each quarter.	No Change
409	35	Recommendation for 3rd Party accrediation	**Add clause** Proposed solution should participated in Miercom security assessment test of IPS and score more then 99% in IPS exploit detection test.	It is highly advisable to have 3rd Party independent like Miercom which is industry leading report for security effictiveness proof so to proof the NIPS have negligable false positives detection and unnecessary alerting	No Change
410	73	Minimum Qualification, Relevant Experience & Certifications at DC/DR & Shastri Park, Delhi	Data center IT networking & architecture expert B.E./B.Tech/MCA with 10 Years relevant experience in IT/ITeS + CCIE-ENT	NA	The clause may be read as : **Data center IT networking & architecture expert** B.E./B.Tech/MCA with 10 Years relevant experience in IT/ITeS **+ CCNP-DC/JNCIP-DC**
411	68 / 171	Part B (CAPEX – II)	Enterprise Management Solution	NA	The Clause 3 under EMS may be read as Additional EMS License Price for IT devices**/MPLS Links**
412	78	Section IV: Bill of Material	Note 2: Contractor should make sure that in new DC-DR, Manpower's certification should be relevant to the product offered in the bid. E.g If CISCO products are offered then certification should be CCNP/CCNA. Similarly, in case of Juniper it should be JNCIA/JNCIP. For other OEM equipment, same philosophy should be followed.	NA	The clause may be read as : Note 2: Contractor should make sure that in new DC-DR, Manpower's certification should be relevant to the product offered in the bid. E.g If CISCO products are offered then certification should be CCNP/CCNA. Similarly, in case of Juniper it should be JNCIA/JNCIP. For other OEM equipment, same philosophy should be followed. **OEM Specialist (such as OEM Security/ Network/ Server Specialist etc.) must be on OEM's Payroll with minimum 5-year experience. Duty shift may be realigned as per requirement.**

413	79	PART-C(OPEX)	Ammendment		PART C (OPEX) & O&M including Manpower= OPEX May be read as PART-C(OPEX & Databases GeoIP, VPN Services) O&M including Manpower= OPEX + Databases GeoIP, VPN Services The specifications for this service are required for the period of 36 months and are as follows : Geo Location Database IP Address, Country, Region, City, Latitude, Longitude, ISP, Time Zone, Domain, Net Speed, IDD & Area Code, ZIP/PIN Code, Weather Station, Mobile Carrier, Mobile Country Code, Mobile Network Code, Elevation, Usage Type, Address Type, Category, District Proxy Database IP Address, Virtual Private Networks (VPN), Tor Exit Nodes (TOR), Public Proxies (PUB), Web Proxies (WEB), Hosting Provider, Data Center or Content Delivery Network (DCH), Search Engine Robots (SES), Residential Proxies (RES), Enterprise Private Networks (EPN), Consumer Privacy Networks (CPN), Proxy Country, Proxy Region & City, Proxy ISP, Proxy Domain, Proxy Usage, Type, Proxy Type, Proxy ASN, Last Seen, Threat Provider OR Database contains IP addresses of VPN servers, open proxies, web proxies, Tor exits, search engine robots, data center ranges, residential proxies, consumer privacy networks , enterprise private networks and VPN provider name .Database contains IP addresses which are being used as VPN servers, open proxies, web proxies, Tor exits, search engine robots, data center ranges, residential proxies consumer privacy networks , enterprise private networks and VPN provider name.

Annexure-A

S. No.	Equipment	Tender Page No.	Tender Clause	Bidder Sought Clarification/Recommendation	ERNET
1	Leaf Switch	29	Should support 250K IPv4 LPM Routes, 125K IPv6 LPM Routes, 100K IPv4/v6 Multicast Routes.	Should support 400K IPv4 LPM Routes, 400K IPv6 LPM Routes, 100K IPv4/v6 Multicast Routes Justification: Since at router 1M route scale is asked, hence requesting to amend the clause to accommodate higher number of routes for east-west traffic.	As per Tender Document
2	Border Leaf Switch	30	Switch should support all functions required to operate as a Border Leaf Switch providing DC Gateway, Service Chaining and Data centre Interconnect (DCI) using EVPN type-5 routes. Should support **300K** **IPv4 Routes,150K IPv6 Routes, 64K Multicast Route**	Requesting to increase the route scale to 1M IPv4 Routes,1M IPv6 Routes, 64K Multicast Route. Justification: Since at router 1M route scale is asked, hence requesting to amend the clause to accommodate higher number of routes for east-west traffic.	Kindly refer Revised Technical specification
3	Network Manager	52	Visibility of the these parameters is expected but not limited to - CPU, Memory, interface stats (traffic counter, error, discard), MAC table, ARP table, IPv6 ND table, IPv4 route table, IPv6 route table, **Multicast table,** BGP, capacity parameters / TCAM ,running config, traffic flow (sflow/IPFIX/Netflow), buffer utilization per interface, MLAG Stats, Switch environment stats(FAN, Temperature, Power Supply).	Requesting to remove "Multicast Table" Justification : For wider participation	Multicast Removed
4	Network Manager	53	"Should be capable of showing hop-by-hop flow path and drops on links taken by a flow between 2 end points.	Requesting to remove the clause. Justification : For wider participation	Should be capable of showing hop-by-hop flow path and drops on links taken by a flow between 2 end points or should support Netflow/SFLOW
5	Network Manager	53	Central controller should provide detailed traffic flow analytics to search and see what protocols/port are used and how much data is transferred between 2 end-points during a period of time.	Requesting to remove the clause. Justification : For wider participation	Central controller should provide detailed traffic flow analytics to search and see what protocols/port are used and how much data is transferred between 2 end-points during a period of time or should support Netflow/SFLOW Or Central controller should provide detailed traffic flow analytics to search and to show ping, traceroute, forward and reverse path between 2 end-points.
6	Network Manager	53	Should provide building customized dashboards using any of the collected telemetry data.	Requesting to remove the clause. Justification : For wider participation	Should provide building customized dashboards/access using any of the collected telemetry data
7	Leaf Switch, Border Leaf, Interconnect Switch Type1 and 2, WAN Switch	28,30,37,39,40	Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN, **data plane telemetry to trace path and per hop latency for a flow ,** buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations.	Requesting to remove "data plane telemetry to trace path and per hop latency for a flow". Also, requesting to include sflow/netflow with IPFIX Justification : For wider participation	Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, sflow/netflow/IPFIX, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN, telemetry , buffer queue depth monitoring/QOS for prioritizing the traffic during congestion with minimum 8 queue per port, Same OS across all the proposed network switches for simplified operations.
8	Spine Switch for DC	203	EVPN+VXLAN (No proprietary protocols to be deployed for leaf-spine fabric), ESI LAG or equivalent technology. Should support EVPN Route Types (Type-1, Type-2, Type-3, Type-4, Type-5,), Tenant routed Multicast / OISM, OSPF, ISIS, BGP	EVPN+VXLAN (No proprietary protocols to be deployed for leaf-spine fabric). Should support EVPN Route Types (Type-1, Type-2, Type-3, Type-4,Type-5,), Tenant routed Multicast / OISM, OSPF/ISIS, BGP Justification: Since Spine is a Layer 3 Device with no Layer 2 termination on it, hence there is no requirement for Layer 2 protocols such as ESI or LAG	EVPN+VXLAN (No proprietary protocols to be deployed for leaf-spine fabric). ESI LAG/ Layer3 port channels or equivalent technology.Should support EVPN Route Types (Type-1, Type-2, Type-3, Type-4,Type-5,), Tenant routed Multicast / OISM, OSPF/ISIS, BGP
9	Spine Switch for DC	203	Port, VLAN & Routed ACL,802.1x,16K or higher ACL Entries/group based-segmentation- entries, GRE (Must Support 1000 or Higher GRE Tunnels or 1000 VXLAN Tunnels)	ospf	Port/ VLAN/Routed ACL ,9K or higher ACL Entries/group based-segmentation-entries, GRE/VXLAN Tunnel (Must Support 1000 or Higher GRE Tunnels or 1000 VXLAN Tunnels)

10	Spine Switch for DC	203	Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sFlow/Netflow, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN, data plane telemetry, buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations.	Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sFlow/Netflow, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN. Same OS across all the proposed network switches for simplified operations. Justification: Data Plane Telemtry and buffer queue depth monitoring is required at the access/leaf level where the application is terminated. Spine acts as a layer 3 backbone to interconnect leaf switches and with the deep buffer and high BW links, this is not a necessity here	Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, sflow/netflow/IPFIX, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN, telemetry , buffer queue depth monitoring/QOS for prioritizing the traffic during congestion with minimum 8 queue per port, Same OS across all the proposed network switches for simplified operations.
11	Spine Switch for DC	203	Virtual output Queue VoQ)/Egress QoS/Intelligent Buffer/dynamic buffer, WRED,ECN,LLQ,PTP, 8GB Packet Buffer per line card or equivalent, 802.1Qbb,8 queues/port, WRR	Virtual output Queue VoQ)/Egress QoS/Intelligent Buffer/dynamic buffer, WRED,PFC/ECN,PTP, 8GB Packet Buffer per line card or equivalent,8 queues/port, WRR	Virtual output Queue VoQ)/Egress QoS/Intelligent Buffer/dynamic buffer, WRED,PFC/ECN,PTP, 8GB Packet Buffer per line card or equivalent,8 queues/port, WRR
12	Spine Switch for DC	203	Should support 250K IPv4 Routes, 125K IPv6 Routes, 100K IPv4/v6 Multicast Routes.	Should support 250K IPv4 Routes, 125K IPv6 Routes, 32K IPv4,8K IPv6 Multicast Routes.	Should support 250K IPv4 Routes, 125K IPv6 Routes, 32K IPv4,8K IPv6 Multicast Routes.
13	Spine Switch for DR	204	EVPN+VXLAN (No proprietary protocols to be deployed for leaf-spine fabric), ESI LAG or equivalent technology. Should support EVPN Route Types (Type-1, Type-2, Type-3, Type-4, Type-5,), Tenant routed Multicast / OISM, OSPF, ISIS, BGP	EVPN+VXLAN (No proprietary protocols to be deployed for leaf-spine fabric). Should support EVPN Route Types (Type-1, Type-2, Type-3, Type-4,Type-5,), Tenant routed Multicast / OISM, OSPF/ISIS, BGP Justification: Since Spine is a Layer 3 Device with no Layer 2 termination on it, hence there is no requirement for Layer 2 protocols such as ESI or LAG	EVPN+VXLAN (No proprietary protocols to be deployed for leaf-spine fabric). ESI LAG/Layer3 port channels or equivalent technology.Should support EVPN Route Types (Type-1, Type-2, Type-3, Type-4,Type-5,), Tenant routed Multicast / OISM, OSPF/ISIS, BGP
14	Spine Switch for DR	204	Port, VLAN & Routed ACL,802.1x,16K or higher ACL Entries/group based-segmentation-entries, GRE (Must Support 1000 or Higher GRE Tunnels or 1000 VXLAN Tunnels)	Port/ VLAN/Routed ACL ,9K or higher ACL Entries/group based-segmentation-entries, GRE/VXLAN Tunnel (Must Support 1000 or Higher GRE Tunnels or 1000 VXLAN Tunnels) Justification: Since Spine is a Layer 3 Device with no Layer 2 termination on it, hence there is no requirement for Layer 2 ACLs.	Port/ VLAN/Routed ACL ,9K or higher ACL Entries/group based-segmentation-entries, GRE/VXLAN Tunnel (Must Support 1000 or Higher GRE Tunnels or 1000 VXLAN Tunnels)
15	Spine Switch for DR	204	Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sFlow/Netflow, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN, data plane telemetry, buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations.	Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sFlow/Netflow, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN. Same OS across all the proposed network switches for simplified operations. Justification: Data Plane Telemtry and buffer queue depth monitoring is required at the access/leaf level where the application is terminated. Spine acts as a layer 3 backbone to interconnect leaf switches and with the deep buffer and high BW links, this is not a necessity here	Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, sflow/netflow/IPFIX, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN, telemetry , buffer queue depth monitoring/QOS for prioritizing the traffic during congestion with minimum 8 queue per por, Same OS across all the proposed network switches for simplified operations.
16	Spine Switch for DR	204	Virtual output Queue VoQ)/Egress QoS/Intelligent Buffer/dynamic buffer, WRED,ECN,LLQ,PTP, 8GB Packet Buffer per line card or equivalent, 802.1Qbb,8 queues/port, WRR	Virtual output Queue VoQ)/Egress QoS/Intelligent Buffer/dynamic buffer, WRED,PFC/ECN,PTP, 8GB Packet Buffer per line card or equivalent,8 queues/port, WRR	Virtual output Queue VoQ)/Egress QoS/Intelligent Buffer/dynamic buffer, WRED,PFC/ECN,PTP, 8GB Packet Buffer per line card or equivalent,8 queues/port, WRR
17	Spine Switch for DR	205	Should support 250K IPv4 Routes, 125K IPv6 Routes, 100K IPv4/v6 Multicast Routes.	Should support 250K IPv4 Routes, 125K IPv6 Routes, 32K IPv4,8K IPv6 Multicast Routes.	Should support 250K IPv4 Routes, 125K IPv6 Routes, 32K IPv4,8K IPv6 Multicast Routes.
18	Border Leaf Switch	208	Port, VLAN & Routed ACL. Should support minimum 16K ACL entries/terms or minimum 32K prefix/host entries for traffic segmentation.	Port, VLAN & Routed ACL. Should support minimum 14K ACL entries/terms or minimum 32K prefix/host entries for traffic segmentation.	Kindly refer Revised Technical specification
19	Interconnect Switch	215	Switch should support all functions required to operate as an interconnect switch connecting various devices including firewall and routers with an non-blocking fabric	Requesting to add 400K Ipv4/Ipv6 route scale. Justification: Requesting to add scale values	As per Tender Document

20	Interconnect Switch Type-2	216	Switch should support all functions required to operate as an interconnect switch connecting various devices including firewall and routers with an non-blocking fabric	Requesting to add 400K Ipv4/Ipv6 route scale. Justification: Requesting to add scale values	As per Tender Document
21	WAN Switch	218	Switch should support all functions required to operate as a WAN Switch acting as interface between Service Provider Links and WAN Router	Requesting to add 400K Ipv4/Ipv6 route scale. Justification: Requesting to add scale values	As per Tender Document
22	Network Manager	230	Should provide ability to view Telemetry data over a timeline. The Data Should be available for at least 60 days.	Should provide ability to view Telemetry data over a timeline. The Data Should be available for at least 30 days.	Should provide ability to view Telemetry data over a timeline. The Data Should be available for at least 30 days.
23	CE Router	221	Type of Switch: Chassis Based/Non-Chassis Based	Please remove Switch and mention Router as the specifications are for Router	Type of Router: Chassis Based/Non-Chassis Based
24	CE Router	221	The Router should be populated with redundant Routing Card/Engines/control plane /supervisor engine/multi-core x86 CPU	Should have multi-core x86 CPU Justification: Since the redundant routers would be deployed, requesting to remove the requirement of redundant routing engines/sup, this is more of the requirement in chassis based router or in the Core/backbone network.	The Router should be populated with Routing Card/Engines/control plane/supervisor engine/multi-core x86 CPU
25	CE Router	221	Aggregated Throughput (Gbps) : 1600 Or higher	Requesting to change the routing throughput to 500gbps: Justification: Unlikely the throughput of any layer-3 Switch, The routing throughput is calculated differently. Requesting to reduce it to 500Gbps	As per Tender Document
26	CE Router	222	Port population: Should be supplied with 16x 10G SFP+ ports and 6 No. of 100G QSFP28 ports with non- blocking architecture and wire-speed from day 1.	Requesting to modify the clause as below: Port population: Should be supplied with 16x 10G SFP+ ports and 6 No. of 100G QSFP28 ports with non- blocking architecture and wire-speed from day 1. Justification: To meet the throughput requirement	As per Tender Document
27	CE Router	222	Feature Support: Device, OS, Optics, Manager from same OEM. Should be managed through unified Network Manager.	Requesting to remove this clause Justification: Generally, the Network Manager is required to manage the Network Switch Fabric , hence requesting to remove the clause. Also there is a separate NMS solution is asked to monitor all the network equipments.	Feature Support: Device, OS, Optics, from same OEM.
28	Internet Router	223	No. of 10G SFP+ ports (Fiber /Copper): 16 or higher	Requesting to modify the clause as below: No. of 10G SFP+ ports (Fiber : 16 or higher Justification: Since the "Coppper/Fiber" ports are something that is required in the switch. In routers , 10G interfaces are generally fiber, basis the type of link that will be connecting to the router . Hence requesting to modify it to remove the ambiguity.	No. of 10G SFP+ ports (Fiber): 16 or higher
29	Internet Router	223	Port Population: Should be supplied on day 1 with 4 x 1000Base-LX Single Mode SFP transceivers, 4 x 10/100/1000Base-T Interface Ports and 4 x 10G Base SR Transceivers. Should be scalable to support additional 4 X 40/100G QSFP ports; Fully Populated from Day-1	Requesting to modify the clause as below: Router should have minimum 20 x 10G and 6 x 40 / 100G QSFP28 LAN / WAN Interface loaded with 10 x 1 G Multimode Fiber SFP, 10 x 10G Multimode Fiber SFP+ , 4 x 40G QSFP28 and 2 x 100G QSFP56	Port Population: Should be supplied on day 1 with 4 x 1000Base-LX Single Mode SFP transceivers, 4 x1000Base-T Interface Ports and 4 x 10G Base SR Transceivers. Should be scalable to support additional 4 X 40/100G QSFP ports; Fully Populated from Day-1
30	Internet Router	223	Switching Capacity (Gbps): 256 or higher	Throughput: Router should have minimum IP forwarding throughput of 500 gbps Justification: Considering the requirement is of router not a Layer-3 Switch. Hence requesting to ammend the clause and throughput accordingly.	As per Tender Document

31	Internet Router	224	Feature Support: Device, OS, Optics, Manager from same OEM. Should be managed through unified Network Manager.	Requesting to remove this clause Justification: Generally, the Network Manager is required to manage the Network Switch Fabric , hence requesting to remove the clause. Also there is a separate NMS solution is asked to monitor all the network equipments.	Device, OS, Optics from same OEM.
32	Web Proxy	302	SWG appliance must have 4x10 GE SFP slots populated with multimode transceiver & 4 x 1GE RJ45 interfaces on each appliance from day one. All these interfaces should be available simultaneously from day one.	Requesting to change to "SWG appliance must have 4x10 GE SFP slots populated with multimode transceiver on each appliance from day one. All these interfaces should be available simultaneously from day one" Web proxy is not an inline network device and hence it doesn't require port density like a firewall, in current form the clause is restricting our participation. Hence requesting change.	SWG appliance must have 4x10 GE SFP slots populated with multimode transceiver on each appliance from day one. All these interfaces should be available simultaneously from day one
33	Web Proxy	303	The solution should provide geo-location awareness for security incidents.	Requesting to change to " The solution should provide geo-location/threat information for security incidents" Web proxy sits inside the network and different vendor have different level of threat information dashboard, geo-location is mostly on the perimeter firewall, while proxy sits inside the network, thus requesting change	The solution should provide geo-location/threat information awareness for security incidents.
34	Web Proxy	304	SWG should not introduce more than 10 microsecond latency	Requesting to remove as latency depends on multiple parameters such as load, policy, granularity, interface, memory consumption	Clause stands deleted
35	Web Proxy	304	The proposed solution must be able to deliver at least 10 Gbps of throughput on full load after enabling multiple security modules together	Requesting to remove, Web proxy is not an inline network firewall device, it is out of path network device working on user requests, In current form this is vendor specific and restricting our participation.	As per Tender Document
36	Web Proxy	304	The SWG should have both SSL/TLS and SSH Inspection capabilities	Requesting to change to "The SWG should have both SSL/TLS Inspection capabilities" SSH is not a web port in the network, in current form it is specific to firewall vendor thus requesting change.	The SWG should have both SSL/TLS Inspection capabilities
37	Web Proxy	305	The propose unit shall be able to support the following configuration of explicit proxy: i Proxy FQDN ii Max HTTP request length iii Max HTTP message length iv Add headers to Forwarded Requests v Proxy Port vi Interfaces that listen to proxy request	Requesting to change as "The propose unit shall be able to support the following configuration of explicit proxy: i Proxy FQDN v Proxy Port vi Interfaces that listen to proxy request" In current form is it specific to vendor thus requesting change for wider participation	The propose unit shall be able to support the following configuration of explicit proxy: i Proxy FQDN ii Proxy Port iii Interfaces that listen to proxy request
38	Web Proxy	306	The proposed solution must be able to deliver at least 1 Gbps of Application inspection throughput	Requesting to remove, Web proxy is not an inline network firewall device, it is out of path network device working on user requests, In current form this is vendor specific and restricting our participation.	As per Tender Document
39	Web Proxy	306	SWG must have capability to do Cloud application based routing not by means of manually adding IPs and or FQDNs i.e. appliance should have database of O365 readily available to select as destination address in security policy and destination address in static route configuration to give particular ISP path	Requesting to change to "SWG must have capability to do Cloud application based routing not by means of manually adding IPs and or FQDNs i.e. appliance should have database of O365 readily available to select as destination address in security policy" in current form it is specific to OEM thus requesting change	SWG must have capability to do Cloud application based routing not by means of manually adding IPs and or FQDNs i.e. appliance should have database of O365 readily available to select as destination address in security policy
40	Web Proxy	306	Should be able to block, allow or monitor only using AV signatures and file blocking based on per security policy based or based on authenticated user groups with configurable selection of the following services and their equivalent encrypted versions, wherever applicable: HTTP, SMTP, POP3, IMAP, FTP, CIFS, NNTP, SSH, MAPI	Requesting to change to "Should be able to block, allow or monitor only using AV signatures and file blocking based on per security policy based or based on authenticated user groups" MAPI, POP3 etc are not web ports they are email channels making it not relevant for web proxy, thus requesting change as in current form it is vendor specific.	Should be able to block, allow or monitor only using AV signatures and file blocking based on per security policy based or based on authenticated user groups
41	Web Proxy	306	SWG should offer both anti-virus scanning options - Proxy mode and Flow (streaming) mode.	Requesting to change to "SWG should offer anti-virus scanning and anti-malware analysis" In current form it is OEM specific thus requesting change	SWG should offer anti-virus scanning and anti-malware analysis
42	Web Proxy	306	The SWG should have capability to protect against Denial of Service (DOS) and DDOS attacks. DOS and DDOS protection should be applied and attacks stopped before security policy look-ups.	Requesting to remove as DOS/DDOS is asked as a dedicated solution DOS/DDOS are perimeter attack and Web Proxy sits inside the network	Clause stands deleted
43	Web Proxy	307	The proposed SWG appliance should be able to provide protection against attacks like Cross Site Scripting, SQL-Injection, Generic Attacks, Trojans, Information disclosure, Credit Card Detection, Bad Robot etc.	Requesting to remove as these are WAF specific features which is already ask in RFP	Clause stands deleted

44	Web Proxy	307	SWG should have capabilities to limit number of parameters in URL, number of cookies in request, number of headers lines in request, total URL and Body parameters in length to block advanced HTTP layer attacks.	Requesting to remove as these are WAF specific features which is already ask in RFP	Clause stands deleted
45	Web Proxy	307	The proposed system shall allow administrator to prevent sensitive data from leaving the network. 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. The DLP capability shall support the following protocol & activities: i HTTP/HTTPS POST, HTTP/HTTPS GET ii FTP PUT, GET iii SMTP, IMAP, POP3, SMTPS, IMAPS, POP3S	Requesting to change to "The proposed system shall allow administrator to prevent sensitive data from leaving the network. 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" except for HTTP/HTTPS mentioned ports are email, firewall specific and not web ports wherein in current form becoming specific to OEM thus requesting change	The proposed system shall allow administrator to prevent sensitive data from leaving the network. 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. The DLP capability shall support the following protocol & activities: HTTP/HTTPS POST, HTTP/HTTPS GET
46	Web Proxy	307	The DLP capability shall be configured by creating individual rules, combining the rules into sensors, and then assigning them to profiles which in turn bind to firewall policies.	Requesting to change to "The DLP capability shall be configured by creating individual rules or combining the rules into sensors, and then assigning them to profiles which in turn bind to policies"	The DLP capability shall be configured by creating individual rules or combining the rules into sensors, and then assigning them to profiles which in turn bind to policies
47	Web Proxy	307	Ban: if the user is authenticated, will block all traffic to or from the user using the protocol that triggered the rule and the user will be added to the Banned User list. If the user is not authenticated, all traffic of the protocol that triggered the rule from the user using will be blocked.	Requesting to change to "Ban: if the user is authenticated, will block all traffic to or from the user using the protocol that triggered the rule" in current form it is specific to OEM, thus requesting change	Ban: if the user is authenticated, will block all traffic to or from the user using the protocol that triggered the rule"
48	SSL VPN	312	The appliance should be dedicated SSL VPN Gateway and not a part of UTM/ firewall/ NGFW/ ADC device It should have should have 1x1GbE port for management and 8x10 SFP+ ports Should be populated with its transceivers	Requesting to change to "The appliance should be dedicated SSL VPN Gateway. It should have should have 1x1GbE port for management and 8x10 SFP+ ports Should be populated with its transceivers" in current form it is OEM specific and thus requesting change for wider participation	The appliance should be dedicated SSL VPN Gateway . It should have should have 1x1GbE port for management and 8x10 SFP+ ports Should be populated with its transceivers
49	SSL VPN	312	The appliance should have multicore CPU, 64GB RAM, 1TB or higher HDD and dual power supply.	Requesting to change to "The appliance should have multicore CPU, 64GB RAM, 800GB or higher HDD/SSD with redundant hot swappable field replaceable dual power supply and fan module/tray" In multiple solutions in RFP the storage ask is 250Gb on perimeter solution and 1Tb ask on VPN gateway is OEM specific, the field replaceability along with redundancy on power supply, fan module is very important considering the VPN device is inline perimeter network device wherein during failure scenario individual modules replacement ensures higher TCO as against every time removing the device, reconfiguring it during the RMA	The appliance should have multicore CPU, 64GB RAM, 400 GB or higher HDD and dual power supply.
50	SSL VPN	312	The solution Should have dedicated hardware SSL card and should support 35 Gbps of SSL Throughput	Requesting change to "The solution Should have dedicated hardware SSL card and should support 35 Gbps of VPN throughput" SSL throughput is relevant for SSL off loaders since this is a VPN device it should have VPN throughput mentioned.	The solution Should have dedicated hardware SSL card and should support 10 Gbps of SSL Throughput
51	SSL VPN	312	The appliance should support 35 Gbps of compression throughput. This capability shall be compatible with most modern browsers, requiring no additional software.	Requesting to remove as this is OEM specific	The appliance should support 10 Gbps of compression throughput. This capability shall be compatible with most modern browsers, requiring no additional software.
52	SSL VPN	312	The solution must provide ranking of at least 4 authentication methods for granular authentication of VPN users	Requesting to remove as this is OEM specific	The solution must provide ranking of at least 3 authentication methods for granular authentication of VPN users
53	SSL VPN	313	The solution should also provide Step-up authentication. This feature allows a per-request policy to authenticate a user at any time during a VPN session. Per-request policy subroutine allows you to create time-limited sub sessions to allow user access to areas of an application based on a different gating criteria. the following authentication types for step-up authentication should be supported: Multi-factor authentication through Radius authentication Certificate-based authentication Password-based authentication	Requesting to change to "The solution should also provide Step-up authentication. This feature allows a per- request policy to authenticate the following authentication types for step-up authentication should be supported: Multi-factor authentication through Radius authentication Certificate-based authentication Password-based authentication" requesting change for wider participation as currently it is OEM specific.	As per Tender Document

54	SSL VPN	313	The Solution should be able to support robust endpoint posture inspection and deny access for non-compliance endpoints. The Solution must support the following checks: * Able to perform Antivirus/Malware software checks, including checks for Enabled State, Engine & Database version, Last Scan, and Last Update of the antivirus software. * Able to perform domain check to auto connect to VPN when outside the office network. * Able to perform IP address / Geolocation check to restrict access from unwanted locations. "* Able to perform Operating System, Windows Registry, File or Process checks. * Able to check if mobile devices have been jailbroken."	Requesting to change to "The Solution should be able to support robust endpoint posture inspection and deny access for non-compliance endpoints. The Solution must support the following checks: * Able to perform Antivirus/Malware software checks, * Able to perform domain check * Able to perform IP address / Geolocation check to restrict access from unwanted locations. "* Able to perform Operating System" requesting change for wider participation as currently it is OEM specific and in overall RFP NAC/AAA is asked which should be used as central authenticator layer irrespective the user comes from land/vpn or wireless.	As per Tender Document
55	NAC (included AAA)	330	The solution should provide below Deep Compliance checks on minimum based on OESIS Framework from Day 1 on windows & mac-OS endpoints: 1) Check Specific Anti-malware product version and last signature update date 2) Threats detected by the installed Anti-malware product with option to configure threat exclusion. 3) Disk Encryption status of System & Local volume Encryption tool & its version.	Requesting to change to "The solution should provide below Deep Compliance checks on minimum from Day 1 on windows, Linux & mac-OS endpoints: 1) Check Specific Anti-malware product version and last signature update date 2) Threats detected by the installed Anti-malware/Vulnerability scanner product with option to configure threat exclusion. 3) Disk Encryption status of System & Application tool & its version" in current form it is OEM specific thus requesting change	As per Tender Document
56	NAC (included AAA)	330	The solution should provide the end user to request for temporary access in case of authentication/authorization failure that can be approved by a admin	Requesting to remove as this is OEM specific	As per Tender Document
57	NAC (included AAA)	330	The solution should allow endpoint to detect Man In the Middle (MITM) attack using the agent	Requesting change as this is firewall related capability not a function of NAC	The solution should allow endpoint to detect Man In the Middle (MITM) attack with/without the agent
58	NAC (included AAA)	330	The solution should have http/SNI proxy based remediation options	Requesting change as this is firewall, web proxy related capability not a function of NAC	The solution should have http/SNI/VLAN based remediation options
59	IPS/IDS	261	NIPS solution should be a purpose built dedicated standalone appliance and not an integrated firewall module or UTM appliance.	Requesting change to "NIPS solution should be a dedicated appliance with dedicated processing engine and not a part of DDOS, UTM, Web Proxy, appliance" many vendors use the common off the shelf OS thus it is important wherein dedicated appliance is required it should also have dedicated processing engines and not shared with other modules	As per Tender Document
60	IPS/IDS	261	The appliance must have Real World Throughput of 10 Gbps and scalable up to 30 Gbps for future requirements on the same appliance	Requesting to change to "The appliance must have Real World Throughput of 30 Gbps" requesting change as it is OEM specific.	The appliance must have Real World Throughput of 10 Gbps and scalable up to 20 Gbps for future requirements on the same appliance
61	IPS/IDS	262	Should have capability for Host quarantine and rate limiting	Requesting to change to "Should have capability for Host quarantine/IP blacklisting and rate limiting" different vendor have different approach the requesting change doesn't change any functionality but allow for more participation thus requesting change	Should have capability for Host quarantine/IP blacklisting and rate limiting
62	IPS/IDS	264	PS must support Inbound SSL Inspection detection and prevention using dynamic agent based key for ECDHA cypher suits	Requesting to change to "IPS must support Inbound SSL Inspection detection and prevention" in current form this is OEM specific thus requesting change for wider participation as the requested change doesn't change any functionality of the RFP	As per Tender Document

63	IPS/IDS	264	IPS must have multiple signature less engines on the appliance without degrading the performance.	Requesting to change to "IPS must have both signature and signature less engines on the appliance without degrading the performance. It must have 25000+ plus pre-build signatures from day1 excluding the custom signatures" IPS must have both approaches as without signatures every time a known attack or traffic is seen it has to be inspected with DPI leading to performance overhead increased latency thus it is important to have the signature count mentioned to improve the overall efficacy of the solution.	As per Tender Document
64	Internet Firewall	259	60 Gbps or higher with 128 KB HTTP/HTTPs	Requesting to change to "60 Gbps or higher with TCP or HTTP/HTTPs" 128KB is a very large packet and only a specific OEM provides reference numbers on it for a interface with MTU of 1500byte 128KB packet would lead to lot of fragmentation thereby negatively impacting the CPU	As per Tender Document
65	Internet Firewall	259	100 Million Layer 4 sessions or 40 Million Layer 7 sessions	Requesting to change to "100 Million Layer 4 sessions or 30 Million Layer 7 sessions measured with Firewall and Application controlled enabled" current clause in as is form is giving a particular OEM advantage thus for equal participation requesting change	100 Million Layer 4 sessions or 30 Million Layer 7 sessions
66	Internet Firewall	260	Minimum 3 Million Layer 4 sessions or Minimum 1.2 Million Layer 7 sessions	Request to change to "Minimum 3 Million Layer 4 sessions or Minimum 600K Layer 7 sessions measured Firewall and Application Control enabled" current clause in as is form is giving a particular OEM advantage thus for equal participation requesting change	As per Tender Document
67	Internet Firewall	260	35 Gbps (Packet size: 128 KB HTTP/HTTPs) or Higher	Requesting to change to "35 Gbps (measured with TCP or HTTP/HTTPs) or Higher" 128KB is a very large packet and only a specific OEM provides reference numbers on it for a interface with MTU of 1500byte 128KB packet would lead to lot of fragmentation thereby negatively impacting the CPU	As per Tender Document
68	Internet Firewall	260	Redundant Power Supply	Requesting to change to Redundant hot swappable and field replaceable power supply" as power supply is an environment directly exposed to the environmental conditions and leading to a failure pf PSU with no field replaceability requires every time the appliance to be replaced manually and then configuring the new appliance thereby increasing the overall TCO and higher downtime window	As per Tender Document
69	Internet Firewall	260	Redundant FAN for fully loaded chassis from day 1	Requesting to change to Redundant hot swappable and field replaceable fan fully loaded chassis from day 1" as fan is an environment directly exposed to the environmental conditions and leading to a failure of fan with no field replaceability requires every time the appliance to be replaced manually and then configuring the new appliance thereby increasing the overall TCO and higher downtime window	As per Tender Document
70	BoQ	168	In case a bidder quotes a solution of higher specifcations than sought specifications , bidder needs to ensure that all specifications / features / functionality/ relevant hardware/SFPs must be delivered , installed & commissioned. E.g instead of 24 port switch , a 48 port switch is quoted by a bidder, he needs to populate SFPs for 48 ports before offering the milestone for delivery	Requesting to remove this clause as the minumum qualifying criteria in terms of feature , interfaces and SFP is already mentioned in the respective section. In case a bidder is quoting 48 port switch to meet the 24 port requirement due to model limitation, then this cluase will increase the overall commercials of the quoted product.	This Clause Stands Deleted
71	Spine Switch for DC	25	**(10) b. Security Features** Port, VLAN & Routed ACL,802.1x,16K or higher ACL Entries/group based-segmentation-entries, GRE (Must Support 1000 or Higher GRE Tunnels or 1000 VXLAN Tunnels)	802.1x is the feature required on access switch where users connect for authentication supported by AAA. Request to remove the clause from SPINE / Core Switch for solution clarity and wider participation .	Port, VLAN & Routed ACL,9K or higher ACL Entries/group based-segmentation-entries, GRE (Must Support 1000 or Higher GRE Tunnels or 1000 VXLAN Tunnels)
72	Spine Switch for DC	25	**(11) c. Management Protocol** Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sFlow/Netflow, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN, data plane telemetry, buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations.	**Request change :-** buffer queue depth monitoring / QOS for prioritizing the traffic during congestion with minimum 8 queue per port.	Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, sflow/netflow/IPFIX, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN, telemetry , buffer queue depth monitoring/QOS for prioritizing the traffic during congestion with minimum 8 queue per port, Same OS across all the proposed network switches for simplified operations.

73	Spine Switch for DC	25	**Feature Support:** Device, OS, Optics, Manager from same OEM. Should be managed through unified Network Manager.	The Fabric build using SPINE and Leaf switches is managed by Fabric Manager , All other switches such as OOB , WAN should be managed by NMS / EMS asked in the tender as these switches will not run EVPN VXLAN .We request to allow Fabric (SPINE & LEAF) to be managed by Fabric Manager with the advance feature required for EVPN -VXLAN fabric and other devices including switches, Router and Firewall to be managed by NMS/EMS asked in the tender . **Requested Clause :-** Device, OS, Optics, Spine & Leaf Fabric Manager from same OEM	As per Tender Document
74	Spine Switch for DR	26	**(10) b. Security Features** Port, VLAN & Routed ACL,**802.1x**,16K or higher ACL Entries/group based-segmentation-entries, GRE (Must Support 1000 or Higher GRE Tunnels or 1000 VXLAN Tunnels)	802.1x is the feature required on access switch where users connect for authentication supported by AAA. Request to remove the clause from SPINE / Core Switch for solution clarity and wider participation .	**(10) b. Security Features** Port, VLAN & Routed ACL,9K or higher ACL Entries/group based-segmentation-entries, GRE (Must Support 1000 or Higher GRE Tunnels or 1000 VXLAN Tunnels)
75	Spine Switch for DR	26	**(11) c. Management Protocol** Role Based CLI, SNMPv1/v2/v3, OpenStack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sFlow/Netflow, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN, data plane telemetry, buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations.	**Request change :-** buffer queue depth monitoring / QOS for prioritizing the traffic during congestion with minimum 8 queue per port.	Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, sflow/netflow/IPFIX, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN, telemetry , buffer queue depth monitoring/QOS for prioritizing the traffic during congestion with minimum 8 queue per por, Same OS across all the proposed network switches for simplified operations.
76	Spine Switch for DR	27	**Feature Support:** Device, OS, Optics, Manager from same OEM. Should be managed through unified Network Manager.	The Fabric build using SPINE and Leaf switches is managed by Fabric Manager , All other switches such as OOB , WAN should be managed by NMS / EMS asked in the tender as these switches will not run EVPN VXLAN .We request to allow Fabric (SPINE & LEAF) to be managed by Fabric Manager with the advance feature required for EVPN -VXLAN fabric and other devices including switches, Router and Firewall to be managed by NMS/EMS asked in the tender . **Requested Clause :-** Device, OS, Optics, Spine & Leaf Fabric Manager from same OEM	As per Tender Document
77	Leaf Switch	28	**(8) c. Management Protocol:** Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN, data plane telemetry to trace path and per hop latency for a flow , buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations.	**Request to change the clause :-** data plane telemetry to check the switch -Switch Port / end to end latency for flow/sflow , buffer queue depth monitoring / QOS for prioritizing the traffic during congestion with minimum 8 queue per port	Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, sflow/netflow/IPFIX, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN, telemetry , buffer queue depth monitoring/QOS for prioritizing the traffic during congestion with minimum 8 queue per por, Same OS across all the proposed network switches for simplified operations.
78	Leaf Switch	29	**Feature Support:** Device, OS, Optics, Manager from same OEM. Should be managed through unified Network Manager.	The Fabric build using SPINE and Leaf switches is managed by Fabric Manager , All other switches such as OOB , WAN should be managed by NMS / EMS asked in the tender as these switches will not run EVPN VXLAN .We request to allow Fabric (SPINE & LEAF) to be managed by Fabric Manager with the advance feature required for EVPN -VXLAN fabric and other devices including switches, Router and Firewall to be managed by NMS/EMS asked in the tender . Requested Clause :- Device, OS, Optics, Spine & Leaf Fabric Manager from same OEM	As per Tender Document
79	Border Leaf Switch	30	(7)c. Management Protocol Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX, PTP, OpenConfig, Filtered packet mirroring over GRE/span, data plane telemetry to trace path and per hop latency for a flow , buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations.	Request to change the clause :- data plane telemetry to check the switch -Switch Port / end to end latency for flow/sflow , buffer queue depth monitoring / QOS for prioritizing the traffic during congestion with minimum 8 queue per port	Please read the modified clause as below: Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, sflow/netflow/IPFIX, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN, telemetry , buffer queue depth monitoring/QOS for prioritizing the traffic during congestion with minimum 8 queue per port, Same OS across all the proposed network switches for simplified operations.

80	Border Leaf Switch	30	(12) Feature Support Device, OS, Optics, Manager from same OEM. Should be managed through unified Network Manager.	The Fabric build using SPINE and Leaf switches is managed by Fabric Manager , All other switches such as OOB , WAN should be managed by NMS / EMS asked in the tender as these switches will not run EVPN VXLAN .We request to allow Fabric (SPINE & LEAF) to be managed by Fabric Manager with the advance feature required for EVPN -VXLAN fabric and other devices including switches, Router and Firewall to be managed by NMS/EMS asked in the tender . Requested Clause :- Device, OS, Optics, Spine & Leaf Fabric Manager from same OEM	As per Tender Document
81	OOB Core Switch for DC	31	(9) b. Security Feature Port, VLAN & Routed ACL, 1500 Ingress /1500 Egress ACL Entries/ Group-based micro-segmentation, 802.1x.	802.1x is the feature required on access switch where users connect for authentication supported by AAA. Request to remove the clause from SPINE / Core Switch for solution clarity and wider participation .	Security Feature Port, VLAN & Routed ACL, 1500 Ingress /1500 Egress ACL Entries/ Group-based micro-segmentation
82	OOB Core Switch for DC	32	(14) Feature Support Device, OS, Optics, Manager from same OEM. Should be managed through unified Network Manager.	The Fabric build using SPINE and Leaf switches is managed by Fabric Manager , All other switches such as OOB , WAN should be managed by NMS / EMS asked in the tender as these switches will not run EVPN VXLAN .We request to allow Fabric (SPINE & LEAF) to be managed by Fabric Manager with the advance feature required for EVPN -VXLAN fabric and other devices including switches, Router and Firewall to be managed by NMS/EMS asked in the tender . Requested Clause :- Device, OS, Optics, from same OEM . Device should be managed by any open standard NMS/ EMS.	As per Tender Document
83	OOB Core Switch for DC	33	(9) b. Security Feature Port, VLAN & Routed ACL, 1500 Ingress /1500 Egress ACL Entries/ Group-based micro-segmentation, 802.1x.	802.1x is the feature required on access switch where users connect for authentication supported by AAA. Request to remove the clause from SPINE / Core Switch for solution clarity and wider participation .	Kindly refer Revised Technical specification
84	OOB Core Switch for DC	33	(14) Feature Support Device, OS, Optics, Manager from same OEM. Should be managed through unified Network Manager.	The Fabric build using SPINE and Leaf switches is managed by Fabric Manager , All other switches such as OOB , WAN should be managed by NMS / EMS asked in the tender as these switches will not run EVPN VXLAN .We request to allow Fabric (SPINE & LEAF) to be managed by Fabric Manager with the advance feature required for EVPN -VXLAN fabric and other devices including switches, Router and Firewall to be managed by NMS/EMS asked in the tender . Requested Clause :- Device, OS, Optics, from same OEM . Device should be managed by any open standard NMS/ EMS.	As per Tender Document
85	OOB Access Switch	35	**(12) QOS** 802.1p,SP,Queues per port, WRED /WTD, Sflow/Netflow, Shaping, Policing/Rate Limiting, Strict Priority Queueing or Low Latency Queueing, PFC and ECN	The switch asked is Access switch which will connect either the user or Mgmt Port of servers / Spine Switch / Leaf Switch / Firewall and Router . PFC is required for Leaf switch which supports DCBX and PFC is part of it and is used to control the flow which is done by 802.3x in normal switch . The same is not required on OOB Access switch . Request to change the clause as PFC / 802.3x	802.1p,SP,Queues per port, WRED /WTD, Sflow/Netflow, Shaping, Policing/Rate Limiting, Strict Priority Queueing or Low Latency Queueing, ECN and PFC / 802.3x

86	OOB Access Switch	35	(14) Feature Support Device, OS, Optics, Manager from same OEM. Should be managed through unified Network Manager.	The Fabric build using SPINE and Leaf switches is managed by Fabric Manager , All other switches such as OOB , WAN should be managed by NMS / EMS asked in the tender as these switches will not run EVPN VXLAN .We request to allow Fabric (SPINE & LEAF) to be managed by Fabric Manager with the advance feature required for EVPN -VXLAN fabric and other devices including switches, Router and Firewall to be managed by NMS/EMS asked in the tender . Requested Clause :- Device, OS, Optics, from same OEM . Device should be managed by any open standard NMS/ EMS.	As per Tender Document
87	Remote Site Switch	36	(9) b. security Feature Port, VLAN & Routed ACL,1500 Ingress/1500 Egress ACL Entries, 802.1x, MAC 220K	The MAC address asked for type of switch are very high , We understand that MAC address on remote location will not be more . Request to relax the MAC scale to 100K for solution clarity and level playing field for OEMs .	security Feature Port, VLAN & Routed ACL,1500 Ingress/1500 Egress ACL Entries, 802.1x, MAC 100K
88	Remote Site Switch	36	(11) d. QOS WRED,SPQ, SDWRR / WRR, 32MB Buffer, 8queues / port, PFC and ECN	The switch will be installed in remote location where huge buffer are not required as the traffic aggregated should be sent to DC/DR hence request to reduce the buffer and change the PFC as the switch is enterprise grade and will be used to aggregate send the traffic on high speed Requested clause :- 8MB buffer , PFC/ 802.3x	OS WRED,SPQ, SDWRR / WRR, 32MB Buffer, 8queues / port, ECN and PFC/802.3x
89	Remote Site Switch	36	(14) Feature Support Device, OS, Optics, Manager from same OEM. Should be managed through unified Network Manager.	The Fabric build using SPINE and Leaf switches is managed by Fabric Manager , All other switches such as OOB , WAN should be managed by NMS / EMS asked in the tender as these switches will not run EVPN VXLAN .We request to allow Fabric (SPINE & LEAF) to be managed by Fabric Manager with the advance feature required for EVPN -VXLAN fabric and other devices including switches, Router and Firewall to be managed by NMS/EMS asked in the tender . Requested Clause :- Device, OS, Optics, from same OEM . Device should be managed by any open standard NMS/ EMS.	Device, OS, Optics, from same OEM .
90	Interconnect Switch	37	(7) c. Management Protocol c. Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, NTP, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sflow/netflow, OpenConfig, Filtered packet mirroring over GRE/SPAN, data plane telemetry to trace path and per hop latency for a flow, buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations.	Request to change the clause :- data plane telemetry to check the switch -Switch Port / end to end latency for flow/sflow , buffer queue depth monitoring / QOS for prioritizing the traffic during congestion with minimum 8 queue per port	Please read the modified clause as below: Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, sflow/netflow/IPFIX, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN, telemetry , buffer queue depth monitoring/QOS for prioritizing the traffic during congestion with minimum 8 queue per port, Same OS across all the proposed network switches for simplified operations.
91	Interconnect Switch	37	(9) Security Features VLAN & Routed ACL, Should support 2K or more ACL entries or 32K or more prefix/host entries as endpoint for traffic segmentation, 802.1x, RADIUS/TACACS, Port Security / equivalent ,BPDU Guard, IGMP snooping	The ACL entries asked are higher for the switch types asked , request to reduce the ACL count as same asked in Leaf switch . Requested clause :- Should support 1500 Ingress /1500 Egress ACL Entries or 32K or more prefix/host entries as endpoint for traffic segmentation	Security Features VLAN & Routed ACL, Should support 1500 Ingress /1500 Egress ACL entries or 32K or more prefix/host entries as endpoint for traffic segmentation, 802.1x, RADIUS/TACACS, Port Security / equivalent ,BPDU Guard, IGMP snooping
92	Interconnect Switch	38	(13) Feature Support Device, OS, Optics, Manager from same OEM. Should be managed through unified Network Manager.	The Fabric build using SPINE and Leaf switches is managed by Fabric Manager , All other switches such as OOB , WAN should be managed by NMS / EMS asked in the tender as these switches will not run EVPN VXLAN .We request to allow Fabric (SPINE & LEAF) to be managed by Fabric Manager with the advance feature required for EVPN -VXLAN fabric and other devices including switches, Router and Firewall to be managed by NMS/EMS asked in the tender . Requested Clause :- Device, OS, Optics, from same OEM . Device should be managed by any open standard NMS/ EMS.	As per Tender Document

93	Interconnect Switch	39	(7) c. Management Protocol c. Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, NTP, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sflow/netflow, OpenConfig, Filtered packet mirroring over GRE/SPAN, data plane telemetry to trace path and per hop latency for a flow, buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations.	Request to change the clause :- data plane telemetry to check the switch -Switch Port / end to end latency for flow/sflow , buffer queue depth monitoring / QOS for prioritizing the traffic during congestion with minimum 8 queue per port	Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, sflow/netflow/IPFIX, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN, telemetry , buffer queue depth monitoring/QOS for prioritizing the traffic during congestion with minimum 8 queue per port, Same OS across all the proposed network switches for simplified operations.
94	Interconnect Switch	39	(9) Security Features VLAN & Routed ACL, Should support 2K or more ACL entries or 32K or more prefix/host entries as endpoint for traffic segmentation, 802.1x, RADIUS/TACACS, Port Security / equivalent ,BPDU Guard, IGMP snooping	The ACL entries asked are higher for the switch types asked , request to reduce the ACL count as same asked in Leaf switch . Requested clause :- Should support 1500 Ingress /1500 Egress ACL Entries or 32K or more prefix/host entries as endpoint for traffic segmentation	Security Features VLAN & Routed ACL, Should support 1500 Ingress /1500 EgressACL entries or 32K or more prefix/host entries as endpoint for traffic segmentation, 802.1x, RADIUS/TACACS, Port Security / equivalent ,BPDU Guard, IGMP snooping
95	Interconnect Switch	39	(13) Feature Support Device, OS, Optics, Manager from same OEM. Should be managed through unified Network Manager.	The Fabric build using SPINE and Leaf switches is managed by Fabric Manager , All other switches such as OOB , WAN should be managed by NMS / EMS asked in the tender as these switches will not run EVPN VXLAN .We request to allow Fabric (SPINE & LEAF) to be managed by Fabric Manager with the advance feature required for EVPN -VXLAN fabric and other devices including switches, Router and Firewall to be managed by NMS/EMS asked in the tender . Requested Clause :- Device, OS, Optics, from same OEM . Device should be managed by any open standard NMS/ EMS.	As per Tender Document
96	WAN Switch	40	(7) b. Security Feature Port, VLAN & Routed ACL, 802.1x. Should support 2K or more ACL entries or 32K or more prefix/host entries as endpoint for traffic segmentation.	The ACL entries asked are higher for the switch types asked , request to reduce the ACL count as same asked in Leaf switch . Requested clause :- Should support 1500 Ingress /1500 Egress ACL Entries or 32K or more prefix/host entries as endpoint for traffic segmentation	Security Feature Port, VLAN & Routed ACL, 802.1x. Should support 1500 Ingress /1500 Egress or more ACL entries or 32K or more prefix/host entries as endpoint for traffic segmentation.
97	WAN Switch	40	(8) c. Management Protocol Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sflow/netflow, OpenConfig, Filtered packet mirroring over GRE/span, data plane telemetry to trace path and per hop latency for a flow , buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations	Request to change the clause :- data plane telemetry to check the switch -Switch Port / end to end latency for flow/sflow , buffer queue depth monitoring / QOS for prioritizing the traffic during congestion with minimum 8 queue per port	Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, sflow/netflow/IPFIX, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN, data plane telemetry , buffer queue depth monitoring/QOS for prioritizing the traffic during congestion with minimum 8 queue per por, Same OS across all the proposed network switches for simplified operations.
98	WAN Switch	41	(13) Feature Support Device, OS, Optics, Manager from same OEM. Should be managed through unified Network Manager.	The Fabric build using SPINE and Leaf switches is managed by Fabric Manager , All other switches such as OOB , WAN should be managed by NMS / EMS asked in the tender as these switches will not run EVPN VXLAN .We request to allow Fabric (SPINE & LEAF) to be managed by Fabric Manager with the advance feature required for EVPN -VXLAN fabric and other devices including switches, Router and Firewall to be managed by NMS/EMS asked in the tender . Requested Clause :- Device, OS, Optics, from same OEM . Device should be managed by any open standard NMS/ EMS.	As per Tender Document
99	Layer 3 Access Switch	43	(16) Feature Support Device, OS, Optics, Manager from same OEM. Should be managed through unified Network Manager.	The Fabric build using SPINE and Leaf switches is managed by Fabric Manager , All other switches such as OOB , WAN should be managed by NMS / EMS asked in the tender as these switches will not run EVPN VXLAN .We request to allow Fabric (SPINE & LEAF) to be managed by Fabric Manager with the advance feature required for EVPN -VXLAN fabric and other devices including switches, Router and Firewall to be managed by NMS/EMS asked in the tender . Requested Clause :- Device, OS, Optics, from same OEM . Device should be managed by any open standard NMS/ EMS.	Device, OS, Optics, from same OEM.

100	CE Router	43	(3) Routing Engine The Router should be populated with redundant Routing Card/Engines/control plane /supervisor engine/multi-core x86 CPU	Multi-core CPU and Redundancy in Routing Card/Engines/control plane /supervisor engine are not same . Due to the critical nature of network it is advised to have physical hardware redundancy of control plane , Multi core can provide more scale and software level redundancy only which may not help in achieving the control plane redundancy in time of failure of CPU . We request to remove the multicore X-86 CPU for solution clarity or allow single control plane for solution clarity and level playing field .	Kindly refer revised Technical Specification
101	CE Router	44	(14) Feature Support Device, OS, Optics, Manager from same OEM. Should be managed through unified Network Manager.	The Fabric build using SPINE and Leaf switches is managed by Fabric Manager , All other switches such as OOB , WAN should be managed by NMS / EMS asked in the tender as these switches will not run EVPN VXLAN .We request to allow Fabric (SPINE & LEAF) to be managed by Fabric Manager with the advance feature required for EVPN -VXLAN fabric and other devices including switches, Router and Firewall to be managed by NMS/EMS asked in the tender . Requested Clause :- Device, OS, Optics, from same OEM . Device should be managed by any open standard NMS/ EMS.	Kindly refer revised Technical Specification
102	Internet Router	45	(3) Port Population :- Should be supplied on day 1 with 4 x 1000Base-LX Single Mode SFP transceivers, 4 x 10/100/1000Base-T Interface Ports and 4 x 10G Base SR Transceivers. Should be scalable to support additional 4 X 40/100G QSFP ports; Fully Populated from Day-1	10m and 100m speed on copper interface is not available on high speed Router , Request to relax the clause for leading OEM to participate . Requested Clause :- 4 X 1000Base T interface	Kindly refer revised Technical Specification
103	Internet Router	45	(6) Routing Protocols:- OSPF, BGP, MPLS, EVPN-MPLS, Segment Routing, Multicasting MVPN, MOFRR, RSVP- TE, LDP, BGP-LU, SR-TE	Multicast VPN and MOFRR provides the same functionality , request to change the clause as below Requested Clause :- Multicasting MVPN / MOFRR	Routing Protocols:- OSPF, BGP, MPLS, EVPN-MPLS, Segment Routing, Multicasting MVPN/MOFRR, RSVP-TE, LDP, BGP-LU, SR-TE
104	Internet Router	46	(13) Feature Support Device, OS, Optics, Manager from same OEM. Should be managed through unified Network Manager.	The Fabric build using SPINE and Leaf switches is managed by Fabric Manager , All other switches such as OOB , WAN should be managed by NMS / EMS asked in the tender as these switches will not run EVPN VXLAN .We request to allow Fabric (SPINE & LEAF) to be managed by Fabric Manager with the advance feature required for EVPN -VXLAN fabric and other devices including switches, Router and Firewall to be managed by NMS/EMS asked in the tender . Requested Clause :- Device, OS, Optics, from same OEM . Device should be managed by any open standard NMS/ EMS.	Device, OS, Optics, from same OEM
105	Network Manager	52	Solution to be provided for unified management and monitoring of all the proposed network switches of DC and DR that are part of the RFP.	We understand that NMS / EMS asked in the RFP will manage all IP based Devices except EVPN-VXLAN Fabric build out of Spine , Leaf and Border leaf switch . Request to change the clause for maximum participation and allow leading OEM to participate . **Requested Clause :-** Solution to be provided for unified management and monitoring of all the proposed Spine , leaf and Border leaf switch in DC and DR .	As per Tender Document
106	Network Manager	52	The solution should provide UI-driven wizard based approach to simplify and accelerate deployment of EVPN overlay fabric by automatically generating the resultant CLI configurations and pushing it to the Data Center network Switches.	**Request to change :-** The solution should provide UI-driven wizard based approach to simplify and accelerate deployment of EVPN overlay fabric by automatically generating the resultant CLI configurations and pushing it to the Data Center network Switches (Spine , Leaf & Border Leaf)	The solution should provide UI-driven wizard based approach to simplify and accelerate deployment of EVPN overlay fabric by automatically generating the resultant CLI configurations and pushing it to the Data Center network Switches (Spine , Leaf & Border Leaf)

107	Network Manager	52	The Solution should provide management of group-based segmentation/ACL rules centrally from the unified dashboard.	**Request to change :-** The Solution should provide management of group-based segmentation rules centrally from the unified dashboard for Fabric (Spine & Leaf).	As per Tender Document
108	Network Manager	52	Image upgradation and patch management of the managed network devices should be supported Centrally.	**Request Change :-** Image upgradation / patch management of the managed network devices should be supported Centrally for Spine and Leaf Fabric .	Image upgradation / patch management of the managed network devices should be supported Centrally for Spine and Leaf Fabric
109	Network Manager	52	The Manager should support user defined work flows to carry out multiple network-wide changes with Support for automated execution and conditional checks.	**Request Change :-** The fabric Manager should support user-defined/configuration work flows to carry out multiple network-wide changes automated execution and conditional/system checks.	The Network Manager should support user-defined/configuration work flows to carry out multiple network-wide changes automated execution and conditional/system checks.
110	Network Manager	52	The Manager should gather streaming telemetry (that is not SNMP and flow data based) in realtime from all the managed devices.	**Request Change :-** The Manager should gather streaming telemetry from all the managed devices for management .	The Network Manager should gather streaming telemetry from all the managed devices for management
111	Network Manager	52	Visibility of the these parameters is expected but not limited to - CPU, Memory, interface stats (traffic counter, error, discard), MAC table, ARP table, IPv6 ND table, IPv4 route table, IPv6 route table, Multicast table, BGP, capacity parameters / TCAM ,running config, traffic flow (sflow/IPFIX/Netflow), buffer utilization per interface, MLAG Stats, Switch environment stats(FAN, Temperature, Power Supply).	**Request Change :-** Visibility of the these parameters is expected - CPU, Memory, interface stats (traffic counter, error, discard), MAC table, ARP table, IPv4 route table, IPv6 route table, BGP, file system storage parameters, VXLAN table / VNID Table , running config, traffic flow (sflow/IPFIX/Netflow), , Switch environment stats(FAN, Temperature, Power Supply).	Visibility of the these parameters is expected but not limited to - CPU, Memory, interface stats (traffic counter, error, discard), MAC table, ARP table, IPv4 route table, IPv6 route table, BGP, capacity parameters / TCAM/VXLAN/VNID table ,running config, traffic flow (sflow/IPFIX/Netflow), Switch environment stats(FAN, Temperature, Power Supply).
112	Network Manager	53	Should be capable of showing hop-by-hop flow path and drops on links taken by a flow between 2 end points.	**Request Change :-** Should be capable of showing hop-by-hop flow path and drops on links taken by a flow between 2 end points or should support SFLOW	Kindly refer Revised Technical specification
113	Network Manager	53	Should be able to show deviation from user defined config/policy and Switch image as part of the compliance.	**Request Change :-** Should be able to show deviation from user defined config/policy	Should be able to show deviation from user defined config/policy
114	Network Manager	53	All proposed network switches part of this RFP should be managed from single dashboard for ease of management.	please remove as the Fabric manger will only manage Spine , Leaf and Border leaf switch only **Request Change :-** All proposed network switches in fabric (Spine, Leaf , Border Leaf) part of this RFP should be managed from single dashboard for ease of management.	As per Tender Document
115	Network Manager	53	Should support ML for dynamic baselining/proactive alerting/suggestion.	**Request Change :-** Should support ML/telemetry for proactive alerting/suggestion.	Should support ML for dynamic baselining/proactive alerting/suggestion or Should support telemetry for proactive alerting/suggestion.

116	Network Manager	53	Central controller should provide detailed traffic flow analytics to search and see what protocols/port are used and how much data is transferred between 2 end-points during a period of time.	**Request Change :-** Central controller should provide detailed traffic flow analytics to search and see what protocols/port are used and how much data is transferred between 2 end-points during a period of time or should support SFLOW .	Central controller should provide detailed traffic flow analytics to search and see what protocols/port are used and how much data is transferred between 2 end-points during a period of time or should support Netflow/SFLOW Or Central controller should provide detailed traffic flow analytics to search and to show ping, traceroute, forward and reverse path between 2 end-points.
117	Network Manager	53	All licenses required for the mentioned features must be available on day-1 for all the proposed network switches as part of this RFP	**Request Change :-** All licenses required for the mentioned features must be available on day-1 for all the proposed Spine switches , Leaf switches and Border Leaf Switches .	All licenses required for the mentioned features as per product specification must be available on day-1 for all the proposed network switches as part of this RFP
118	Network Manager	54	All the communication between Fabric management appliance and switches should be TLS1.2 or higher encrypted.	**Request Change :-** All the communication between Fabric management appliance and switches should be encrypted.	All the communication between Fabric management appliance and switches should encrypted
119	Network Manager	54	Bidder shall provide required server Hardware & Software to run the solution in HA within a site and to support HA across sites. Failure of all server hardware should not impact packet forwarding on the network devices.	**Request Change :-** Bidder shall provide required server Hardware & Software to run the solution in HA for DC & DR Respectively . Failure of all server hardware should not impact packet forwarding on the network devices.	Bidder shall provide required server Hardware & Software to run the solution in HA for DC & DR Respectively . Failure of all server hardware should not impact packet forwarding on the network devices.
120	Network Manager	54	C.) Each DR spine switch will have 150 X 100G port (Total 2 X 150, 100G port).	**Request Clarification :-** Total 140 Ports are been asked of 100G in DR Spine (page 26 -11 Spine switch for DR) , Kindly change the clause to 140 or more in Section " Annexure-1 (Technical Specifications) / 31 Network-1,100G Network:" Requested Clause :- Each DR spine switch will have 140 X 100G port (Total 2 X 140, 100G port).	ok Cabling need to be changes 150*2 to 140*2
121	financial Bid	168	In case a bidder quotes a solution of higher specifcations than sought specifications , bidder needs to ensure that all specifications / features / functionality/ relevant hardware/SFPs must be delivered , installed & commissioned. E.g instead of 24 port switch , a 48 port switch is quoted by a bidder, he needs to populate SFPs for 48 ports before offering the milestone for delivery	**Request Change :-** In case a bidder quotes a solution of higher specifcations than sought specifications , bidder needs to ensure that all specifications / features / functionality/ relevant hardware/SFPs asked in the tender must be delivered , installed & commissioned. E.g instead of 24 port switch , a 48 port switch is quoted by a bidder, he needs to populate SFPs for 24 ports before offering the milestone for delivery	This Clause Stands Deleted
122	TAC for 365*24*7	47	12) For minimizing the downtime & maintaining the overall resiliency, for the core equipments supplied at new DC-new DR (i.e. all type of Networking equipments , all types of firewalls, & PAM), the comprehensive warranty along with next business day warranty service is sought. The next business day warranty services shall ensure hardware replacements by the next day (within 24hrs) which is applicable 365x24x7 days per year.	We are looking for clarification is the support of 365x24x7 days is looking for TAC support or hardware replacement	Clause is self Explanatory

123	HLD and LLD	92	Contractor needs to provide an independent data center IT networking & architecture expert consultant at within 30 days from the date of issue of contract (available till end of DC-DR project commissioning) & will be responsible for: i. Designing (HLD, LLD) and implementing the data center networking, compute & other solutions . ii. Ensuring the sufficent scope while designing (including Racking Stacking, HLD, LLD etc.) to keep the solutions iii. Support in knowledge sharing, reviews of various related artifacts, Design of SoPs etc	What is independent consultant, Please clarify	Dedicated Subject Matter Expert on SI's Payroll with desired certification requirements as per Tender
124	General Activities to be performed by Contractor	97	12) The bid should include OEM professional services for the successful implementation of project. The OEM professional services shall include but not limited to solution architecture, design, installation, preparation of acceptance test plan & procedure with expected results and end user training leading to OEM Certification. **The above activities should be jointly done by the Contractor and the OEM, as per the best security practices for the final acceptance.**	What is meant by Jointly done by the Contractor, Please clarify is OEM professional services need to be quoted by Bidder or not	OEM Professional Services are required for best in class implementation of the project, however, it is overall responsibility of the System Integrator/Contractor to plan, co-ordinate/manage and complete the overall integration in time. OEM professional services cost need ensured by SI in the overall bid cost.
125		179	In DC and DR, all Networking equipment(s) should be from same OEM. Name of such equipment(s) are Spine & Leaf Switch, OOB Switch, Interconnect Type1 & Type 2 Switch, Border Leaf Switch, WAN Switch, CE Routers (WAN Router), Internet Router etc.	Please confirm same OEM products required for remote sites - remote switch, L3 access switch, OOB Access Switch and OOB Core Switch (DC & DR)	As per Tender Document
126	GPU Server	195	Four OSFP ports serving eight single- port NVIDIA ConnectX-7 VPI or 8* Single port with required Transceivers & Cables and two dual-port NVIDIA ConnectX-7 VPI or 2* Dual Port 100G with required Transceivers & Cables	Switch configuration for GPU servers are missing. Please confirm is switches for GPU need to be managed from Network Manager or not Also detailed specification of Network switches are not mentioned, we request you to please include specification of switches for GPU servers	As per Tender Document
127	SFP-10G (SR) for	202	Fibre Cable Type - MMF	Please clarity the distance support required	It is bidder's/OEM responsibility to select correct SFP which can run and support functions.
128	Spine Switch for	203	min. 250 or more without breakout. All the slots and ports should be fully populated with QSFP optics on day-1.	We request to make this changed to 220 in palce of 250	As per Tender Document
129	Spine Switch for	203	Virtual output Queue VoQ)/Egress QoS/Intelligent Buffer/dynamic buffer, WRED,ECN,LLQ,PTP, 8GB Packet Buffer per line card or equivalent, 802.1Qbb,8 queues/port, WRR	Please clarify what is menat by equivalent	Kindly refer revised Technical Specification
130	Spine Switch for	204	min. 140 or more without breakout. All the slots and ports should be fully populated with QSFP optics on day-1.	We request to make this changed to 120 in palce of 250	As per Tender Document
131	Spine Switch for	204	Port, VLAN & Routed ACL,802.1x,,12K ACL or higher Entries/group based-segmentation-entries, GRE (Must Support 1000 or Higher GRE Tunnels or 1000 VXLAN Tunnels)	We request to make ACL as 16K as per DC Spine Switch	Kindly refer revised Technical Specification
132	Leaf Switch	206	WRED, SPQ, SDWRR/WRR, , , 802.1Qbb PFC and ECN, 8queues/port, Remarking of bridged packets	What is the Packet Buffer Required for Leaf switch	As per Tender Document
133	Other	208	Switch should support all functions required to operate as a Border Leaf Switch providing DC Gateway, Service Chaining and Data centre Interconnect (DCI) using EVPN type-5 routes. Should support 300K IPv4 Routes,150K IPv6 Routes, 64K Multicast Route	We request to make 300K IPv4 Routes to 250K IPv4 Routes	As per Tender Document
134	Remote Site	214	Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sflow/netflow, OpenConfig, Filtered packet mirroring over GRE/SPAN	Please confirm is Same OS "Same OS across all the proposed network switches" required in "Remote Site Switch"	As per Tender Document
135	Interconnect Switch	215	d. WRED, SPQ, SDWRR/ WRR, , , 802.1Qbb, 8queues /port, Remarking of bridged packet, PFC, ECN	What is the Packet Buffer Required for Interconnect Switch - Type 1	As per Tender Document

136	Interconnect Switch	217	WRED, SPQ, SDWRR/ WRR, , , 802.1Qbb ,802.1Qaz, 8queues /port, Remarking of bridged packets, PFC, ECN	What is the Packet Buffer Required for Interconnect Switch - Type 2	As per Tender Document
137	WAN	218	WRED, SPQ, SDWRR / WRR, , , 8queues /port, PFC, ECN	What is the Packet Buffer Required for WAN Switch	As per Tender Document
138	Layer-3 Access	220	802.1p, SP, Queues per port, WRED /WTD, Sflow/Netflow, Shaping, Policing/Rate Limiting, Strict Priority Queueing or Low Latency Queueing.	Please confirm PFC & ECN is required in Layer-3 Access Switch, as these are asked in all other switches but missing in Layer-3 Access Switch. So Request to please add the same	As per Tender Document
139	CE Router	221	The Router should be populated with redundant Routing Card/Engines/control plane/supervisor engine/multi-core x86 CPU	Request to please remove "redundant", so that Arista can also qualify and be competitive in the Tender	The Router should be populated with Routing Card/Engines/control plane/supervisor engine/multi-core x86 CPU
140	SFPTransceiver-10GBase-SR (For Networking	228	Fibre Cable Type - MMF	Please clarity the distance support required	It is bidder's/OEM responsibility to select correct SFP which can run and support functions.
141	QSFP+28 Transceiver-100 GBase-SR4 (For Networking	228	Fibre Cable Type - MMF	Please clarity the distance support required	It is bidder's/OEM responsibility to select correct SFP which can run and support functions.
142	SFP Transceiver - 10GBase-LR (For Networking	229	Fibre Cable Type - SMF	Please clarity the distance support required	It is bidder's/OEM responsibility to select correct SFP which can run and support functions.
143	QSFP+28 Transceiver-100GBase-LR4 (For Networking	229	Fibre Cable Type - SMF	Please clarity the distance support required	It is bidder's/OEM responsibility to select correct SFP which can run and support functions.
144	Network Manager in	230	Solution to be provided for unified management and monitoring of all the proposed network switches of DC and DR that are part of the RFP.	Please clarity is the Network Manager need to manage all Networking switches in a single dashboard as mentioned in this RFP or not or multiple dashboards are accepted or not	As per Tender Document
145		47	12) For minimizing the downtime & maintaining the overall resiliency, for the core equipments supplied at new DC-new DR (i.e. all type of Networking equipments , all types of firewalls, & PAM), the comprehensive warranty along with next business day warranty service is sought. The next business day warranty services shall ensure hardware replacements by the **next day (within 24hrs)** which is applicable 365x24x7 days per year.	"Next business day" is a standard practice across OEMs and is considered 5 days a week when it is about hardware replacement, while the TAC support is commonly provided 365x24x7. It is therefore requested to modify the clause as mentioned below to remove the ambiguity: "12) For minimizing the downtime & maintaining the overall resiliency, for the core equipments supplied at new DC-new DR (i.e. all type of Networking equipments , all types of firewalls, & PAM), the comprehensive warranty along with next business day warranty service is sought. The next business day warranty services shall ensure hardware replacements by the **next business day with TAC availability of** 365x24x7 days per year."	Clause is self Explanatory
146	Training	99	Training for 20 Persons (in batches) shall be provided onsite by the OEM experts/OEM representatives for equipment of respective OEMs for installation and operations of installed equipment(s) per equipment supplied	Given the criticality of the project and OEM professional services being sought for Plan, Design and Implementation across product lines it is imperative that the training should also be done by OEM experts rather than risking the project with 3rd party trainers. Hence we request to modify the clause as : "Training for 20 Persons (in batches) shall be provided onsite by the OEM experts for equipment of respective OEMs for installation and operations of installed equipment(s) per equipment supplied"	As per Tender Document

147		179	In DC and DR, all Networking equipment(s) should be from same OEM. Name of such equipment(s) are Spine & Leaf Switch, OOB Switch, Interconnect Type1 & Type 2 Switch, Border Leaf Switch, WAN Switch, CE Routers (WAN Router), Internet Router etc.	Considering the specs of all the network switches and routers: It is suggested to modify the clause as suggested below to avoid ambiguity: In DC, DR **and remote sites**, all proposed Networking equipment(s) should be from same OEM. Name of such equipment(s) are Spine & Leaf switch, **OOB core, OOB access, L3 access, remote site switch,** Interconnect Type1 & Type 2 Switch, Border Leaf Switch, WAN Switch, CE Routers (WAN Router), Internet Router etc.	No Change. However OOB Switch means OOB Core and OOB Access Switch only.
148	SFP	228	Fibre Cable Type - MMF	Given that the SFP-10G-SR optics would primarily be used for Server to leaf switch connectivity and intra DC connectivity requirements we would recommend changing this clause to : "Fibre Cable Type - MMF with minimum 100 meters distance support"	It is bidder's/OEM responsibility to select correct SFP which can run and support functions.
149	SFP	228	Fibre Cable Type - MMF	Given that the 100GSR4 optics would primarily be used for leaf to spine connectivity and other intra DC connectivity requirements we would recommend changing this clause to : "Fibre Cable Type - MMF with minimum 100 meters distance support"	It is bidder's/OEM responsibility to select correct SFP which can run and support functions.
150	SFP	229	Fibre Cable Type - SMF	Given that the 10GBase-LR optics would primarily be used for intra DC OR to mux locations withing the vicinity of the data centers we would recommend changing this clause to : "Fibre Cable Type - SMF with minimum 1 KM distance support"	It is bidder's/OEM responsibility to select correct SFP which can run and support functions.
151	SFP	229	Fibre Cable Type - SMF	Given that the 100GBase-LR4 optics would primarily be used for intra DC OR to mux locations withing the vicinity of the data centers we would recommend changing this clause to : "Fibre Cable Type - SMF with minimum 1 KM distance support"	It is bidder's/OEM responsibility to select correct SFP which can run and support functions.
152	GPU Server	195	Four OSFP ports serving eight single- port NVIDIA ConnectX-7 VPI or 8* Single port with required Transceivers & Cables and two dual-port NVIDIA ConnectX-7 VPI or 2* Dual Port 100G with required Transceivers & Cables	Switch configuration for GPU servers are missing. Please confirm is switches for GPU need to be managed from Network Manager or not Also detailed specification of Network switches are not mentioned, we request you to please include specification of switches for GPU servers	As per Tender Document
153	Spine Switch for DC	202	6. Support for 100G QSFP28 Port- Yes	Please modify this clause as below to ensure versatility of use cases in the long duration of the project : "Support for 1G,10G,25G,40G,100G : Yes"	As per Tender Document
154	Spine Switch for DC	203	7. Number of 100G QSFP28 Port- min. 250 or more without breakout. All the slots and ports should be fully populated with QSFP optics on day-1.	Please clarify if the optics are over and above the quantity mentioned in the BOQ. If not please mention the type of optics to be provided.	As per Tender Document
155	Spine Switch for DC	203	7. Number of 100G QSFP28 Port- min. 250 or more without breakout. All the slots and ports should be fully populated with QSFP optics on day-1.	We request you to modify this clause as below to align with the number of leaf switches asked in DC : "**min. 220** or more without breakout. All the slots and ports should be fully populated with QSFP optics on day-1."	As per Tender Document
156	Spine Switch for DC	203	10 b. Security Feature- Port, VLAN & Routed ACL,802.1x,16K or higher ACL Entries/group based-segmentation- entries, GRE (Must Support 1000 or Higher GRE Tunnels or 1000 VXLAN Tunnels)	It is understood that 16K entries can be achieved through any of the two mentioned mechanisms. i.e. 1) ACL entries 2) group-based segmentation entries. Requesting to confirm if the understanding is correct.	As per Tender Document

157	Spine Switch for DC	203	11 c. Management Protocol- Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sFlow/Netflow, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN, data plane telemetry, buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations.	It is understood that the OS should be same across all the proposed network switch **categories**, and not just the switches belonging to single category. Requesting to confirm the understanding.	As per Tender Document
158	Spine Switch for DC	203	11 c. Management Protocol- Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sFlow/Netflow, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN, data plane telemetry, buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations.	SPAN is a local port mirroring mechanism and is not equivalent to mirror over GRE which is layer-3 remote port mirroring mechanism. ERSPAN is a similar mechanism to mirror over GRE. Therefore requesting to modify the clause as " "Capable to support Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sFlow/Netflow, PTP, OpenConfig, Filtered packet mirroring over GRE/**ERSPAN**, data plane telemetry, buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations."	Kindly refer revised Technical Specification
159	Spine Switch for DC	203	12 d. QoS Virtual output Queue VoQ)/Egress QoS/Intelligent Buffer/dynamic buffer, WRED,ECN,LLQ,PTP, 8GB Packet Buffer per line card or equivalent, 802.1Qbb,8 queues/port, WRR	at avoid ambiguity please modify "8GB Packet Buffer per line card or equivalent" to "8GB packet Buffer per line card".	Kindly refer revised Technical Specification
160	Spine Switch for DR	204	6. Support for 100G QSFP28 Port- Yes	Please modify this clause as below to ensure versatility of use cases in the long duration of the project : "Support for 1G,10G,25G,40G,100G : Yes"	As per Tender Document
161	Spine Switch for DR	204	7. Number of 100G QSFP28 Port- min. 140 or more without breakout. All the slots and ports should be fully populated with QSFP optics on day-1.	We request you to modify this clause as below to align with the number of leaf switches asked in DR : "**min. 125** or more without breakout. All the slots and ports should be fully populated with QSFP optics on day-1."	As per Tender Document
162	Spine Switch for DR	204	7. Number of 100G QSFP28 Port min. 140 or more without breakout. All the slots and ports should be fully populated with QSFP optics on day-1.	Please clarify if the optics are over and above the quantity mentioned in the BOQ. If not please mention the type of optics to be provided.	As per Tender Document
163	Spine Switch for DR	204	10 b. Security Feature Port, VLAN & Routed ACL,802.1x,,12K ACL or higher Entries/group based-segmentation- entries, GRE (Must Support 1000 or Higher GRE Tunnels or 1000 VXLAN Tunnels)	It is understood that 16K entries can be achieved through any of the two mentioned mechanisms. i.e. 1) ACL entries 2) group-based segmentation entries. Requesting to confirm if the understanding is correct.	As per Tender Document
164	Spine Switch for DR	204	11 c. Management Protocol- Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sFlow/Netflow, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN, data plane telemetry, buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations.	It is understood that the OS should be same across all the proposed network switch **categories**, and not just the switches belonging to single category. Requesting to confirm the understanding.	As per Tender Document
165	Spine Switch for DR	204	11 c. Management Protocol- Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sFlow/Netflow, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN, data plane telemetry, buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations.	SPAN is a local port mirroring mechanism and is not equivalent to mirror over GRE which is layer-3 remote port mirroring mechanism. ERSPAN is a similar mechanism to mirror over GRE. Therefore requesting to modify the clause as " "Capable to support Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sFlow/Netflow, PTP, OpenConfig, Filtered packet mirroring over GRE/**ERSPAN**, data plane telemetry, buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations."	Kindly refer revised Technical Specification

166	Spine Switch for DR	204	12 d. QoS- Virtual output Queue VoQ)/Egress QoS/Intelligent Buffer/dynamic buffer, WRED,ECN,LLQ,PTP, 8GB Buffer per line card or equivalent, 802.1Qbb,8 queues/port, WRR	at avoid ambiguity please modify "8GB Buffer per line card or equivalent" to "8GB packet Buffer per line card".	Kindly refer revised Technical Specification
167	Leaf Switch	206	8 c. Management Protocol- Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN, data plane telemetry to trace path and per hop latency for a flow , buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations.	It is understood that the OS should be same across all the proposed network switch **categories**, and not just the switches belonging to single category. Requesting to confirm the understanding.	As per Tender Document
168	Leaf Switch	206	8 c. Management Protocol- Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN, data plane telemetry to trace path and per hop latency for a flow , buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations.	SPAN is a local port mirroring mechanism and is not equivalent to mirror over GRE which is layer-3 remote port mirroring mechanism. ERSPAN is a similar mechanism to mirror over GRE. Therefore requesting to modify the clause as " "Capable to support Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX, PTP, OpenConfig, Filtered packet mirroring over GRE**/ERSPAN**, data plane telemetry to trace path and per hop latency for a flow , buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations."	Kindly refer revised Technical Specification
169	Leaf Switch	206	9 d. QoS- WRED, SPQ, SDWRR/WRR, , , 802.1Qbb PFC and ECN, 8queues/port, Remarking of bridged packets	Packet buffer is one of the important performance criteria. It is therefore requested to mention the buffer as 2Gb to ensure optimal performance for critical applications. We would request you to modify the clause as : "WRED, SPQ, SDWRR/WRR, 802.1Qbb PFC and ECN, 8queues/port, Remarking of bridged packets, 2GB of VoQ buffer"	As per Tender Document
170	Border Leaf Switch	208	7. c. Management Protocol- Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX, PTP, OpenConfig, Filtered packet mirroring over GRE/span, data plane telemetry to trace path and per hop latency for a flow , buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations.	It is understood that the OS should be same across all the proposed network switch **categories**, and not just the switches belonging to single category. Requesting to confirm the understanding.	As per Tender Document
171	Border Leaf Switch	208	7. c. Management Protocol- Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX, PTP, OpenConfig, Filtered packet mirroring over GRE/span, data plane telemetry to trace path and per hop latency for a flow , buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations.	SPAN is a local port mirroring mechanism and is not equivalent to mirror over GRE which is layer-3 remote port mirroring mechanism. ERSPAN is a similar mechanism to mirror over GRE. Therefore requesting to modify the clause as " "Capable to support Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX, PTP, OpenConfig, Filtered packet mirroring over GRE**/ERSPAN**, data plane telemetry to trace path and per hop latency for a flow , buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations."	As per Tender Document
172	Border Leaf Switch	208	9. Other features- Switch should support all functions required to operate as a Border Leaf Switch providing DC Gateway, Service Chaining and Data centre Interconnect (DCI) using EVPN type-5 routes. Should support 300K IPv4 Routes,150K IPv6 Routes, 64K Multicast Route	We would request you to kindly relax this clause as to align with overall route scale requirements in the Data center : "Switch should support all functions required to operate as a Border Leaf Switch providing DC Gateway, Service Chaining and Data centre Interconnect (DCI) using EVPN type-5 routes. Should support 250K IPv4 Routes,150K IPv6 Routes, 64K Multicast Route"	Switch should support all functions required to operate as a Border Leaf Switch providing DC Gateway, Service Chaining and Data centre Interconnect (DCI) using EVPN type-5 routes. Should support 250K IPv4 Routes,150K IPv6 Routes, 64K Multicast Route
173	OOB Core Switch for DC	209	3. No of 10G SFP/SFP+ Ports- Minimum 110 Nos (Without breakout or Stacking). Fully Populated from Day-1	Please clarify if the optics are over and above the quantity mentioned in the BOQ. If not please mention the type of optics to be provided.	As per Tender Document

174	OOB Core Switch for DC	209	6.No .of 100G QSFP+ Port 12 or higher ; Fully Populated from Day-1	Please clarify if the optics are over and above the quantity mentioned in the BOQ. If not please mention the type of optics to be provided.	As per Tender Document
175	OOB Core Switch for DC	209	10 c. Management Protocol Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/Netflow/sFlow, OpenConfig, Filtered packet mirroring over GRE/SPAN/GRE Encapsulation, Same OS across all the proposed network switches for simplified operations.	It is understood that the OS should be same across all the proposed network switch **categories**, and not just the switches belonging to single category. Requesting to confirm the understanding.	As per Tender Document
176	OOB Core Switch for DC	209	10 c. Management Protocol- Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/Netflow/sFlow, OpenConfig, Filtered packet mirroring over GRE/SPAN/GRE Encapsulation, Same OS across all the proposed network switches for simplified operations.	SPAN is a local port mirroring mechanism and is not equivalent to mirror over GRE which is layer-3 remote port mirroring mechanism. ERSPAN is a similar mechanism to mirror over GRE. Therefore requesting to modify the clause as "Capable to support Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/Netflow/sFlow, OpenConfig, Filtered packet mirroring over GRE/ERSPAN, Same OS across all the proposed network switches for simplified operations."	As per Tender Document
177	OOB Core Switch for DR	210	3. No of 10G SFP/SFP+Ports- Minimum 60 Nos (Without breakout or Stacking); Fully Populated from Day-1	Please clarify if the optics are over and above the quantity mentioned in the BOQ. If not please mention the type of optics to be provided.	As per Tender Document
178	OOB Core Switch for DR	211	6. No .of 100G QSFP+ Port 8 or higher ; Fully Populated from Day-1	Please clarify if the optics are over and above the quantity mentioned in the BOQ. If not please mention the type of optics to be provided.	As per Tender Document
179	OOB Core Switch for DR	211	10. c. Management Protocol- Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/Netflow/sFlow, OpenConfig, Filtered packet mirroring over GRE/Span, Same OS across all the proposed network switches for simplified operations.	It is understood that the OS should be same across all the proposed network switch **categories**, and not just the switches belonging to single category. Requesting to confirm the understanding.	As per Tender Document
180	OOB Core Switch for DR	211	10 c. Management Protocol- Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/Netflow/sFlow, OpenConfig, Filtered packet mirroring over GRE/Span, Same OS across all the proposed network switches for simplified operations.	SPAN is a local port mirroring mechanism and is not equivalent to mirror over GRE which is layer-3 remote port mirroring mechanism. ERSPAN is a similar mechanism to mirror over GRE. Therefore requesting to modify the clause as "Capable to support Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/Netflow/sFlow, OpenConfig, Filtered packet mirroring over GRE/ERSPAN, Same OS across all the proposed network switches for simplified operations."	As per Tender Document
181	OOB Access Switch	212	3. Number of 10G SFP+ Port(Uplink)- 2 or higher Fully Populated from Day-1	Please clarify if the optics are over and above the quantity mentioned in the BOQ. If not please mention the type of optics to be provided.	As per Tender Document
182	OOB Access Switch	212	11 Management Protocol GUI/Web, CLI, Telnet, TFTP, SMPv1, SNMPv2/V2C, SNMPv3, NTP, RMON, SSHv2, IP Based Management, IPFIX/Netflow/sFlow, OpenConfig, filtered packet mirroring over GRE/SPAN, Same OS across all the proposed network switches for simplified operations.	It is understood that the OS should be same across all the proposed network switch **categories**, and not just the switches belonging to single category. Requesting to confirm the understanding.	As per Tender Document
183	OOB Access Switch	212	11 Management Protocol GUI/Web, CLI, Telnet, TFTP, SMPv1, SNMPv2/V2C, SNMPv3, NTP, RMON, SSHv2, IP Based Management, IPFIX/Netflow/sFlow, OpenConfig, filtered packet mirroring over GRE/SPAN, Same OS across all the proposed network switches for simplified operations.	SPAN is a local port mirroring mechanism and is not equivalent to mirror over GRE which is layer-3 remote port mirroring mechanism. ERSPAN is a similar mechanism to mirror over GRE. Therefore requesting to modify the clause as "Capable to support GUI/Web, CLI, Telnet, TFTP, SMPv1, SNMPv2/V2C, SNMPv3, NTP, RMON, SSHv2, IP Based Management, IPFIX/Netflow/sFlow, OpenConfig, filtered packet mirroring over GRE/ERSPAN, Same OS across all the proposed network switches for simplified operations."	As per Tender Document

184	Remote Site Switch	214	3. No of 1G/10G SFP/SFP+Ports- 12 Nos (Without breakout or Stacking); Fully Populated from Day-1	Please clarify if the optics are over and above the quantity mentioned in the BOQ. If not please mention the type of optics to be provided.	As per Tender Document
185	Remote Site Switch	214	6. No of 25G SFP Ports- 4 Nos (Without breakout or Stacking); Fully Populated from Day-1	Please clarify if the optics are over and above the quantity mentioned in the BOQ. If not please mention the type of optics to be provided.	As per Tender Document
186	Remote Site Switch	214	10 c. Management Protocol- Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sflow/netflow, OpenConfig, Filtered packet mirroring over GRE/SPAN	SPAN is a local port mirroring mechanism and is not equivalent to mirror over GRE which is layer-3 remote port mirroring mechanism. ERSPAN is a similar mechanism to mirror over GRE. Therefore requesting to modify "Filtered packet mirroring over GRE/SPAN" as "Filtered packet mirroring over GRE/ERSPAN" Please modify this clause as "Capable to support Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sflow/netflow, OpenConfig, Filtered packet mirroring over GRE/ERSPAN"	Kindly refer revised Technical Specification
187	Remote Site Switch	214	10 c. Management Protocol- Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sflow/netflow, OpenConfig, Filtered packet mirroring over GRE/SPAN	As the switch will be managed through centralised Manager, it is suggested that same OS is considered for this switch also for simplified operations. The clause is suggested to be augmented with " Same OS across all the proposed network switches categories for simplified operations."	Kindly refer revised Technical Specification
188	Interconnect Switch	215	3. No. of Ports- Should have minimum 8 Nos of 10G and 8 Nos of 100G QSFP28 Ports; Fully Populated from Day-1	Please clarify if the optics are over and above the quantity mentioned in the BOQ. If not please mention the type of optics to be provided.	As per Tender Document
189	Interconnect Switch	215	7. c. Management Protocol- Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, NTP, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sflow/netflow, OpenConfig, Filtered packet mirroring over GRE/SPAN, data plane telemetry to trace path and per hop latency for a flow, buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations.	It is understood that the OS should be same across all the proposed network switch **categories**, and not just the switches belonging to single category. Requesting to confirm the understanding.	As per Tender Document
190	Interconnect Switch	215	7. c. Management Protocol Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, NTP, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sflow/netflow, OpenConfig, Filtered packet mirroring over GRE/SPAN, data plane telemetry to trace path and per hop latency for a flow, buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations.	SPAN is a local port mirroring mechanism and is not equivalent to mirror over GRE which is layer-3 remote port mirroring mechanism. ERSPAN is a similar mechanism to mirror over GRE. Therefore requesting to modify "Filtered packet mirroring over GRE/SPAN" as "Filtered packet mirroring over GRE/ERSPAN" ; Kindly modify this clause as : "c. Capable to support Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, NTP, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sflow/netflow, OpenConfig, Filtered packet mirroring over GRE/**ERSPAN**, data plane telemetry to trace path and per hop latency for a flow, buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations."	Kindly refer revised Technical Specification
191	Interconnect Switch	215	8. d. QoS- WRED, SPQ, SDWRR/ WRR, , , 802.1Qbb, 8queues /port, Remarking of bridged packet, PFC, ECN	Is understood that interconnect switches will play a critical role in serving north south traffic over varying link speeds (10G and 100G). A packet drop at such network points will have much higher impact on the application performance. It is therefore requested to consider 2GB of packet buffer on this device to avoid network performance issues. Kindly modify this clause as : "d. WRED, SPQ, SDWRR/ WRR, 802.1Qbb, 8queues /port, Remarking of bridged packet, PFC, ECN , **2Gb of packet buffer**"	As per Tender Document

192	Interconnect Switch	216	3. No. of Ports- Should have minimum 16 Nos of 10G and 8 Nos 100G QSFP28 Ports; Fully Populated from Day-1	Please clarify if the optics are over and above the quantity mentioned in the BOQ. If not please mention the type of optics to be provided.	As per Tender Document
193	Interconnect Switch	217	7. c. Management Protocol- Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, NTP, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sflow/netflow, OpenConfig, Filtered packet mirroring over GRE/SPAN, data plane telemetry to trace path and per hop latency for a flow, buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations.	It is understood that the OS should be same across all the proposed network switch **categories**, and not just the switches belonging to single category. Requesting to confirm the understanding.	As per Tender Document
194	Interconnect Switch	217	7 c. Management Protocol- Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, NTP, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sflow/netflow, OpenConfig, Filtered packet mirroring over GRE/SPAN, data plane telemetry to trace path and per hop latency for a flow, buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations.	SPAN is a local port mirroring mechanism and is not equivalent to mirror over GRE which is layer-3 remote port mirroring mechanism. ERSPAN is a similar mechanism to mirror over GRE. Therefore requesting to modify "Filtered packet mirroring over GRE/SPAN" as "Filtered packet mirroring over GRE/ERSPAN" ; Kindly modify this clause as : "c. Capable to support Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, NTP, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sflow/netflow, OpenConfig, Filtered packet mirroring over GRE/**ERSPAN**, data plane telemetry to trace path and per hop latency for a flow, buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations."	Kindly refer revised Technical Specification
195	Interconnect Switch	217	8 d. QoS- WRED, SPQ, SDWRR/ WRR, , , 802.1Qbb ,802.1Qaz, 8queues /port, Remarking of bridged packets, PFC, ECN	Is understood that interconnect switches will play a critical role in serving north south traffic over varying link speeds (10G and 100G). A packet drop at such network points will have much higher impact on the application performance. It is therefore requested to consider 2GB of packet buffer on this device to avoid network performance issues. Kindly modify this clause as : "d. WRED, SPQ, SDWRR/ WRR, 802.1Qbb, 8queues /port, Remarking of bridged packet, PFC, ECN , **2Gb of packet buffer**"	As per Tender Document
196	WAN Switch	218	4 No. of Slots- Should be populated with 4x1GBase-LX, 4x1000 Base-T,4x10G Base- LR and 4 x 10GBase- SR transceivers. Also should have minimum 8 Nos of 100G QSFP28 Ports and populated with 8 x100G Transceivers (LR/SR will be decided as per TSP MUX); Fully Populated from Day-1	Please clarify if the optics are over and above the quantity mentioned in the BOQ.	As per Tender Document
197	WAN Switch	218	8. c. Management Protocol- Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sflow/netflow, OpenConfig, Filtered packet mirroring over GRE/span, data plane telemetry to trace path and per hop latency for a flow , buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations.	It is understood that the OS should be same across all the proposed network switch **categories**, and not just the switches belonging to single category. Requesting to confirm the understanding.	As per Tender Document
198	WAN Switch	218	8. c. Management Protocol- Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sflow/netflow, OpenConfig, Filtered packet mirroring over GRE/span, data plane telemetry to trace path and per hop latency for a flow , buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations.	SPAN is a local port mirroring mechanism and is not equivalent to mirror over GRE which is layer-3 remote port mirroring mechanism. ERSPAN is a similar mechanism to mirror over GRE. Therefore requesting to modify "Filtered packet mirroring over GRE/SPAN" as "Filtered packet mirroring over GRE/ERSPAN" ; Kindly modify this clause as : "Capable to support Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sflow/netflow, OpenConfig, Filtered packet mirroring over GRE**/ERSPAN**, data plane telemetry to trace path and per hop latency for a flow , buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations."	As per Tender Document

199	WAN Switch	218	9. d. QoS- WRED, SPQ, SDWRR / WRR, 8queues /port, PFC, ECN	Is understood that interconnect switches will play a critical role in serving north south traffic over varying link speeds (10G and 100G). A packet drop at such network points will have much higher impact on the application performance. It is therefore requested to consider 2GB of packet buffer on this device to avoid network performance issues. Kindly modify the clause as : "WRED, SPQ, SDWRR / WRR, 8queues /port, PFC, ECN, **2Gb of Packet Buffer**"	As per Tender Document
200	Layer-3 Access Switch	220	12 Management Protocol- GUI/Web, CLI, Telnet, TFTP, SMPv1, SNMPv2/V2C, SNMPv3, NTP, RMON, SSHv2, IP Based Management, IPFIX/Sflow/Netflow, OpenConfig, filtered packet mirroring over GRE/span, Same OS across all the proposed network switches for simplified operations.	It is understood that the OS should be same across all the proposed network switch **categories**, and not just the switches belonging to single category. Requesting to confirm the understanding.	As per Tender Document
201	Layer-3 Access Switch	220	12 Management Protocol- GUI/Web, CLI, Telnet, TFTP, SMPv1, SNMPv2/V2C, SNMPv3, NTP, RMON, SSHv2, IP Based Management, IPFIX/Sflow/Netflow, OpenConfig, filtered packet mirroring over GRE/span, Same OS across all the proposed network switches for simplified operations.	SPAN is a local port mirroring mechanism and is not equivalent to mirror over GRE which is layer-3 remote port mirroring mechanism. ERSPAN is a similar mechanism to mirror over GRE. Therefore requesting to modify "Filtered packet mirroring over GRE/SPAN" as "Filtered packet mirroring over GRE/ERSPAN" ; Kindly modify this clause as : "Capable to support GUI/Web, CLI, Telnet, TFTP, SMPv1, SNMPv2/V2C, SNMPv3, NTP, RMON, SSHv2, IP Based Management, IPFIX/Sflow/Netflow, OpenConfig, filtered packet mirroring over GRE**/ERSPAN**, Same OS across all the proposed network switches for simplified operations."	GRE/SPAN/ERSPAN Agreed. Add ERSPAN at all places in networking equipment
202	Layer-3 Access Switch	220	13 QoS- 802.1p, SP, Queues per port, WRED /WTD, Sflow/Netflow, Shaping, Policing/Rate Limiting, Strict Priority Queueing or Low Latency Queueing.	Please confirm PFC & ECN is required in Layer-3 Access Switch, as these are asked in all other switches but missing in Layer-3 Access Switch. So Request to please add the same. Kindly modify this clause as : "802.1p, SP, Queues per port, WRED /WTD, Sflow/Netflow, Shaping, Policing/Rate Limiting, Strict Priority Queueing or Low Latency Queueing, **PFC , ECN** "	As per Tender Document
203	CE Router	221	3 Routing Engine- The Router should be populated with redundant Routing Card/Engines/control plane /supervisor engine/multi-core x86 CPU	As the routers will be deployed in redundant fashion only, requesting to remove "redundant" from the clause to qualify a "non-chassis based" devices which will be much more cost effective while also consuming much lower rack space and power. Kindy modify this clause as : "The Router should be populated with Routing Card/Engines/control plane/supervisor engine/multi-core x86 CPU"	The Router should be populated with Routing Card/Engines/control plane/supervisor engine/multi-core x86 CPU
204	Internet Router	223	3 Port population- Should be supplied on day 1 with 4 x 1000Base-LX Single Mode SFP transceivers, 4 x 10/100/1000Base-T Interface Ports and 4 x 10G Base SR Transceivers. Should be scalable to support additional 4 X 40/100G QSFP ports; Fully Populated from Day-1	10Mb is not used these days and the minimum bandwidth available from SPs is also 100Mb ; would request you modify this clause as : "Should be supplied on day 1 with 4 x 1000Base-LX Single Mode SFP transceivers, 4 x 100/1000Base-T Interface Ports and 4 x 10G Base SR Transceivers. Should be scalable to support additional 4 X 40/100G QSFP ports; Fully Populated from Day-1"	Kindly refer revised Technical Specification
205	Network Manager	230	1. Solution to be provided for unified management and monitoring of all the proposed network switches of DC and DR that are part of the RFP.	As network manager is asked for "Remote Site Switch" from the same OEM, it is requested to also include remote sites also in the clause as suggested below to avoid ambiguity. Please clarity is the Network Manager need to manage all Networking switches in a single dashboard as mentioned in this RFP or not or multiple dashboards are accepted or not "Solution to be provided for unified management **from a single pane of glass** and monitoring of all the proposed network switches of **DC, DR and remote sites** that are part of the RFP."	As per Tender Document

206	Network Manager	230	3. The solution should provide UI-driven wizard based approach to simplify and accelerate deployment of EVPN overlay fabric by automatically generating the resultant CLI configurations and pushing it to the **Data Center** network Switches.	Kindly modify this clause as : "The solution should provide UI-driven wizard based approach to simplify and accelerate deployment of EVPN overlay fabric by automatically generating the resultant CLI configurations and pushing it to the **all proposed network Switches.**"	As per Tender Document
207	Network Manager	230	5 Image upgradation and patch management of the managed network devices should be supported Centrally.	Kindly modify this clause as : "Image upgradation and patch management of the proposed network switches should be supported Centrally."	Kindly refer revised Technical Specification
208	Network Manager	230	8 The Manager should gather streaming telemetry (that is not SNMP and flow data based) in realtime from all the managed devices.	Kindly modify this clause as : "The Manager should gather streaming telemetry (that is not SNMP and flow data based) in realtime from all the **proposed network switches**."	Kindly refer revised Technical Specification
209	Network Manager	230	9 Should provide ability to view Telemetry data over a timeline. The Data Should be available for at least 60 days.	Kindly modify this clause as : "Should provide ability to view Telemetry data over a timeline. The telemetry Data Should be available for at least 60 days. Should provide capability to compare two points in time and visualize the difference"	Kindly refer revised Technical Specification
210	Network Manager	231	13 Should be able to show deviation from user defined config/policy and Switch image as part of the compliance.	Kindly modify this clause as: "Should be able to show deviation from user defined config/policy and Switch image as part of the compliance. Should provide notifications on exposure to known software bugs and CVEs "	Kindly refer revised Technical Specification
211	Network Manager	231	16 Should support ML for dynamic baselining/proactive alerting/suggestion.	Kindly modify this clause as "Should support ML for dynamic baselining/proactive alerting/suggestion. **Solution should support Email capability**"	Kindly refer revised Technical Specification
212	Network Manager	231	24 Bidder shall provide required server Hardware & Software to run the solution in HA within a site and to support HA across sites. Failure of all server hardware should not impact packet forwarding on the network devices.	Kindly modify this clause as : "Bidder shall provide required server Hardware & Software to run the solution in HA within a site and to support HA across sites. Failure of all server hardware should not impact packet forwarding on the network devices. Solution should be capable to support minimum 700 switches from a single dashboard"	Kindly refer revised Technical Specification
213	Storage Server	181	Processor: 2 Quantity (Dual socket) x Intel Xeon Gold/Platinum scalable series 5th Gen, 32+ cores/64+ Threads (2.7+ GHz base frequency, Cache Size 60+ MB) or Processor: 2 Quantity (Dual socket) x AMD Epyc 9004 or latest Series, 32+ cores/64+ Threads (2.7+ GHz base frequency, Cache Size 128+ MB)	As per our design, we support 60 or above internal HDDs within the 4U storage server chassis. Hence to manage the heat dissipation coming from CPU, memory and HDDs becomes very challenging. **For the reasons mentioned above, we request to change the processor to 32 Cores / 2.1 GHz base frequency.**	As per Tender Document
214	Storage Server	181	Total 2TB or higher RAM, DDR5 5000+ MHz ECC REG DIMM	As per our design, we support 60 or above internal HDDs within the 4U storage server chassis. Hence to manage the heat dissipation coming from CPU, memory and HDDs becomes very challenging. **For the reasons mentioned above, we request to change the Memory from 2TB to 1.5TB.**	As per Tender Document
215	Storage Server	181	Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS SSD/M.2 NVME SSD Each SSD spec: 960GB+ Capacity, Write Intensive, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size	Latest generation servers are coming with E3.S NVMe SSDs in compact factor. Also, we recommend to remove the write intensive SSDs as the mentioned performance parameteres can be achieved using read intensive SSDs.also. Hence, request to change the clause as "Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS SSD/M.2 NVME SSD/**E3.S NVMe SSDs** Each SSD spec: 960GB+ Capacity, **Read Intensive**, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours,2000+ TBW, **1 DWPD** IOPS: Each SSD should have 150K+/75K+ Random Read/Write IOPS at 4K block size" for wider participation.	Add E3.S NVMe SSDs , Replace Write Intensive with Write Intensive/Mixed use Allowed E3.S NVMe SSDs , Write Intensive/Mixed use in boot storage of all servers .

216	Storage Server	182	Each Server With Minimum Storage of 1440 TB, With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s Note: 1. Single DAS expansion can be used. However, the effective I/O throughput of all the disks combined should not be impacted due to any DAS expansion connector limitations. 2. DAS and Server should be compatible and support of DAS to be provided by Server OEM only. Server OEM shall give undertaking for the support of DAS on their letterhead.	We wish to highlight that we use Encryption using controller on HDDs with ISE(Instant Sanitise Erase) in HPE systems which is better in security as compared to SED. Citing the reasons mentioned above, we request you to make the below changes: "Each Server With Minimum Storage of 1440 TB, With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive)**/Encryption using controller along with ISE(Instant Sanitise Erase)** Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s" for wider participation. *Additioanlly, we also request you to consider the Storage Systems with internal HDD ONLY becasue the connectivity to external DAS using cables will create* ***additional point of failure.*** *This will severely impact the availability/reliability/performance of the solution.* *Also, storage servers with internal HDDs are* ***30-40% efficient*** *in terms of rack space and power.*	As per Tender Document
217	Storage Server	182	Dedicated Hardware Raid controller= RAID 0,1,5,6,10, 50, 60, SATA/SAS-3 connectivity, 4+ GB cache, battery or flash backed protection for all HDDs.	We request you to kindly change the clause asDedicated Hardware Raid controller= RAID 0,1,5,10 SATA/SAS-3 connectivity,**No** cache.	As per Tender Document
218	Load Balancer Server	188	Power Supply Efficiency: Titanium or higher.	Power Supply Efficiency: **Platinum/titanium** or Higher , Every OEM has different offerring in terms of power supplies , request to kindly ammend the clause to ensure maximum participation.	Platinum/titanium or Higher
219	Web Server	186	Power Supply Efficiency: Titanium or higher.	Power Supply Efficiency: **Platinum/titanium** or Higher , Every OEM has different offerring in terms of power supplies , request to kindly ammend the clause to ensure maximum participation.	Platinum/titanium or Higher
220	Application Server	184	Power Supply Efficiency: Titanium or higher.	Power Supply Efficiency: **Platinum/titanium** or Higher , Every OEM has different offerring in terms of power supplies , request to kindly ammend the clause to ensure maximum participation.	Platinum/titanium or Higher
221	Storage Server	183	Power Supply Efficiency: Titanium or higher.	Power Supply Efficiency: **Platinum/titanium** or Higher , Every OEM has different offerring in terms of power supplies , request to kindly ammend the clause to ensure maximum participation.	Platinum/titanium or Higher. Replace in all servers
222	Storage Server	182/183	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe Sequential read 6,200 MB/s, Sequential write 2,600 MB/s (Sequential performance 128KB block size with queue depth 32) Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1) Endurance 3 DWPD with additional 2 free slots for populating additional cache drives.	Latest generation servers are coming with E3.S NVMe SSDs in compact factor. Hence request you to change the clause as "Enterprise NVMe/ drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe/` Sequential read 6,200 MB/s, Sequential write 2,600 MB/s (Sequential performance 128KB block size with queue depth 32) Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1) Endurance 3 DWPD with additional 2 free slots for populating additional cache drives.	/E3.S NVMe add

223	Application Server	184	Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS/M.2 SSD Each SSD spec: 960GB+ Capacity , Write Intensive, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size	Latest generation servers are coming with E3.S NVMe SSDs in compact factor. Also, we recommend to remove the write intensive SSDs as the mentioned performance parameteres can be achieved using read intensive SSDs.also. Hence, request to change the clause as "Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS SSD/M.2 NVME SSD/**E3.S NVMe SSDs** Each SSD spec: 960GB+ Capacity, **Read Intensive**, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours,2000+ TBW, **1 DWPD** IOPS: Each SSD should have 150K+/75K+ Random Read/Write IOPS at 4K block size" for wider participation.	Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS/M.2 SSD/E3.S NVMe SSDs. Each SSD spec: 960GB+ Capacity , Write Intensive/Mixed Use, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size
224	Application Server	184	Each Server With Minimum Storage of 200 TB, With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency : between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	We wish to highlight that we use Encryption using controller on HDDs with ISE(Instant Sanitise Erase) in HPE systems which is better in security as compared to SED. Citing the reasons mentioned above, we request you to make the below changes: "Each Server With Minimum Storage of 200 TB, With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive)/**Encryption using controller** along with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s" for wider participation.	As per Tender Document
225	Web Server	187	Boot Storage subsystem with HW RAID 1 having 2 no:s x Enterprise SAS SSD/M.2 NVME SSD, Each SSD spec: 400GB+ Capacity, Write Intensive, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size	Latest generation servers are coming with E3.S NVMe SSDs in compact factor. Also, we recommend to remove the write intensive SSDs as the mentioned performance parameteres can be achieved using read intensive SSDs.also. Hence, request to change the clause as "Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS SSD/M.2 NVME SSD/**E3.S NVMe SSDs** Each SSD spec: 960GB+ Capacity, **Read Intensive**, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours,2000+ TBW, **1 DWPD** IOPS: Each SSD should have 150K+/75K+ Random Read/Write IOPS at 4K block size" for wider participation.	Boot Storage subsystem with HW RAID 1 having 2 no:s x Enterprise SAS SSD/M.2 NVME SSD/E3.S NVMe SSDs, Each SSD spec: 400GB+ Capacity, Write Intensive/Mixed Use, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size
226	Web Server	187	Storage: 2 nos x 18+ TB Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours) SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	We wish to highlight that we use Encryption using controller on HDDs with ISE(Instant Sanitise Erase) in HPE systems which is better in security as compared to SED. Citing the reasons mentioned above, we request you to make the below changes: "Storage: 2 nos x 18+ TB Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours) SED (Self encrypting drive)/**Encryption using controller** along with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	As per Tender Document

227	Load Balancer Server	189	Boot Storage subsystem with HW RAID 1 having 2 no:s x Enterprise SAS SSD/M.2 NVME SSD, Each SSD spec: 400GB+ Capacity , Write Intensive, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size	Latest generation servers are coming with E3.S NVMe SSDs in compact factor. Also, we recommend to remove the write intensive SSDs as the mentioned performance parameteres can be achieved using read intensive SSDs.also. Hence, request to change the clause as "Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS SSD/M.2 NVME SSD/**E3.S NVMe SSDs** Each SSD spec: 960GB+ Capacity, **Read Intensive**, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours,2000+ TBW, **1 DWPD** IOPS: Each SSD should have 150K+/75K+ Random Read/Write IOPS at 4K block size" for wider participation.	E3.S NVMe SSDs , Write Intensive/Mixed Use, agreed
228	Utility Server	191	Boot Storage subsystem with HW RAID 1 having 2 no:s x Enterprise SAS/M.2 SSD, Each SSD spec: 960GB or more Capacity , Write Intensive, Read (1 GB/s or more) Write (500 MB/s or more), MTBF = 2 million hours or more, 2000 TBW or more, 2 DWPD or more	Latest generation servers are coming with E3.S NVMe SSDs in compact factor. Also, we recommend to remove the write intensive SSDs as the mentioned performance parameteres can be achieved using read intensive SSDs.also. Hence, request to change the clause as "Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS SSD/M.2 NVME SSD/**E3.S NVMe SSDs** Each SSD spec: 960GB+ Capacity, **Read Intensive**, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours,2000+ TBW, **1 DWPD**	E3.S NVMe SSDs , Write Intensive/Mixed Use, M.2 NVMe SSD/M.2 SSD in all servers
229	Utility Server	191/192	UEFI Specification v2.8 or above , SMBIOS Specification v3.5 or above , ACPI Specification v6.4 or above , PMBUs Specification v1.2 or above , Redfish API , Advanced Encryption standard (AES) , SNMP v3 , TLS 1.2 or above , Active Directory v1.0. Manufactured in accordance with the international quality standards ISO 9001:2015 Compliance to Safety of IT Equipment: BIS / IEC 62368 Standards for EMC (Electro Magnetic Compatibility) Standards: EN 55035 Class A RoHS : EN IEC 63000	SMBIOS v3.5 and PMBUs v1,2 are OEM specific. Hence for wider participation, request to change the clause as "UEFI Specification v2.8 or above , **SMBIOS Specification v3.4** or above , ACPI Specification v6.4 or above , **PMBUs Specification v1.2 or equivalent technology** , Redfish API , Advanced Encryption standard (AES) , SNMP v3 , TLS 1.2 or above , Active Directory v1.0. Manufactured in accordance with the international quality standards ISO 9001:2015 Compliance to Safety of IT Equipment: BIS / IEC 62368 Standards for EMC (Electro Magnetic Compatibility) Standards: EN 55035 Class A RoHS : EN IEC 63000"	UEFI Specification v2.7 or above , SMBIOS Specification v3.3 or above , PMBUs Specification v1.2 or equivalent technology to be change in specification
230	Utility Server	192	Power Supply Efficiency: Platinum or Higher Storage (HDD) Drives: Sanitize Instant Erase, Self-Encrypting (SED). Required support should be available in RAID controller	Power Supply Efficiency: Platinum or Higher Storage (HDD) Drives: Sanitize Instant Erase, Self-Encrypting (SED)/**encryption using controllers**. Required support should be available in RAID controller	As per Tender Document
231	Storage Server	181	DAS and Server should be compatible and support of DAS to be provided by Server OEM only. Server OEM shall give undertaking for the support of DAS on their letterhead.	DAS and Server should be compatible and support of DAS to be provided by Server **OEM/Bidder** only. Server **OEM/Bidder** shall give undertaking for the support of DAS on their letterhead. Request you to kindly change to ensure maximum participation.	As per Tender Document
232	Storage Server	181	Processor: 2 Quantity (Dual socket) x Intel Xeon Gold/Platinum scalable series 5th Gen, 32+ cores/64+ Threads (2.7+ GHz base frequency, Cache Size 60+ MB) or Processor: 2 Quantity (Dual socket) x AMD Epyc 9004 or latest Series, 32+ cores/64+ Threads (2.7+ GHz base frequency, Cache Size 128+ MB)	As per our design, we support 60 or above internal HDDs within the 4U storage server chassis. Hence to manage the heat dissipation coming from CPU, memory and HDDs becomes very challenging. **For the reasons mentioned above, we request to change the processor to 32 Cores / 2.1 GHz base frequency.**	As per Tender Document
233	Storage Server	181	Total 2TB or higher RAM, DDR5 5000+ MHz ECC REG DIMM	As per our design, we support 60 or above internal HDDs within the 4U storage server chassis. Hence to manage the heat dissipation coming from CPU, memory and HDDs becomes very challenging. **For the reasons mentioned above, we request to change the Memory from 2TB to 1.5TB.**	As per Tender Document

234	Storage Server	181	Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS SSD/M.2 NVME SSD Each SSD spec: 960GB+ Capacity, Write Intensive, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size	Latest generation servers are coming with E3.S NVMe SSDs in compact factor. Also, we recommend to remove the write intensive SSDs as the mentioned performance parameteres can be achieved using read intensive SSDs.also. Hence, request to change the clause as "Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS SSD/M.2 NVME SSD/**E3.S NVMe SSDs** Each SSD spec: 960GB+ Capacity, **Read Intensive**, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours,2000+ TBW, **1 DWPD** IOPS: Each SSD should have 150K+/75K+ Random Read/Write IOPS at 4K block size" for wider participation.	Kindly refer revised Technical Specification
235	Storage Server	182	Each Server With Minimum Storage of 1440 TB, With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s Note: 1. Single DAS expansion can be used. However, the effective I/O throughput of all the disks combined should not be impacted due to any DAS expansion connector limitations. 2. DAS and Server should be compatible and support of DAS to be provided by Server OEM only. Server OEM shall give undertaking for the support of DAS on their letterhead.	We wish to highlight that we use Encryption using controller on HDDs with ISE(Instant Sanitise Erase) in HPE systems which is better in security as compared to SED. Citing the reasons mentioned above, we request you to make the below changes: "Each Server With Minimum Storage of 1440 TB, With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive)**/Encryption using controller along with ISE(Instant Sanitise Erase)** Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s" for wider participation. *Additioanlly, we also request you to consider the Storage Systems with internal HDD ONLY becasue the connectivity to external DAS using cables will create* ***additional point of failure.*** *This will severely impact the availability/reliability/performance of the solution.* *Also, storage servers with internal HDDs are* ***30-40% efficient*** *in terms of rack space and power.*	As per Tender Document
236	Storage Server	182/183	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe Sequential read 6,200 MB/s, Sequential write 2,600 MB/s (Sequential performance 128KB block size with queue depth 32) Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1) Endurance 3 DWPD with additional 2 free slots for populating additional cache drives.	Latest generation servers are coming with E3.S NVMe SSDs in compact factor. Hence request you to change the clause as "Enterprise NVMe/ drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe/**E3.S NVMe** Sequential read 6,200 MB/s, Sequential write 2,600 MB/s (Sequential performance 128KB block size with queue depth 32) Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1) Endurance 3 DWPD with additional 2 free slots for populating additional cache drives.	Kindly refer revised Technical Specification
237	Application Server	184	Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS/M.2 SSD Each SSD spec: 960GB+ Capacity , Write Intensive, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size	Latest generation servers are coming with E3.S NVMe SSDs in compact factor. Also, we recommend to remove the write intensive SSDs as the mentioned performance parameteres can be achieved using read intensive SSDs.also. Hence, request to change the clause as "Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS SSD/M.2 NVME SSD/**E3.S NVMe SSDs** Each SSD spec: 960GB+ Capacity, **Read Intensive**, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours,2000+ TBW, **1 DWPD** IOPS: Each SSD should have 150K+/75K+ Random Read/Write IOPS at 4K block size" for wider participation.	Kindly refer revised Technical Specification

238	Application Server	184	Each Server With Minimum Storage of 200 TB, With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency : between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	We wish to highlight that we use Encryption using controller on HDDs with ISE(Instant Sanitise Erase) in HPE systems which is better in security as compared to SED. Citing the reasons mentioned above, we request you to make the below changes: "Each Server With Minimum Storage of 200 TB, With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive)/**Encryption using controller** along with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s" for wider participation.	As per Tender Document
239	Web Server	187	Boot Storage subsystem with HW RAID 1 having 2 no:s x Enterprise SAS SSD/M.2 NVME SSD, Each SSD spec: 400GB+ Capacity, Write Intensive, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size	Latest generation servers are coming with E3.S NVMe SSDs in compact factor. Also, we recommend to remove the write intensive SSDs as the mentioned performance parameteres can be achieved using read intensive SSDs.also. Hence, request to change the clause as "Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS SSD/M.2 NVME SSD/**E3.S NVMe SSDs** Each SSD spec: 960GB+ Capacity, **Read Intensive**, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours,2000+ TBW, **1 DWPD** IOPS: Each SSD should have 150K+/75K+ Random Read/Write IOPS at 4K block size" for wider participation.	Kindly refer revised Technical Specification
240	Web Server	187	Storage: 2 nos x 18+ TB Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours) SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	We wish to highlight that we use Encryption using controller on HDDs with ISE(Instant Sanitise Erase) in HPE systems which is better in security as compared to SED. Citing the reasons mentioned above, we request you to make the below changes: "Storage: 2 nos x 18+ TB Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours) SED (Self encrypting drive)/**Encryption using controller** along with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	As per Tender Document
241	Load Balancer Server	189	Boot Storage subsystem with HW RAID 1 having 2 no:s x Enterprise SAS SSD/M.2 NVME SSD, Each SSD spec: 400GB+ Capacity , Write Intensive, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size	Latest generation servers are coming with E3.S NVMe SSDs in compact factor. Also, we recommend to remove the write intensive SSDs as the mentioned performance parameteres can be achieved using read intensive SSDs.also. Hence, request to change the clause as "Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS SSD/M.2 NVME SSD/**E3.S NVMe SSDs** Each SSD spec: 960GB+ Capacity, **Read Intensive**, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours,2000+ TBW, **1 DWPD** IOPS: Each SSD should have 150K+/75K+ Random Read/Write IOPS at 4K block size" for wider participation.	Kindly refer revised Technical Specification

242	Utility Server	191	Boot Storage subsystem with HW RAID 1 having 2 no:s x Enterprise SAS/M.2 SSD, Each SSD spec: 960GB or more Capacity , Write Intensive, Read (1 GB/s or more) Write (500 MB/s or more), MTBF = 2 million hours or more, 2000 TBW or more, 2 DWPD or more	Latest generation servers are coming with E3.S NVMe SSDs in compact factor. Also, we recommend to remove the write intensive SSDs as the mentioned performance parameteres can be achieved using read intensive SSDs.also. Hence, request to change the clause as "Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS SSD/M.2 NVME SSD/**E3.S NVMe SSDs** Each SSD spec: 960GB+ Capacity, **Read Intensive**, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours,2000+ TBW, **1 DWPD**	Kindly refer revised Technical Specification
243	Utility Server	191/192	UEFI Specification v2.8 or above , SMBIOS Specification v3.5 or above , ACPI Specification v6.4 or above , PMBUs Specification v1.2 or above , Redfish API , Advanced Encryption standard (AES) , SNMP v3 , TLS 1.2 or above , Active Directory v1.0. Manufactured in accordance with the international quality standards ISO 9001:2015 Compliance to Safety of IT Equipment: BIS / IEC 62368 Standards for EMC (Electro Magnetic Compatibility) Standards: EN 55035 Class A RoHS : EN IEC 63000	SMBIOS v3.5 and PMBUs v1,2 are OEM specific. Hence for wider participation, request to change the clause as "UEFI Specification v2.8 or above , **SMBIOS Specification v3.4** or above , ACPI Specification v6.4 or above , **PMBUs Specification v1.2 or equivalent technology** , Redfish API , Advanced Encryption standard (AES) , SNMP v3 , TLS 1.2 or above , Active Directory v1.0. Manufactured in accordance with the international quality standards ISO 9001:2015 Compliance to Safety of IT Equipment: BIS / IEC 62368 Standards for EMC (Electro Magnetic Compatibility) Standards: EN 55035 Class A RoHS : EN IEC 63000"	Kindly refer revised Technical Specification
244	Utility Server	192	Power Supply Efficiency: Platinum or Higher Storage (HDD) Drives: Sanitize Instant Erase, Self-Encrypting (SED). Required support should be available in RAID controller	Power Supply Efficiency: Platinum or Higher Storage (HDD) Drives: Sanitize Instant Erase, Self-Encrypting (SED)/**encryption using controllers**. Required support should be available in RAID controller	As per Tender Document
245	Storage Server	181	Processor: 2 Quantity (Dual socket) x Intel Xeon Gold/Platinum scalable series 5th Gen, 32+ cores/64+ Threads (2.7+ GHz base frequency, Cache Size 60+ MB) or Processor: 2 Quantity (Dual socket) x AMD Epyc 9004 or latest Series, 32+ cores/64+ Threads (2.7+ GHz base frequency, Cache Size 128+ MB)	As per our design, we support 60 or above internal HDDs within the 4U storage server chassis. Hence to manage the heat dissipation coming from CPU, memory and HDDs becomes very challenging. **For the reasons mentioned above, we request to change the processor to 32 Cores / 2.1 GHz base frequency.**	As per Tender Document
246	Storage Server	181	Total 2TB or higher RAM, DDR5 5000+ MHz ECC REG DIMM	As per our design, we support 60 or above internal HDDs within the 4U storage server chassis. Hence to manage the heat dissipation coming from CPU, memory and HDDs becomes very challenging. **For the reasons mentioned above, we request to change the Memory from 2TB to 1.5TB.**	As per Tender Document
247	Storage Server	181	Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS SSD/M.2 NVME SSD Each SSD spec: 960GB+ Capacity, Write Intensive, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size	Latest generation servers are coming with E3.S NVMe SSDs in compact factor. Also, we recommend to remove the write intensive SSDs as the mentioned performance parameteres can be achieved using read intensive SSDs.also. Hence, request to change the clause as "Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS SSD/M.2 NVME SSD/**E3.S NVMe SSDs** Each SSD spec: 960GB+ Capacity, **Read Intensive**, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours,2000+ TBW, **1 DWPD** IOPS: Each SSD should have 150K+/75K+ Random Read/Write IOPS at 4K block size" for wider participation.	Kindly refer revised Technical Specification

248	Storage Server	182	Each Server With Minimum Storage of 1440 TB, With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s Note: 1. Single DAS expansion can be used. However, the effective I/O throughput of all the disks combined should not be impacted due to any DAS expansion connector limitations. 2. DAS and Server should be compatible and support of DAS to be provided by Server OEM only. Server OEM shall give undertaking for the support of DAS on their letterhead.	We wish to highlight that we use Encryption using controller on HDDs with ISE(Instant Sanitise Erase) in HPE systems which is better in security as compared to SED. Citing the reasons mentioned above, we request you to make the below changes: "Each Server With Minimum Storage of 1440 TB, With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive)**/Encryption using controller along with ISE(Instant Sanitise Erase)** Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s" for wider participation. *Additioanlly, we also request you to consider the Storage Systems with internal HDD ONLY becasue the connectivity to external DAS using cables will create* ***additional point of failure.*** *This will severely impact the availability/reliability/performance of the solution.* *Also, storage servers with internal HDDs are* ***30-40% efficient*** *in terms of rack space and power.*	As per Tender Document
249	Storage Server	182/183	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe Sequential read 6,200 MB/s, Sequential write 2,600 MB/s (Sequential performance 128KB block size with queue depth 32) Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1) Endurance 3 DWPD with additional 2 free slots for populating additional cache drives.	Latest generation servers are coming with E3.S NVMe SSDs in compact factor. Hence request you to change the clause as "Enterprise NVMe/ drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe/**E3.S NVMe** Sequential read 6,200 MB/s, Sequential write 2,600 MB/s (Sequential performance 128KB block size with queue depth 32) Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1) Endurance 3 DWPD with additional 2 free slots for populating additional cache drives.	Kindly refer revised Technical Specification
250	Application Server	184	Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS/M.2 SSD Each SSD spec: 960GB+ Capacity , Write Intensive, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size	Latest generation servers are coming with E3.S NVMe SSDs in compact factor. Also, we recommend to remove the write intensive SSDs as the mentioned performance parameteres can be achieved using read intensive SSDs.also. Hence, request to change the clause as "Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS SSD/M.2 NVME SSD/**E3.S NVMe SSDs** Each SSD spec: 960GB+ Capacity, **Read Intensive**, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours,2000+ TBW, **1 DWPD** IOPS: Each SSD should have 150K+/75K+ Random Read/Write IOPS at 4K block size" for wider participation.	Kindly refer revised Technical Specification
251	Application Server	184	Each Server With Minimum Storage of 200 TB, With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency : between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	We wish to highlight that we use Encryption using controller on HDDs with ISE(Instant Sanitise Erase) in HPE systems which is better in security as compared to SED. Citing the reasons mentioned above, we request you to make the below changes: "Each Server With Minimum Storage of 200 TB, With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive)/**Encryption using controller** along with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s" for wider participation.	As per Tender Document

252	Web Server	187	Boot Storage subsystem with HW RAID 1 having 2 no:s x Enterprise SAS SSD/M.2 NVME SSD, Each SSD spec: 400GB+ Capacity, Write Intensive, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size	Latest generation servers are coming with E3.S NVMe SSDs in compact factor. Also, we recommend to remove the write intensive SSDs as the mentioned performance parameteres can be achieved using read intensive SSDs.also. Hence, request to change the clause as "Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS SSD/M.2 NVME SSD/**E3.S NVMe SSDs** Each SSD spec: 960GB+ Capacity, **Read Intensive**, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours,2000+ TBW, **1 DWPD** IOPS: Each SSD should have 150K+/75K+ Random Read/Write IOPS at 4K block size" for wider participation.	Kindly refer revised Technical Specification
253	Web Server	187	Storage: 2 nos x 18+ TB Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours) SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	We wish to highlight that we use Encryption using controller on HDDs with ISE(Instant Sanitise Erase) in HPE systems which is better in security as compared to SED. Citing the reasons mentioned above, we request you to make the below changes: "Storage: 2 nos x 18+ TB Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours) SED (Self encrypting drive)/**Encryption using controller** along with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	As per Tender Document
254	Load Balancer Server	189	Boot Storage subsystem with HW RAID 1 having 2 no:s x Enterprise SAS SSD/M.2 NVME SSD, Each SSD spec: 400GB+ Capacity , Write Intensive, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size	Latest generation servers are coming with E3.S NVMe SSDs in compact factor. Also, we recommend to remove the write intensive SSDs as the mentioned performance parameteres can be achieved using read intensive SSDs.also. Hence, request to change the clause as "Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS SSD/M.2 NVME SSD/**E3.S NVMe SSDs** Each SSD spec: 960GB+ Capacity, **Read Intensive**, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours,2000+ TBW, **1 DWPD** IOPS: Each SSD should have 150K+/75K+ Random Read/Write IOPS at 4K block size" for wider participation.	Kindly refer revised Technical Specification
255	Utility Server	191	Boot Storage subsystem with HW RAID 1 having 2 no:s x Enterprise SAS/M.2 SSD, Each SSD spec: 960GB or more Capacity , Write Intensive, Read (1 GB/s or more) Write (500 MB/s or more), MTBF = 2 million hours or more, 2000 TBW or more, 2 DWPD or more	Latest generation servers are coming with E3.S NVMe SSDs in compact factor. Also, we recommend to remove the write intensive SSDs as the mentioned performance parameteres can be achieved using read intensive SSDs.also. Hence, request to change the clause as "Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS SSD/M.2 NVME SSD/**E3.S NVMe SSDs** Each SSD spec: 960GB+ Capacity, **Read Intensive**, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours,2000+ TBW, **1 DWPD**	Kindly refer revised Technical Specification
256	Utility Server	191/192	UEFI Specification v2.8 or above , SMBIOS Specification v3.5 or above , ACPI Specification v6.4 or above , PMBUs Specification v1.2 or above , Redfish API , Advanced Encryption standard (AES) , SNMP v3 , TLS 1.2 or above , Active Directory v1.0. Manufactured in accordance with the international quality standards ISO 9001:2015 Compliance to Safety of IT Equipment: BIS / IEC 62368 Standards for EMC (Electro Magnetic Compatibility) Standards: EN 55035 Class A RoHS : EN IEC 63000	SMBIOS v3.5 and PMBUs v1,2 are OEM specific. Hence for wider participation, request to change the clause as "UEFI Specification v2.8 or above , **SMBIOS Specification v3.4** or above , ACPI Specification v6.4 or above , **PMBUs Specification v1.2 or equivalent technology** , Redfish API , Advanced Encryption standard (AES) , SNMP v3 , TLS 1.2 or above , Active Directory v1.0. Manufactured in accordance with the international quality standards ISO 9001:2015 Compliance to Safety of IT Equipment: BIS / IEC 62368 Standards for EMC (Electro Magnetic Compatibility) Standards: EN 55035 Class A RoHS : EN IEC 63000"	Kindly refer revised Technical Specification

257	Utility Server	192	Power Supply Efficiency: Platinum or Higher Storage (HDD) Drives: Sanitize Instant Erase, Self-Encrypting (SED). Required support should be available in RAID controller	Power Supply Efficiency: Platinum or Higher Storage (HDD) Drives: Sanitize Instant Erase, Self-Encrypting (SED)/**encryption using controllers**. Required support should be available in RAID controller	As per Tender Document
258	Scope of work of	89	Supply, Installation, Testing & Commissioning (SITC) of IT Infrastructure & Monitoring and Management software at DC, DR by OEM's manpower	We understand the installation, testing & commissioning need to be carried out by OEM, Request clarification on Monitoring & Management software, scope & ownership (OEM/SI). Do we need to consider 3rd party software for Monitoring & Management purpose.	As per Tender Document
259	General Activities to be performed by Contractor for the project, Point	97	The bid should include OEM professional services for the successful implementation of project. The OEM professional services shall include but not limited to solution architecture, design, installation, preparation of acceptance test plan & procedure with expected results and end user training leading to OEM Certification. The above activities should be jointly done by the Contractor and the OEM, as per the best security practices for the final acceptance.	We request for pre defined criteria & procedures of acceptance testing, if available	ATP will be made by successful bidder in consultation with ERNET India and CERT-In
260	Training	99	Training for 20 Persons (in batches) shall be provided onsite by the OEM experts/OEM representatives for equipment of respective OEMs for installation and operations of installed equipment(s) per equipment supplied.	We understand that we need to factor training for total of 20 users which will be further divided into 5 batches, kindly confirm if the understanding is correct These trainings need to be completed within 3 months Implementation of Infrastructure supplied by Dell is completed.	Training batches will be decided by successful bidder in consultation with ERNET India and CERT-In
261	Note	117	OEM Specialist (such as OEM Security/ Network/ Server Specialist etc.) must be on OEM's Payroll with minimum 5-year experience.	We request to kindly allow OEM to provide the manpower on OEM Payroll/OEM empaneled Service delivery partner payroll with ownership of OEM.	As per Tender Document
262	Heavy Duty Workstation	170	3. OS: Windows 10/11 Pro with Latest Microsoft Office License (Perpetual) along with Antivirus (for 5 Years)	Windows 10 will reach end of support in October 2025. We recommend Windows 11 to ensure your system is equipped with the latest technology from the outset.	OS: Windows 11 Pro with Latest Microsoft Office License (Perpetual) along with Antivirus (for 5 Years)
263	Heavy Duty Workstation	170	4. RAM: 64GB+, DDR5, 4500MHz	Is 64GB+ the expandibility? Also, the average processing speed of DDR5 type memory in desktops starts from 4000MHz onwards. We request a change of **4000MHz or** more on similar lines.	As per Tender Document
264	Heavy Duty Workstation	171	9. Ports: 2 HDMI, 1 VGA, 2 Audio-in / out, 1 USB 2.0, 3 USB 3.0, 1 USB C	We request to change 2HDMI to **2HDMI/ 2DP**. Display ports are primary video ports used in commercial models. We request to change the port ask and open it for DP too as it serves the same function and can support similar resolutions.	As per Tender Document
265	Mobile Workstation Laptop	172	5. Monitor: 14'' inch UHD or above with Capacitive Touch screen	We request to change UHD to FHD for paticipation	As per Tender Document
266	Mobile Workstation Laptop	172	7. USB Ports: USB 3, USB 2.0, USB Type-C	**We request to change this to 2X USB 3**, USB Type C instead of USB 3, USB 2, USB Type C. As USB 3 is the current industry update. USB 3 can improve the data transfer speeds by approx. 10 times.	Bidder may also give 2xUSB 3
267	Storage Server	181	Each SSD spec: 960GB+ Capacity, Write Intensive, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size	Kindly remove the performance parameters since these are OS drives only; and change the specifications as below: **Each SSD spec: 960GB SSD SAS, Mixed Use**	Kindly refer revised Technical Specification
268	Storage Server	182	With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	Kindly modify the clause as below: With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (**at 4KB, QD32**): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	As per Tender Document

269	Storage Server	182	All the HDDs in the server should be configurable under a single virtual drive with RAID 5,6,50,60. Storage management including raid configuration. Required support for SED (Self Encrypting Drive) and ISE (Instant Sanitise Erase) should be available in RAID controller.	We understand that only the drives asked for the capacity as asked in Storage i.e 1440TB shall confirm to SED and ISE. Kindly confirm. Pls note that SED and ISE is a feature of the proposed HDD and will be supported by the RAID Controller only if the HDD is SED and ISE enabled. Hope the understanding is correct.	Each hard disk should be with SED and ISE features. "Instant Sanitise Erase" may be read as "Instant Secure Erase" in all servers.
270	Application Server	184	Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS/M.2 SSD Each SSD spec: 960GB+ Capacity , Write Intensive, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size	Kindly modify the performance parameters since these are OS drives only; and change the specifications as below: **Each SSD spec: 960GB SSD SAS, Mixed Use**	Kindly refer revised Technical Specification
271	Application Server	184	With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency : between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	Kindly change the specifications as below: With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (**at 4KB, QD32**): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	As per Tender Document
272	Application Server	185	All the HDDs in the server should be configurable under a single virtual drive with RAID 5, 6, 50, 60 Storage management including raid configuration. Required support for SED (Self Encrypting Drive) and ISE (Instant Sanitise Erase) should be available in RAID controller.	We understand that only the drives asked for the capacity as asked in Storage i.e 200TB shall confirm to SED and ISE. Kindly confirm. Pls note that SED and ISE is a feature of the proposed HDD and will be supported by the RAID Controller only if the HDD is SED and ISE enabled. Hope the understanding is correct.	Each hard disk should be with SED and ISE features. "Instant Sanitise Erase" may be read as "Instant Secure Erase"
273	Web Server	186	Processor: 2 Quantity (Dual socket) x Intel Xeon Gold/Platinum scalable series 5th Gen 8 core processor (3.1+ GHz base frequency, Cache Size 20+ MB) OR Processor: 2 Quantity (Dual socket) x AMD Epyc 9004 or latest Series, 8 core processor (3.1+ GHz base frequency, Cache Size 64+ MB)	Kindly Modify the specifications as below: - Processor: 2 Quantity (Dual socket) x Intel Xeon Gold/Platinum scalable series 5th Gen 8 core processor (3.1+ GHz base frequency, Cache Size 20+ MB) OR Processor: 2 Quantity (Dual socket) x AMD Epyc 9004 or latest Series, 8 core processor (3.0+ GHz base frequency, Cache Size 64+ MB)	3.0 Ghz accepted
274	Web Server	187	Each SSD spec: 400GB+ Capacity, Write Intensive, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size	Kindly modify the performance parameters since these are OS drives only; and change the specifications as below: **Each SSD spec: 800GB SSD SAS ISE, Mixed Use**	Kindly refer revised Technical Specification
275	Web Server	187	Storage: 2 nos x 18+ TB Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours) SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	Kindly change the specifications as below: **Storage: 2 nos x 18+ TB Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours) SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms**	As per Tender Document
276	Web Server	187	All the HDDs in the server should be configurable under a single virtual drive with RAID 5, 6, 50, 60 Storage management including raid configuration. Required support for SED (Self Encrypting Drive) and ISE (Instant Sanitise Erase) should be available in RAID controller.	We understand that only the drives asked for the capacity as asked in Storage i.e 2* 18TB shall confirm to SED and ISE. Kindly confirm. Pls note that SED and ISE is a feature of the proposed HDD and will be supported by the RAID Controller only if the HDD is SED and ISE enabled. Hope the understanding is correct.	Each hard disk should be with SED and ISE features. "Instant Sanitise Erase" may be read as "Instant Secure Erase"
277	Load Balancer Server	189	Each SSD spec: 400GB+ Capacity , Write Intensive, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size	Kindly modify the performance parameters since these are OS drives only; and change the specifications as below: **Each SSD spec: 800GB SSD SAS ISE, Mixed Use**	Kindly refer revised Technical Specification
278	Utility Server	191	Each SSD spec: 960GB or more Capacity , Write Intensive, Read (1 GB/s or more) Write (500 MB/s or more), MTBF = 2 million hours or more, 2000 TBW or more, 2 DWPD or more	Kindly remove the performance parameters since these are OS drives only; and change the specifications as below: **Each SSD spec: 960GB SSD SAS, Mixed Use**	Kindly refer revised Technical Specification

279	Utility Server	191	Storage: 6 or more no:s x 8 TB or more Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12 Gb/s, 7200 RPM, 256 MB Cache. 3.5°, MTBF = 8 Lakhs hours) System must have atleast 12 x LFF front accessible Hot-Swap Drive Bays with backplane supporting SAS/SATA/NVMe drives	Kindly Modify the drive capacity to 18TB for standardization. Kindly change the specifications as below: **Storage: 6 or more 8 TB Enterprise drives OR 3 nos of 18+ TB Enterprise Drives, (With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD32): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s**	As per Tender Document
280	Utility Server	191	All PCIe slots must support Gen 5 speed and supporting 10.5" Length based Controllers	Kindly modify the specifications as below:- **All PCIe slots must support Gen 4/5 speed and supporting X8/X16 and FH/ LP or 10.5" Length based Controllers.**	All PCIe slots must support Gen 4/5 speed and supporting (X8/X16 and FH/ LP) or supporting 10.5" Length based Controllers.
281	Utility Server		UEFI Specification v2.8 or above , SMBIOS Specification v3.5 or above.....	This clause is conflicting with the clause under section "Common Management & Security Features for all Servers Pt. 4". Kindly remove the same. The aksed specifications under Pt. 4 asks for "UEFI specifications v2.7 and SMBIOS Specifications v3.3.0 or above" which we comply.	Kindly refer revised Technical Specification
282	Utility Server	192	Storage (HDD) Drives: Sanitize Instant Erase, Self-Encrypting (SED). Required support should be available in RAID controller	Pls note that SED and ISE is a feature of the proposed HDD and will be supported by the RAID Controller only if the HDD is SED and ISE enabled. Kindly confirm if the understanding is correct.	understanding is correct
283	GPU Server		3TB memory using DDR5 (4800 MHz or higher) operating at min. 4400MHz Server should be populated in balanced memory configuration.	Kindly Modify the specifications as below: Kindly note that as per best practices of OEM, 2TB is recommended for such AI workload specific systems. **Hence kindly change it to 2TB memory using DDR5 (4800 MHz or higher) operating at min. 4400MHz Server should be populated in balanced memory configuration.**	As per Tender Document
284	Monitoring & Management Tool for	200	iv. System tagging giving admin flexibility to provide metadata tags to each system to enable users to filter and sort systems based on user assigned attributes	Kindly modifythe specifications as below:- iv. System tagging giving admin flexibility to provide metadata tags to each system to enable users to filter and sort systems based on user assigned attributes **OR the management console should be enabled with Elastic search feature capable of accessing all information within the console**	Accepted ; OR the management console should be enabled with Elastic search feature capable of accessing all information within the console
285	Section VI : Qualification Criteria B. Original Equipment Manufacturer (OEM)'s	RFP Page 87 of 389	2. The annual average financial turnover of the Server OEM; during the last three years (FY 21-22, 22-23, 23-24), on standalone basis ;should not be less than Rs.350 Cr. A certificate from a practicing Chartered Accountant (with UDIN of the CA) on its letter head confirming annual turnover and average annual turnover have to be provided along with the bid. In case the OEM has been incorporated in a country outside India then specified financial detail needs to be provided in INR by converting the foreign currency with INR.	Requested to kindly delete "on standalone basis " for the reason to maintain homogeneity with Turnover Criteria mentioned for Bidders in A. Bidder's Qualification Criteria Clause-2 , where minimum average annual audited financial turnover is asked, and secondly since the current language of the clause asks for average turnover hence specifying "standalone" is contrary to the average criteria. Hence the revised clause is requested as below : 2.The annual average financial turnover of the Server OEM; during the last three years (FY 21-22, 22-23, 23-24), ;should not be less than Rs.350 Cr. A certificate from a practicing Chartered Accountant (with UDIN of the CA) on its letter head confirming annual turnover and average annual turnover have to be provided along with the bid. In case the OEM has been incorporated in a country outside India then specified financial detail needs to be provided in INR by converting the foreign currency with INR.	The clause may be read as : 2. The annual average financial turnover of the Server OEM; during the last three years (FY 21-22, 22-23, 23-24) should not be less than Rs.350 Cr. A certificate from a practicing Chartered Accountant (with UDIN of the CA) on its letter head confirming annual turnover and average annual turnover have to be provided along with the bid. In case the OEM has been incorporated in a country outside India then specified financial detail needs to be provided in INR by converting the foreign currency with INR.
286	Storage Server	RFP Page 181 of 389	3. Memory : Total 2TB or higher RAM, DDR5 5000+ MHz ECC REG DIMM	Request to kindly change to below as per memory configuration Operating Frequency Total 2TB or higher RAM, DDR5 5000+ MHz (operating frequemncy at 4400 MHz) ECC REG DIMM	As per Tender Document

287	Servers	RFP Page 193 of 389	1. Management Features 16. Out of band web management should support automatic backup system configuration settings (BIOS, IPMI, NIC) for restoration of configuration	Requested to kindly delete "automatic" as per best practice of configuration setting backup by administrator which are latest/correct 16. Out of band web management should support backup system configuration settings (BIOS, IPMI, NIC) for restoration of configuration	Accepted; 1. Management Features 16. Out of band web management should support automatic/manual backup system configuration settings (BIOS, IPMI, NIC) for restoration of configuration
288	Monitoring and Management Tool for	RFP Page 199 of 389	5. Real-time monitoring, logging and alerting of several parameters like: c. SSD wear monitoring	Requested to kindly change to below for maintaining homogeneity with specifications mentioned in Common Management & Security features for all above servers clause 5c. C. SSD wear monitoring/SSD impending and active failure alerts	Accepted; c. SSD wear monitoring/SSD impending and active failure alerts
	Storage Server	181	Processor: 2 Quantity (Dual socket) x Intel Xeon Gold/Platinum scalable series 5th Ge**n, 32+ cores/64+ Thread**s (**2.7+** GHz base frequency, Cache Size **60+ MB)** or Processor: 2 Quantity (Dual socket) x A**MD Epyc 9004 or** latest Series, **32+ cores/64+** Threads (2.7+ GHz base frequency, Cache Size **128+ MB)**	1.Has the storage server been benchmarked with tools like FIO that will give a good spread of read/write operations, for the different CPU options . Pls consider measuring same on latets Gen CPUs (viz Intel Platinum scalable series 5th Gen) with 2.1Ghz frequency 2.Given that the disks will be 7200 RPM, has there been a profiling done to determine the percentage of disk-io-waits vs. cpu contentions? 3.Do the storage servers employ a storage-as-a-service solution – that will bring in compression (employ the power of QAT on the CPUs) reduce the disk pressure and give more job to the CPUs to do. 4.Do the storage servers consider a hot/warm/cold storage pools, storage software intelligently landing payloads based on the access patterns across the different pools. 5.What is the storage client? What is the frequency of data access? What is the time-profile of the data elements that are accessed?	As per tender document
	Application Server	184	2 Quantity (Dual socket) x Intel Xeon Gold/Platinum scalable series 5th Gen, 28+ cores (2.7+ GHz base frequency, Cache Size 60+ MB) OR 2 Quantity (Dual socket) x AMD Epyc 9004 or latest , 28+ cores (2.7+ GHz base frequency, Cache Size 128+ MB)		as per tender document
	Web Server		Processor: 2 Quantity (Dual socket) x Intel Xeon Gold/Platinum scalable series 5th Gen 8 core processor (3.1+ GHz base frequency, Cache Size 20+ MB) OR Processor: 2 Quantity (Dual socket) x AMD Epyc 9004 or latest Series, 8 core processor (3.1+ GHz base frequency, Cache Size 64+ MB)		Kindly refer revised Technical Specification
290	Load Balancer Server	189	2 Quantity (Dual socket) x Intel Xeon Gold/Platinum scalable series 5th Gen, 24+ cores (2.7+ GHz base frequency, Cache Size 30+ MB) OR 2 Quantity (Dual socket) x AMD Epyc 9004 or latest , 24+ cores (2.7+ GHz base frequency, Cache Size 128+ MB)	1.Has the storage server been benchmarked with tools like FIO that will give a good spread of read/write operations, for the different CPU options . Pls consider measuring same on latets Gen CPUs (viz Intel Platinum scalable series 5th Gen) with 2.1Ghz frequency 2.Given that the disks will be 7200 RPM, has there been a profiling done to determine the percentage of disk-io-waits vs. cpu-contentions? 3.Do the storage servers employ a storage-as-a-service solution – that will bring in compression (employ the power of QAT on the CPUs) reduce the disk pressure and give more job to the CPUs to do. 4.Do the storage servers consider a hot/warm/cold storage pools, storage software intelligently landing payloads based on the access patterns across the different pools. 5.What is the storage client? What is the frequency of data access? What is the time-profile of the data elements that are accessed?	As per tender document
	Utility Server	190	2 Quantity (Dual socket) x Intel Xeon Gold/Platinum scalable series 5th Gen, 32 or more cores (2.4 GHz or more base frequency. Cache Sze 60 MB or more) OR 2 Quantity (Dual socket) x AMD Epyc 9004 or latest Series, 32 or more cores (2.4 GHz or more base frequency Cache Size 60 MB or more)		as per tender document

	GPU Server	195	Processor: 2 Quantity (Dual socket) x Intel Platinum scalable series 5th Ge**n, 48+ cores/96+ Thread**s (**2.1+** GHz base frequency, Cache Size **260+ MB)** or Processor: 2 Quantity (Dual socket) x A**MD Epyc 9004 or** latest Series, **48+ cores/96+** Threads (2.1+ GHz base frequency, Cache Size **256+ MB)**		as per tender document
295	Heavy Duty Workstatio	Page No - 348	Processor - Intel 13th Generation Core i7 Processor or AMD Zen 5 Ryzen 7 series or higher	**1-Requesting the dept. to update the Processor Specification as 14th Generation Intel Core-i7 or 8000-Series AMD Ryzen 7 or Higher.** **2-The department has compared an older generation of Intel processors with the latest available AMD series, which does not provide an equivalent solution in terms of Techno-Commercial performance ratio.** **3- Furthermore, the department has referred to AMD's architecture name, Zen5, which is technically not comparable to any specific generation. This is incorrect and needs to be removed.**	1-Intel 14th Generation Core i7 Processor or 8000-Series AMD Ryzen 7 or Higher. 2- As per Tender Document 3-Accepted; Kindly refer to revised Tech Specifications
296	Heavy Duty Workstatio	Page No - 348	Cores - 12 (minimum)	**1- Requesting the dept. to update the Core-Count as: Minimum 8-Multithreaded Cores.** **The internal architectures of AMD and Intel differ significantly. AMD exclusively uses High Performance Cores, while Intel employs a Hybrid Architecture that combines Performance and Efficiency Cores.** **2- Requesting the dept. to update the Processor Specification as 13th Generation Intel Core-i7 or 7000-Series AMD Ryzen 7 or Higher.**	As per Tender Document
297	Mobile Workstation Laptop	Page No - 350	13th Generation Intel® Core™ i7 Processor or AMD Zen4 Ryzen 7/8 Series	The department has referred to AMD's architecture name, Zen4, which is technically not comparable to any specific generation. This is incorrect and needs to be removed.	13th Generation Intel® Core™ i7 Processor or 7000-Series AMD Ryzen 7 or higher
298	Utility Server	Part A Page 13	Virtualization Stack: Enterprise virtualization software license for the system for asked cores to be supplied with the system. System offered must be certified with offered virtualization software, certificate must be submitted with technical bid	**Request:** Request to add detailed technical specifications **Justification**: In reference to the guidelines of MeitY for deploying ICT solutions leveraging the latest technologies, virtualization plays a crucial role to ensure scalable and secure infrastructure that enables enhanced application availability and performance. However, the current RFP only covers basic specifications. We kindly request that you provide comprehensive specifications for virtualization stack, similar to those outlined for other products in the RFP. We have attached the detailed generic virtualization specifications for inclusion in the RFP. Request to please incorporate the same	as per tender document
299	Utility Server			Solution should include compute Virtualization layer that sits directly on the bare metal server hardware with no dependence on a general purpose OS with features like proactive HA, DRS, agentless anti - malware/anti-virus, replication, fault tolerance with continuous availability of VMs with zero downtime and zero data loss, hot add of CPU, memory, devices for windows as well as linux VMs, VM level encryption, secure boot, uninterrupted service delivery within and across datacenter at geographical distance (<100ms latency), distributed virtual switch, kernel embedded network and storage virtualization technology.	as per tender document
300	Utility Server			The server virtualizatoin managment solution should have the ability to expand up to at least 8 racks worth of servers without the need addition of additional management points	as per tender document
301	Utility Server			Should include storage virtualization /HCI software supporting all flash nodes which is Hardware independent to provide flexibility of choosing hardware from any server manufacturer & should support mixing of different compatible Server brands in same Cluster. It should work on mutually certified hardware of any vendor like dell, HP, Cisco, Lenovo, Hitachi etc. Compatibility certification should be publicly endorsed by both, i.e. hardware OEM & Hyper Converged Software OEM.	as per tender document

302	Utility Server			Storage virtualization should support VM-Centric controls for managing storage service levels for capacity, IOPS, availability QoS by storage policy-based management and should not be dependent on Luns. Should also support features like rack awareness, deduplication, compression & raid 5,6 through erasure coding (for all flash).	as per tender document
303	Utility Server			The solution should have an automated upgrade and patching process that allows full administrative control on the selection of storage software bundles, resources to upgrade and the timing of the upgrades and provide periodic pre-integrated and interop tested software bundles for patching and upgrade of the storage component products.	as per tender document
304	Utility Server			Solution provide traffic visibility, end point monitoring for visibility up to layer 7 for network monitoring and automating application security rules, firewall planning & management, network virtualization operations & troubleshooting tools.	as per tender document
305	Utility Server			The solution should provide the network virtualization platform for software defined datacenter, delivering the operational model of a virtual machine for entire networks including switching, routing, and firewalling are embedded in the hypervisor and distributed across the environment.	as per tender document
306	Utility Server			The solution should have highly granular (per VM or per VM interface) level security capabilities - potentially accessed through the network virtualization layer.	as per tender document
307	Utility Server			The solution should provide virtual machine workload isolation, ensuring each VM workload is securely segregated from others and individually secured.	as per tender document
308	Utility Server			The solution should offer comprehensive flow assessment and analytics and security groups and firewall rules suggestion for the purpose of implementing a zero-trust security within the datacentre.	as per tender document
309	Utility Server			Solution should provide automation and orchestration solution for automated delivery of IaaS, PaaS, XaaS/ SaaS services so that when VM/app is created it should automatically get the required virtualized compute, storage, switching, routing services without any manual intervention.	as per tender document
310	Utility Server			The solution should include unique lifecycle management services that automate day 0 to day 2 operations, from bring up to configuration, resources provisioning and patching/upgrades.	as per tender document
311	Utility Server			Solution should monitor utilization of running VMs and should reclaim resources from idle VMs and allocate to other VMs in automated fashion.	as per tender document
312	Utility Server			Solution should provide monitoring and management of complete virtualized infrastructure with prebuilt and configurable operations dashboards to provide real-time insight into infrastructure behaviour, upcoming problems, and opportunities for efficiency improvements.	as per tender document
313	Utility Server			Solution capacity analytics should provide "What If" scenarios for physical, virtual & container environment and provide infrastructure and operations, log analytics to eliminate time-consuming problem resolution processes through automated root cause analysis	as per tender document
314	Utility Server			The solution shall preemptively rebalance workloads in advance of upcoming demands and spikes, eliminating resource contention before it happens thus ensuring that workloads get the resources that they need at all times	as per tender document
315	Utility Server			The health of the various subcomponents should be monitored and reported within the solution	as per tender document
316	Utility Server			The solution should provide alert management on problem detection. Each notification should include a clear description of the problem and provides remediation actions needed to restore service, degradations or failures are aggregated and correlated to workload/ virtual domains to enable a clear view of the impact of any issue.	as per tender document

317	Utility Server			The virtual domains/group/DC in the solution should be policy controlled to provide specific capacity, availability and performance as required by workloads	as per tender document
318	Utility Server			The solution should provide Workload Automation capabilities. that dynamically defines and controls the environment in the Optimal State in real time. This should Enforce data sovereignty & business continuity policies for each workload by having full stak visibility.	as per tender document
319	Utility Server			The solution should offer a data-as-a-service toolkit for on-demand provisioning and automated management of PostgreSQL and MySQL databases within the proposed virtualized environment.	as per tender document
320	Utility Server			The provided solution should possess the capability to enable seamless mobility across data centers and remote locagtion, allowing for the movement of VMs within ERNET India data center, from local data center to remote location, or across data centers and remote locations, thereby optimizing resource utilization.	as per tender document
321	Utility Server			The management components of the solution should have high availability that allows nondisruptive operation of the running workloads.	as per tender document
322	Utility Server			Bidder should ensure OEM support (web & telephonic)for L1, L2 and L3 levels 24x7x365 with unlimited incident support and 30 mins or less response time including the unlimited upgrades and updates for a period of 3 years from the date of commissioning.	as per tender document
323	Load balancer with WAF	145	The Appliance must support minimum two 40/100Gig SFP Slots and 8 * 10G SFP+ slots populated with 10Gig SR and same should be upgradeable to 25Gig by changing transceivers only.	This clause is favoring a spcific vendor and a specific model , since 25 G is not a generic connectivity used...We request to modify the clause as "The Appliance should have dedicated 1x1Gb port for management, 40/100Gig SFP Slots and 8 * 10G SFP+ ."	The Appliance must support minimum two 40/100G SFP Slots and 8 * 10G SFP+ slots populated with 10G SR with transrecievers
324	L4 Load balancer	104	Each Load balancer must have minimum 6 X 100G Ports and should be fully populated with associated MPO based multimode QSFPs. Ports should be usable as 4x10G ports or 4x25G or 1x40G or 1x50G using breakout cables	This clause is favoring a spcific vendor and a specific model as for load balancing 100 Gbps we only need maximum of 4 ports of 100 G NIC..We request to modify the clause as "Each Load balancer must have minimum 4 X 100G Ports and should be fully populated with associated MPO based multimode QSFPs. Ports should be usable as 4x10G ports or 4x25G or 1x40G or 1x50G using breakout cables"	6 X 100G is modified as 4 X 100G
325	Anti DDOS	285	8 x 10G SFP+ from day 1. 8 x 10Gig SR populated from day one and should be upgradeable to 25gig by changing transceivers only. The appliance should also support 40G ports for future use.	Since through asked is only for 10 Gbps maximum We request to modify the clause as "The Appliance should have dedicated 1x1Gb port for management and 8x10 GbE SFP+ ports."	8 x 10G SFP+ from day 1(one) 8 x 10G SR fully populated from day one
326	Anti DDOS	285	SSL TPS 50K with RSA 2k keys and 25K TPS with ECC with SSL throughput of 25 Gbps	DDOS is deployed at perimeter level and does not need to decrypt SSL traffic , This will impact performance and security compliance.We recommend to change this clause "Device should be able to mitigate SSL attack of maximum 10 GBPS traffic"	SSL TPS 50K with RSA 2k keys or 25K TPS with ECC with SSL throughput of 10 Gbps
327	Anti DDOS	286	Must have full Authoritative DNS capability to understand records like A, AAAA, CNAME, DNAME, HINFO, MX, NAPTR, NS, PTR, SOA, SRV, Should be able to do on the fly DNSSec.	Most of the DDOS solution act as stateless device and does not maintain sessions for all traffic, Mentioned features are favoring a specfic OEM that are not primary features required on DDOS appliance, We recommend to remove these clause	"deleted". Kindly refer revised Technical Specification
328	Anti DDOS	286	the product should convert DNS requests to DNSSec on the fly, should support 1)Delegated DNS and 2) Proxy DNS, supports an GUI integrated zone file management tool that simplifies.	Most of the DDOS solution act as stateless device and does not maintain sessions for all traffic, Mentioned features are favoring a specfic OEM that are not primary features required on DDOS appliance, We recommend to remove these clause	"deleted". Kindly refer revised Technical Specification
329	Anti DDOS	286	DNS Zone file management and reduce the risk of misconfiguration	Most of the DDOS solution act as stateless device and does not maintain sessions for all traffic, Mentioned features are favoring a specfic OEM that are not primary features required on DDOS appliance, We recommend to remove these clause	"deleted". Kindly refer revised Technical Specification
330	Anti DDOS	286	It shall provide a secure environment to manage DNS infrastructure while validating and error- checking zone files. It shall be built on the latest version of BIND.	Most of the DDOS solution act as stateless device and does not maintain sessions for all traffic, Mentioned features are favoring a specfic OEM that are not primary features required on DDOS appliance, We recommend to remove these clause	"deleted". Kindly refer revised Technical Specification

331	Anti DDOS	286	Should be able to define amount of memory for use of DNS caching	Most of the DDOS solution act as stateless device and does not maintain sessions for all traffic, Mentioned features are favoring a specfic OEM that are not primary features required on DDOS appliance, We recommend to remove these clause	"deleted". Kindly refer revised Technical Specification
332	IPS/IDS	Page No. 84	The IPS Solution should support Anti-malware protection through various engines as part of solution offerings.	Malware protection should be part of dedicated solution, it can't be clubbed with network protection device like NIPS. Known and unknown attacks like zero-day should be asked to provide wide protection against next gen attacks. **Suggested Clause:** **The IPS Solution should provide protection against zero-day attack without any manual intervention in less than 20 seconds.**	The IPS Solution should support Anti-malware protection/propogation through various engines as part of solution offerings.
333	IPS/IDS	Page No. 84	The IPS Solution should have real time emulation techniques for embedded malware protection.	Malware protection should be part of dedicated solution, it can't be clubbed with network protection device like NIPS. Known and unknown attacks should be asked to provide wide protection against next gen attacks. **Suggested Clause:** **The IPS Solution should provide protection known as well as unknown attacks.**	The IPS Solution should have real time emulation techniques for embedded malware protection/ propogation
334	IPS/IDS	Page No. 86	NIPS should support High Availability. It should support stateful HA such that state information is shared between the HA appliance. In case one of the appliances fails state is maintained.	IPS should be transparent in network so that attacker should not be able to identify its presence, state tabel information is relevant for statefull device not stateless. It should also have sufficient capacity to handle large attack request without any performance degradation. **Suggested Clause:** **NIPS should support High Availability. It should be stateless appliance with unlimited attacks concurrent sessions handling.**	NIPS should support High Availability.
335	IPS/IDS	Page No. 86	NIPS should support Active-Active high availability. The HA should be out of the box solution and should not require any third party or additional software for the same	Transparent appliance achieve failover by combining with other routing solution like router or firewall. Dual MNG port should be considered. **Suggested Clause:** **NIPS should support Active-Active high availability. 2x1G RJ45 MNG port should be out of the box**	NIPS should support Active-Active High Availability. It should not require any third party or additional software for the same
336	IPS/IDS	Page No. 87	NIPS solution should provide Intelligent security management: ■ Intelligent alert correlation and prioritization ■ Robust malware investigation dashboards ■ Preconfigured investigation workflows ■ Scalable web-based management	Malware protection should be part of dedicated solution, it can't be clubbed with network protection device like NIPS. Known and unknown attacks should be asked to provide wide protection against next gen attacks. **Suggested Clause:** **NIPS solution should provide Intelligent security management:** **■ Intelligent alert** **■ Web-based management**	NIPS solution should provide Intelligent security management: ■ Intelligent alert prioritization ■ Robust dashboards for investigation of attacks/Robust malware investigation dashboards ■ Preconfigured investigation workflows ■ web-based management
337	L4 Load Balancer	Page No. 104	Each Load balancer must have minimum 6 X 100G Ports and should be fully populated with associated MPO based multimode QSFPs. Ports should be usable as 4x10G ports or 4x25G or 1x40G or 1x50G using breakout cables	The asked port requirement is not inline with the throughput requirement. It can be catered with the cost effective solution, As per the asked throughput, 100G interfaces will unnecessary increase the cost of the solution. **Suggested Clause:** **The solution should be able to provide at least 6 x 40G QSFP+ interfaces and 12 x 10G SFP+ interfaces from day 1 . Dedicated 2x1G RJ45 Management Port and RJ45 Console Port.**	Kindly refer Revised Technical specification
338	L4 Load Balancer	Page No. 105	The proposed appliance should support minimum 595 Million packets per second (400X1.488) L4 concurrent connections at line rate, considering minimum packet size of 1500 Bytes.	Appliance should not be oversized, it will unnecessary increase the overall cost of the solution without any requirement. Almost OEMs publish concurrent data, pls consider the same. **Suggested Clause:** **The proposed appliance should support minimum 180 Million L4 concurrent connections**	The proposed appliance should support minimum 75 Million L4 concurrent connections

339	L4 Load Balancer	Page No. 105	New Clause Request	Next gen features like virtualization is missing, it must be added to create isolated environment from application and management perspective. **Suggested Changes:** **The proposed device should have Hypervisor Based Virtualization feature(that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. Should be capable of virtualization and support minimum 10 and scalable up to 50 virtual instances each virtual instance having dedicated resources including Management, Operating system and resources from day1**	As per Tender Document
340	L4 Load Balancer	Page No. 105	New Clause Request	Certification like EAL should be considered to choose right and reliable product for such critical data centre. **Suggested Clause:** **Appliance's software should be EAL2 certified**	As per Tender Document
341	Anti DDOS	Page No. 107	Anti DDOS and LLB functionalities. The solution must not be part of any UTM or NGFW or any white labelled or virtual solution running on third party hardware.	DDOS should always be a stateless appliance to effectively mitigate large attacks whereas LLB is a statefull appliance, both can't be clubbed together. **Suggested Clause:** **Anti DDOS functionalities. The solution must not be part of any UTM or NGFW or any white labelled or virtual solution running on third party hardware or any statefull appliance.** **Attack Concurrent Sessions: Unlimited**	and LLB deleted. Kindly refer revised Technical Specification
342	Anti DDOS	Page No. 107	10 Gbps of L7 Throughput	DDoS should be sized based on legit and attack throughput. **Suggested Clause:** **Legit Throughput: 10Gbps and scalable upto 40Gbps** **Attack Mitigation Throughput: 60Gbps**	10 Gbps of L7 Throughput or Legit Throughput: 10Gbps
343	Anti DDOS	Page No. 107	8 x 10G SFP+ from day 1. 8 x 10Gig SR populated from day one and should be upgradeable to 25gig by changing transceivers only. The appliance should also support 40G ports for future use.	Appliance should have sufficient port to cater current as well as future requirement, asking the 25G or 40G port is of no use as per throughput requirement. **Suggested Clause:** **12 x 10G SFP+ from day 1. 12 x 10Gig SR populated from day one and should be upgradeable to in total 24 x 10G SFP+ for future only.**	Kindly refer Revised Technical specification
344	Anti DDOS	Page No. 107	Dedicated1 x 1G RJ45 Out-of-band Management Port and RJ45 Console Port	As DDOS is a stateless appliance, it has only MNG port for management and reporting which should be redundant in nature. **Suggested Clause:** **Dedicated 2x1G RJ45 Management Port and RJ45 Console Port.**	As per Tender Document
345	Anti DDOS	Page No. 107	SSL TPS 50K with RSA 2k keys and 25K TPS with ECC with SSL throughput of 25 Gbps	SSL and PPS sizing should be sufficient to handle all technical requirements.Hence, request to ammend the clause. **Suggested Clause:** **Should support minimum 25 MPPS & minimum 90K TPS on RSA 2K Key**	Kindly refer Revised Technical specification
346	Anti DDOS	Page No. 107	Must have full Authoritative DNS capability to understand records like A, AAAA, CNAME, DNAME, HINFO, MX, NAPTR, NS, PTR, SOA, SRV, Should be able to do on the fly DNSSec.	Record resolution should be part of DNS server not DDOS.It can protect from DNS attacks as well as zero-day attacks. **Suggested Clause:** **Must protect from DNS attacks. Solution should also protect from zero-day using real time signature within 20sec automatically.**	kindly refer Revised Technical specification

347	Anti DDOS	Page No. 107	the product should convert DNS requests to DNSSec on the fly, should support 1) Delegated DNS and 2) Proxy DNS, supports an GUl integrated zone file management tool that simplifies.	Appliance should not work like DNS server, it is meant for DDoS protection. **Suggested Clause:** **Delete the clause**	Kindly refer Revised Technical specification
348	Anti DDOS	Page No. 107	DNS Zone file management and reduce the risk of misconfiguration	Appliance should not work like DNS server, it is meant for DDoS protection. **Suggested Clause:** **Delete the clause**	Kindly refer Revised Technical specification
349	Anti DDOS	Page No. 107	It shall provide a secure environment to manage DNS infrastructure while validating and error- checking zone files. It shall be built on the latest version of BIND.	Appliance should not work like DNS server, it is meant for DDoS protection. **Suggested Clause:** **Delete the clause**	Kindly refer Revised Technical specification
350	Anti DDOS	Page No. 107	Should be able to define amount of memory for use of DNS caching	Appliance should not work like DNS server, it is meant for DDoS protection. **Suggested Clause:** **Delete the clause**	Kindly refer Revised Technical specification
351	Anti DDOS	Page No. 108	The solution shall have built-in high availability (HA) features in the following mode: Active- Passive, Active-Active using standard VRRP or equivalent	VRRP is not relevant for stateless appliance like DDoS, DDoS should support clustering. **Suggested Clause:** **The solution shall have clustering features for HA**	The solution shall have built-in high availability (HA).
352	Anti DDOS	Page No. 109	The solution shall be able to support IPv4 & IPv6 routing protocols for traffic mitigation: Static Routing, OSPF Routing, BGPv4 Routing and Policy Based routing.	Routing is not relevant for stateless appliance like DDoS. **Suggested Clause:** **The solution shall be able to support IPv4 & IPv6 traffic mitigation along with L3-L7 mitigation.**	The solution shall be able to support IPv4 & IPv6 routing protocols for traffic mitigation
353	Anti DDOS	Page No. 109	Active-Active and Active- Passive Mode configuration, when deployed in dual mode and should have seamless takeover in- case if one device fails. Support in transparent failover between the devices, and support session mirroring, SSL mirroring, persistence mirroring, connection mirroring and heartbeat check.	Should be transparent in network so that attacker should not be able to identify its presence, state tabel information is relevant for statefull device not stateless. It should also have sufficient capacity to handle large attack request without any performance degradation. **Suggested Clause:** **Should support High Availability.**	Should support High Availability.
354	Anti DDOS	Page No. 109	The solution should provide online troubleshooting and traffic analysis tool where the administrator can take a snapshot of the config and upload it on web based diagnostic tool to check the health and vulnerability of the solution with the recommended solution provided on the knowledge base link.	Clause should be generic, using single OEM terminology is restrictive. **Suggested Clause:** **The solution should provide troubleshooting and traffic analysis as well as recommendation using knowledge base link.**	The solution should provide troubleshooting and traffic analysis

355	Load Balancer with WAF	Page No. 145	Must display a visual representation of authentication in the GUI. The Appliance must support minimum two 40/100Gig SFP Slots and 8 * 10G SFP+ slots populated with 10Gig SR and same should be upgradeable to 25Gig by changing transceivers only. The solution must be appliance based, 1U rack mountable and it should be having internal redundant Power Supply from day one.	Visual representation of authentication is of no use, system should alert admin. 100G port will unneccessary increase overall cost without any requirement. 1U is restrictive clause and does not create any advantages. **Suggested Clause:** **Must alert administrator.** **The Appliance must support minimum six 40 SFP+ Slots and 12 * 10G SFP+ slots populated with 10Gig SR.** **The solution must be appliance based, 1U/2U rack mountable and it should be having internal redundant Power Supply from day one.** **Dedicated 2x1G RJ45 Management Port and RJ45 Console Port.**	1U/2U agreed
356	Load Balancer with WAF	Page No. 148	New Clause Request	Next gen features like virtualization is missing, it must be added to create isolated environment from application and management perspective. **Suggested Changes:** **The proposed device should have Hypervisor Based Virtualization feature(that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. Should be capable of virtualization and support minimum 10 and scalable up to 50 virtual instances each virtual instance having dedicated resources including Management, Operating system and resources from day1**	as per tender document
357	Annexure 1 Technical Specificatio	117 and 179/1	Only the Manpower on OEM payrolls shall perform network planning, designing, implementation, integration and testing/validation for all Networking equipment(s) i.e. only direct OEM payroll manpower would be allowed to work on the project's designing, implementation & testing phase. An undertaking for same shall be provided.	we request you to please modify this clause as OEM/OEM Certified Partner on the proposed Technology and work experience should be binded to Technology experience rather than to OEM/OEM certified SI	as per tender document
358	Internal Firewall Clause	255/77	Throughput (Real World/Prod Performance) (All Features enabled)(Gbps) : 270 Gbps.	Please mention all the features to be enabled for example : Throughput (Real World/Prod Performance) with AVC/Application Control/App-ID, IPS, antivirus, antispyware and logging enabled : 300 Gbps	As per Tender Document
359	Internal Firewall Clause	255/77	75 Million Layer 4 sessions or 30 Million Layer 7 sessions	It is requested to please increase Concurrent Session/Concurrent Connection as throughput with all features enabled too high and amend this clause as below : 400 Million Layer 4 sessions or 150 Million Layer 7 sessions	As per Tender Document
360	Internal Firewall Clause	255/77	Minimum 600K Layer 4 sessions or Minimum 300K Layer 7 sessions	It is requested to please increase New session/Connection per second as throughput with all features enabled too high and amend this clause as below : Minimum 4 Million Layer 4 sessions or Minimum 2 Million Layer 7 sessions	As per Tender Document
361	Internal Firewall Clause	255/77	Layer3-Layer4, NAT, Application Visibility and Control (AVC), Next Generation Intrusion Prevention System (IPS)	As per Best Practices and Defense in Depth approach, Internal firewall will serve as a protective barrier between internal and external networks. It works by examining and filtering data using specific security modules. Malware and Anti-Virus protection is one of the most important tools to protect internal networks from Different Types of Malware. It is requested to please include malware protection and Anti-Virus protection also along with Layer3-Layer4, NAT, Application Visibility and Control (AVC), Next Generation Intrusion Prevention System (IPS) for enhanced protection. **Layer3-Layer4, NAT, Application Visibility and Control (AVC), Next Generation Intrusion Prevention System (IPS), Anti-Virus and Malware Protection from same OEM on premise without any dependency on cloud.**	As per Tender Document

362	Internal Firewall Clause	255	Application Visibility License, IPS License	"As per Best Practices and Defense in Depth approach, Internal firewall will serve as a protective barrier between internal and external networks. It works by examining and filtering data using specific security modules. Malware and Anti-Virus protection is one of the most important tools to protect internal networks from Different Types of Malware. It is requested to please include malware protection also along with Application Visibility License, IPS License and amend the clause as below : **Application Visibility License, IPS License, Anti-Virus and Anti malware protection.**	As per Tender Document
363	Internal Firewall Clause	255	5"Throughput (Real World/Prod Performance) (All Features enabled)(Gbps)"Throughput (Real World/Prod Performance) (All Features enabled)(Gbps) : 270 Gbps. 6IPsec ThroughputMinimum 240Gbps 7SSL Inspection Throughput200 Gbps or Higher 8"Concurrent Session/Concurrent Connection"75 Million Layer 4 sessions or 30 Million Layer 7 sessions 9"New session/Connection per second"Minimum 600K Layer 4 sessions or Minimum 300K Layer 7 sessions 10"Type of Interface Supported Multi- select"GECopper, 10GSFP+, QSFP+40G,GESFP, QSFP28 100G 11Port PopulationThe Firewall should have minimum 12 x 10GSFP+, 12 x 40G /100G QFSP 28. All the ports shall be fully Populated with respective Transceivers.	Please clarify if these performance perameters should be available in single unit of propsed solution or HA/Clustering/stacking of solution is permitted.	Performance parameters should be available in single unit
364	Annexure-1 (Technical Specifications)	179	f. Internet, Internal and Solution firewall should not be from offered networking OEM in this bid.	Please clarify if Firewalls can be proposed as blade/chassis in server/storage solutions.	As per Tender Document
365	Internet Firewall	260/82	Port population Should be supplied on day1 with 8x10GBase-SR Transceivers and 4 x100G Base-SR4 Transceivers	Request you to Please modify the clause as "**Should be supplied on day 1 with minimum 8*1G Copper, 24 x10G SFP+ with Base SR Transceivers and 4 x100G Base-SR4 Transceivers**" because Copper ports are also desired for the connectivity	As per Tender Document
366	Internet Firewall			It is requested to Please add **"Performance Validation - The bidder should submit the performance test report reference from public documents or Legal Attested Test Reports from Global Product Engineering department / Global Testing Department/ Global POC team of OEM certifying the mentioned performance and signed by Engineering/Product Management on the OEM Legal Letter Head in case Public Document/Datasheet does not have the reference. POC of the solution proposed may be done where the bidder/OEM will have to showcase all the technical features mentioned in the RFP"**	As per Tender Document
367	Solution Firewall			Please request to add **"URL Filtering Features : The proposed firewall should have full web payload analysis with deep learning CNN models, Machine Learning Powered domain analysis, fake captcha detection, HTML character encoding analysis, phishing redirection chain analysis and decoding enabled JavaScript engine to stop data exfiltration attacks from day1 "**	As per Tender Document
368	Solution Firewall			Please request to add **"DNS Security Features - The proposed firewall should have protection against DGA, Dynamic DNS, DOT, DOH, NXNS and DNS tunneling based attacks. The proposed Firewall should also have capability to detect DNS Misconfigurations, DNS Spoofing and DNS injection based attacks from day 1. Connector/Plugin based solution to achieve DNS security features will not be acceptable and no workaround on this will be accepted by the department"**	As per Tender Document

369	L4 Load balancer	104	Each Load balancer must have minimum 6 X 100G Ports and should be fully populated with associated MPO based multimode QSFPs. Ports should be usable as 4x10G ports or 4x25G or 1x40G or 1x50G using breakout cables	The ports asked for L4 load balancer solution is on the higher side considering other performance numbers of LB. Also the sine leaf switch is asked with 10G connectivity only not 100G with which the LB will be connected.. Therefore, in order to have more commercially viable solution, request you to change the clause to" **Each Load balancer must have minimum 8x10G SFP+ ports from day 1 and should support 40G ports for future scalability."**	Kindly refer Revised Technical specification
370	L4 Load balancer	105	The proposed appliance should support minimum 595 Million packets per second (400X1.488) L4 concurrent connections at line rate, considering minimum packet size of 1500 Bytes.	The sizing of the L4 load balancer solution's concurrent connections is on the much higher side considering other performance numbers of LB. Therefore, in order to have more commercially viable solution, request you to change the clause to **"The proposed appliance should support minimum 50 Million L4 concurrent connections per second"**	Kindly refer Revised Technical specification
371	L4 Load balancer	105	Additional point for credible solution	**Solutions Operating System should be tested and certified for EAL 2 / NDPP (Network Device Protection Profile)/NDcPP (Network Device collaborative Protection Profile)/ or above under Common Criteria Program for security related functions**	As per Tender Document
372	L4 Load balancer	105	Additional point for credible solution	**The proposed solution must support SSL VPN and Single Sign On functionality on same hardware solution running on same OS version from same OEM in future. Solution should be able to support robust endpoint posture inspection for every request-based application access instead of session-based application access and deny access for non-compliance endpoints. The Solution must support the following checks and has ability to define different security checks for different user groups:** *** Able to perform Antivirus/Malware software checks, including checks for Enabled State, Engine & Database version, Last Scan, and Last Update of the antivirus software.** *** The proposed VPN Solution shall have functionality to restrict copy & paste on RDP session and same should be configurable.** *** Able to perform Operating System, Windows Registry, File or Process checks.** *** Able to check if mobile devices have been jailbroken**	As per Tender Document
373	Anti DDOS	107	10 Gbps of L7 Throughput	The sizing of the Anti-DDOS solution is on the lower side considering RFP overall requirements and ERNET internet bandwidth traffic volume. Therefore, in order to have more robust solution, request you to change the clause to"**50 Gbps of L7 Throughput"**	Kindly refer Revised Technical specification
374	SSL VPN Gateway	108	The appliance should be dedicated SSL VPN Gateway and not a part of UTM/ firewall/ NGFW/ ADC device It should have should have 1x1GbE port for management and 8x10 SFP+ ports Should be populated with its transceivers	The sizing of the SSL VPN solution is on the higher side considering RFP overall requirements and ERNET userbase. Therefore, in order to have more commercially viable solution, request you to change the clause to **"The appliance should be dedicated SSL VPN Gateway and not a part of UTM/ firewall/ NGFW device It should have should have 1x1GbE port for management and 4x10 SFP+ ports Should be populated with its transceivers"**	Kindly refer Revised Technical specification
375	SSL VPN Gateway		The appliance should have multicore CPU, 64GB RAM, 1TB or higher HDD and dual power supply.	The sizing of the SSL VPN solution is on the higher side considering RFP overall requirements and ERNET userbase. Therefore, in oredr to have more commercially viable solution, request you to change the clause to **"The appliance should have multicore CPU, 64GB RAM, 450 GB or higher HDD and dual power supply."**	Kindly refer Revised Technical specification
376	SSL VPN Gateway		The solution Should have dedicated hardware SSL card and should support 35 Gbps of SSL Throughput	The sizing of the SSL VPN solution is on the higher side considering RFP overall requirements and ERNET userbase. Therefore, in oredr to have more commercially viable solution, request you to change the clause to **"The solution Should have dedicated hardware SSL card and should support 20 Gbps of SSL Throughput"**	Kindly refer Revised Technical specification

377	SSL VPN Gateway		The appliance should be capable of creating multiple virtual portals and support minimum 1000 concurrent users scalable to 10000 concurrent users on the same appliance without changing any hardware	The sizing of the SSL VPN solution is on the higher side considering RFP overall requirements and ERNET userbase. Therefore, in oredr to have more commercially viable solution, request you to change the clause to **"The appliance should be capable of creating multiple virtual portals and support minimum 1000 concurrent users scalable to 5000 concurrent users on the same appliance without changing any hardware"**	"The appliance should be capable of creating multiple virtual portals and support minimum 1000 concurrent users scalable to 5000 concurrent users on the same appliance without changing any hardware"
378	SSL VPN Gateway		The appliance should support 35 Gbps of compression throughput. This capability shall be compatible with most modern browsers, requiring no additional software.	The sizing of the SSL VPN solution is on the higher side considering RFP overall requirements and ERNET userbase. Therefore, in oredr to have more commercially viable solution, request you to change the clause to **"The appliance should support 20 Gbps of compression throughput. This capability shall be compatible with most modern browsers, requiring no additional software."**	Kindly refer Revised Technical specification
379	SSL VPN Gateway		Additional point for credible solution	**Solutions Operating System should be tested and certified for EAL 2 / NDPP (Network Device Protection Profile)/NDcPP (Network Device collaborative Protection Profile)/ or above under Common Criteria Program for security related functions**	As per Tender Document
380	Load balancer with WAF	145	All the features asked should be available from day one. Must support high availability.	Please elaborate the clause to specify the use cases required from high availability. Request you to change the clause to **"The solution shall be provided in High Availability in Active-Active and Active-Passive Mode configuration, when deployed in dual mode and should have seamless takeover in case if one device fails. It should also support in transparent failover between the devices, and support session mirroring, SSL mirroring, persistence mirroring, connection mirroring and heartbeat check. The solution must support N+1 architecture to provision more than 2 appliances in a HA cluster to acheive horizontal scaling"**	As per Tender Document
381	Load balancer with WAF	145	The solution should support 50K TPS 2K SSL or 25K TPS ECDHE-ECDSA P-256 SSL transactions per second.	The solution must support both RSA and ECC algorithms for SSL TPS as most of the appliactions are moving towards ECC from RSA now a days. Therefore, request you to change the clause to **"The solution should support 50K TPS 2K SSL and 25K TPS ECDHE-ECDSA P-256 SSL transactions per second."**	As per Tender Document
382	Load balancer with WAF	145	In the RFP, there are no technical specifications of Web application firewall for application security. Hence for robust WAF solution, request you to add this additional clause to WAF section	**The solution should provide OWASP Compliance Dashboard which provides holistic and interactive interface that clearly measures app's compliancy against the Application Security Top 10 attacks and also provide suggestions/shortcuts to address the compliances and configure policies for it.**	As per Tender Document
383	Load balancer with WAF	145	In the RFP, there are no technical specifications of Web application firewall for application security. Hence for robust WAF solution, request you to add this additional clause to WAF section	**A given user must be enforced to follow a sequence of pages while accessing without any script and should have provision to apply the restriction to the application or part of the application based on Geo Location**	As per Tender Document
384	Load balancer with WAF	145	In the RFP, there are no technical specifications of Web application firewall for application security. Hence for robust WAF solution, request you to add this additional clause to WAF section	**The Solution must protect against HTTP, HTTPS and Application layer DOS and DDOS attacks including stress-based DOS and Heavy URL attacks. The solution must support all the common web application vulnerability assessment tools (Web application scanners) including Acunetix, Qualys, Rapid 7, IBM Appscan, etc (or) Equivalent Gartner vulnerability assessment tools to virtually patch web application vulnerabilities. Necessary logs to be generated for audit and compliance.**	As per Tender Document
385	Load balancer with WAF	145	In the RFP, there are no technical specifications of Web application firewall for application security. Hence for robust WAF solution, request you to add this additional clause to WAF section	**The solution must support the configuration to allow some pages in a web application to be in blocking mode and some pages to be in detection / learning mode. The solution must allow the re-learning of an application profile on a per-URL or per-page basis. The administrator should not be required to relearn the entire application when only a few pages have changed.**	As per Tender Document

386	Load balancer with WAF	145	In the RFP, there are no technical specifications of Web application firewall for application security. Hence for robust WAF solution, request you to add this additional clause to WAF section	**The solution should have pre-built templates for well-known applications attack signatures eg, ActiveSync, SAP, Oracle Applications/Portal. Solution should have the ability to build a base policy and inherit child policies from the same. Inheritance should support restricting modifications to the base policy settings**	As per Tender Document
387	Load balancer with WAF	145	In the RFP, there are no technical specifications of Web application firewall for application security. Hence for robust WAF solution, request you to add this additional clause to WAF section	**Proposed WAF Solution should have functionality to showcase how many URLs in the application have been completely learned & move them into Protection Mode automatically i.e. some URLs to be in learning mode & some URLs in the Protection Mode of the same Application**	As per Tender Document
388	Load balancer with WAF	145	In the RFP, there are no technical specifications of Web application firewall for application security. Hence for robust WAF solution, request you to add this additional clause to WAF section	**System should support inbuilt ability to encrypt the user credentials in real time at the browser level (data at rest) before the traffic hits the network so as to protect the credentials especially password, Aadhar number or any other sensitive parameter to protect from cyber actors, key loggers and credential stealing malware residing in the end user's browsers. Necessary logs to be generated for audit and compliance.**	As per Tender Document
389	Load balancer with WAF	145	In the RFP, there are no technical specifications of Web application firewall for application security. Hence for robust WAF solution, request you to add this additional clause to WAF section	**The solution must distinguish between browsers and bots which are able to execute Java script by using advanced techniques such as browser capability challenge and CAPTCHA challenge to do device fingerprinting.The Solution should have inbuilt ability within the appliance (without accessing the internet/cloud service) to generate and issue CAPTCHA to challenge suspicious clients. Should provide PCIDSS compliance requirements for web application servers. Necessary logs to be generated for audit and compliance.**	As per Tender Document
390	Load balancer with WAF	145	In the RFP, there are no technical specifications of Web application firewall for application security. Hence for robust WAF solution, request you to add this additional clause to WAF section	**POSITIVE and NEGATIVE SECURITY MODEL should have advanced behavior-analysis technologies to separate malicious threats from legitimate traffic. The administrators should be able to see all the signatures and not just the signature categories. Admins can apply Specific signatures to specific policies**	As per Tender Document
391	Load balancer with WAF	145	In the RFP, there are no technical specifications of Web application firewall for application security. Hence for robust WAF solution, request you to add this additional clause to WAF section	**The solution must be able to block transactions with content matching known attack signatures while allowing everything else.The solution should also have an option to put a signature in staging mode. Meaning that the system applies the attack signatures to the web application traffic, but does not apply the blocking policy action to requests that trigger those attack signatures.**	As per Tender Document
392	Load balancer with WAF	145	In the RFP, there are no technical specifications of Web application firewall for application security. Hence for robust WAF solution, request you to add this additional clause to WAF section	**Proposed WAF Solution should have capability to automatic learning should include Directories, URLs, Form Field Values, Whether the field values is numeric/alphanumeric/alphabets, length of the field etc. Solution should support different profiling like different values like Directories, URLs, Form Field Values, Metacharacters etc. for different applications.**	As per Tender Document
393	Load balancer with WAF	145	In the RFP, there are no technical specifications of Web application firewall for application security. Hence for robust WAF solution, request you to add this additional clause to WAF section	**WAF solution should have GraphQL content profile and policy template and attack signatures on GraphQL traffic**	As per Tender Document
394	Load balancer with WAF	145	In the RFP, there are no technical specifications of Web application firewall for application security. Hence for robust WAF solution, request you to add this additional clause to WAF section	**The solution must protect against FTP, SMTP, HTTP, HTTPS and Application layer Dos and DDOS attacks including stress based DOS and Heavy URL attacks.**	As per Tender Document

395	Load balancer with WAF	145	In the RFP, there are no technical specifications of Web application firewall for application security. Hence for robust WAF solution, request you to add this additional clause to WAF section	**The proposed solution must support SSL VPN and Single Sign On functionality on same hardware solution running on same OS version from same OEM in future. Solution should be able to support robust endpoint posture inspection for every request-based application access instead of session-based application access and deny access for non-compliance endpoints. The Solution must support the following checks and has ability to define different security checks for different user groups:** *** Able to perform Antivirus/Malware software checks, including checks for Enabled State, Engine & Database version, Last Scan, and Last Update of the antivirus software.** *** The proposed VPN Solution shall have functionality to restrict copy & paste on RDP session and same should be configurable.** *** Able to perform Operating System, Windows Registry, File or Process checks.** *** Able to check if mobile devices have been jailbroken**	As per Tender Document
396	Load balancer with WAF	145	In the RFP, there are no technical specifications of Web application firewall for application security. Hence for robust WAF solution, request you to add this additional clause to WAF section	**WAF must provide inbuilt capability of API security including support for uploading swagger file and protect leakage of user credentials accessing the web applications using HTML field Obfuscation to protect against malware-based attacks and the solution should have capability to protect Credential Attacks that can steal credentials from the user's browser to avoid cyber exploits. It should be able to authenticate users based on browser type and version, operating system type and version. Necessary logs to be generated for audit and compliance.**	As per Tender Document
397	Load balancer with WAF	145	In the RFP, there are no technical specifications of Web application firewall for application security. Hence for robust WAF solution, request you to add this additional clause to WAF section	**Solution should able to Imported OpenAPI file automatically and configures policy with all API specific parameters as a list of allowed URLs, parameters, methods, and so on.Solution should have API security template which pre-configures WAF policy with all necessary violations and signatures to protect API backend.**	As per Tender Document
398	Load balancer with WAF	145	In the RFP, there are no technical specifications of Web application firewall for application security. Hence for robust WAF solution, request you to add this additional clause to WAF section	**The solution should address and mitigate the OWASP Top 10 API security vulnerabilities. Solution should support reverse engineering for API Schema via Learning mode, should able to Discover New API Paths/ Shadow paths/ Stale API Paths/ Authenticated Paths/ Unauthenticated Paths.**	As per Tender Document
399	Remote Firewall	179/1	Remote Firewalls should be from Internal Firewall OEM	Please relax this clause and make it generic so that other leading OEMs can also participate in the BOQ Annexure components defined from security posture standpoint both for DC, DR and Remote Sites	As per Tender Document
400	Annexure 1 Technical Specifications Clause Number : l	117 and 179/1	**Clause -** Note 5 : OEM Specialist (such as OEM Security/ Network/ Server Specialist etc.) must be on OEM's Payroll with minimum 5-year experience and **Another Clause :** Only the Manpower on OEM payrolls shall perform network planning, designing, implementation, integration and testing/validation for all Networking equipment(s) i.e. only direct OEM payroll manpower would be allowed to work on the project's designing, implementation & testing phase. An undertaking for same shall be provided.	Please allow OEM recommended and Certified Partners/MSIs in the defined ManPower clause for Network Planning, design, implementation and other defined scope instead of OEM Manpower. OEM recommended and Certified Partner/MSI resources are trained on the proposed technology with relevant product certifications and those specific inclusions can be amended/added in the existing clause. Costing of OEM Manpower Resources is a substantial amount and huge cost implications to the overall project cost	as per tender document
401	Internal Firewall	255/77	Traffic handled : TCP, UDP, HTTP/TCP	Please modify the clause to include ONLY HTTP/HTTPs in the defined Traffic mix benchmarking as it has been defined for other Set of Solution/Application Firewalls and make the clause as "**Traffic handled : HTTP/HTTPs**" . NGFW Firewall benchmarking varies with the kind of traffic mix taken into while computation is performed. Hence, Layer 7 traffic mix of HTTP/HTTPs benchmarking will ensure no performance bottleneck in case of any traffic mix variation	TCP, UDP, HTTP/HTTPS

402	Internal Firewall	255/77	Packet Size : 1024 Bytes or 64KB HTTP/application-mix/Enterprise Mix	Please modify the clause to include ONLY HTTP/HTTPs transaction size as it has been defined for other Set of Solution/Application Firewalls and make the clause as "**Packet Size : 64KB HTTP/HTTPs**" . NGFW Firewall benchmarking varies with the transaction size taken into while computation is performed. Hence, Layer 7 traffic mix of HTTP/HTTPs and baseline Transaction size benchmarking will ensure no performance bottleneck in case of any traffic mix and packet size variations	As per Tender Document
403	Internal Firewall	255/77	Throughput (Real World/Prod Performance) (All Features enabled)(Gbps) : 270 Gbps.	**Please mention all the features to be enabled for example : Throughput (Real World/Prod Performance) with AVC/Application Control/App-ID, IPS, antivirus, antispyware, Sandboxing, file blocking, and logging enabled : 90 Gbps**. Throughput consideration earlier were defined same for both the traffic mix/packet size categories. Please change this to minimum 90 Gbps considering 64KB HTTP traffic mix	As per Tender Document
404	Internal Firewall	255/77	IPsec Throughput : Minimum 240Gbps	**Please modify the IPsec Throughput : Minimum 100Gbps considering the same traffic mix and HTTP packet size defined above** because Throughput consideration earlier were defined same for both the traffic mix/packet size categories	IPsec Throughput : Minimum 240 Gbps at layer 4 and Minimum185 Gbps at layer 7
405	Internal Firewall	255/77	SSL Inspection Throughput 200 Gbps or Higher	Please remove this clause as SSL inspection is not performed on the Internal Firewall considering the components defined in the BOQ annexure	SSL Inspection Throughput 150 Gbps or Higher
406	Internal Firewall	256/78	Virtual Domain minimum 10 and scalable to 300	Please modify the clause as **Virtual Domain minimum 25 from day 1 and scalable to 200** as 300 is OEM specific and does not allow wider OEM participation	Virtual Domain minimum 10 and scalable to 200
407	Internal Firewall	256/78	Onboard storage : 4 TB SSD or higher	Please modify the clause as "**480 GB SSD or higher** " as defined storage is OEM specific clause	Onboard storage : 3 TB or higher
408	Solution Firewall	258/80	Details of the Firewall Policies for the Firewall provided with the License : Application Visibility License, IPS License, URL Filtering and DNS Security with features listed in the specifications	Please include **URL Filtering License and DNS Security License from day 1** provisioned on the Solution Firewalls for advanced security posture against zero day attack vectors	As per Tender Document
409	Solution Firewall			**Request to add** "URL Filtering Features : The proposed firewall should have full web payload analysis with deep learning CNN models, Machine Learning Powered domain analysis, fake captcha detection, HTML character encoding analysis, phishing redirection chain analysis and decoding enabled JavaScript engine to stop data exfiltration attacks from day1" **Justification -** NGFW appliance should not just be whitelisting /blackilisting URLs with few phishing/credential theft detection mechanisms. NGFW should have advanced engines to do the full web payload analysis including HTTP, HTML character encoded data attributes, etc. Fake Captcha and other web crawling based attacks are also prevalent these days. Hence, Requested features should be included in the current feature ask from better security efficacy of the solution	As per Tender Document
410	Solution Firewall			**Request to add** "DNS Security Features - The proposed firewall should have protection against DGA, Dynamic DNS, DOT, DOH, NXNS and DNS tunneling based attacks. The proposed Firewall should also have capability to detect DNS Misconfigurations, DNS Spoofing and DNS injection based attacks from day 1. Connector/Plugin based solution to achieve DNS security features will not be acceptable and no workaround on this will be accepted by the department" **Justification -** DNS Based attacks are very advanced these days and respective detection/remediaton modules should have capabilities to detect such advanced attack vectors so that compromise/breach can be prevented at an early stage with these requested advanced DNS security capabilities	As per Tender Document

411	Solution Firewall			**Request to add** "Performance Validation - The bidder should submit the performance test report reference from public documents or Legal Attested Test Reports from Global Product Engineering department / Global Testing Department/ Global POC team of OEM certifying the mentioned performance and signed by Engineering/Product Management on the OEM Legal Letter Head in case Public Document/Datasheet does not have the reference. POC of the solution proposed may be done where the bidder/OEM will have to showcase all the technical features mentioned in the RFP practically. If bidder/OEM fails to showcase any technical feature mentioned in the RFP, then their bid will be rejected" **Justification** - This will ensure that defined benchmarking and feature ask should be met in the proposed Firewall appliance without any compromise on the requested ask in case the submitted reference/documentation does not comply to the stated ask	As per Tender Document
412	Internet Firewall	260/82	Port population Should be supplied on day1 with 8x10GBase-SR Transceivers and 4 x100G Base-SR4 Transceivers	Please modify the clause as "**Should be supplied on day 1 with minimum 8*10G Copper, 24 x10G SFP+ with Base-SR Transceivers and 4 x100G Base-SR4 Transceivers**" because Copper ports are also desired for the connectivity considering uplink/downlink connections including higher number of 10G SFP+ ports	As per Tender Document
413	Internet Firewall	260/82	Details of the Firewall Policies for the Firewall provided with the License : Application Visibility License, IPS License, URL Filtering and DNS Security with features listed in the specifications	Please include **URL Filtering License and DNS Security License from day 1** provisioned on the Internet Firewalls for advanced security posture against zero day attack vectors	As per Tender Document
414	Internet Firewall			**Request to add** "URL Filtering Features : The proposed firewall should have full web payload analysis with deep learning CNN models, Machine Learning Powered domain analysis, fake captcha detection, HTML character encoding analysis, phishing redirection chain analysis and decoding enabled JavaScript engine to stop data exfiltration attacks from day1" **Justification -** NGFW appliance should not just be whitelisting /blackilisting URLs with few phishing/credential theft detection mechanisms. NGFW should have advanced engines to do the full web payload analysis including HTTP, HTML character encoded data attributes, etc. Fake Captcha and other web crawling based attacks are also prevalent these days. Hence, Requested features should be included in the current feature ask from better security efficacy of the solution	As per Tender Document
415	Internet Firewall			**Request to add** "DNS Security Features - The proposed firewall should have protection against DGA, Dynamic DNS, DOT, DOH, NXNS and DNS tunneling based attacks. The proposed Firewall should also have capability to detect DNS Misconfigurations, DNS Spoofing and DNS injection based attacks from day 1. Connector/Plugin based solution to achieve DNS security features will not be acceptable and no workaround on this will be accepted by the department" **Justification -** DNS Based attacks are very advanced these days and respective detection/remediaton modules should have capabilities to detect such advanced attack vectors so that compromise/breach can be prevented at an early stage with these requested advanced DNS security capabilities	As per Tender Document

416	Internet Firewall			**Request to add** "Performance Validation - The bidder should submit the performance test report reference from public documents or Legal Attested Test Reports from Global Product Engineering department / Global Testing Department/ Global POC team of OEM certifying the mentioned performance and signed by Engineering/Product Management on the OEM Legal Letter Head in case Public Document/Datasheet does not have the reference. POC of the solution proposed may be done where the bidder/OEM will have to showcase all the technical features mentioned in the RFP practically. If bidder/OEM fails to showcase any technical feature mentioned in the RFP, then their bid will be rejected" **Justification** - This will ensure that defined benchmarking and feature ask should be met in the proposed Firewall appliance without any compromise on the requested ask in case the submitted reference/documentation does not comply to the stated ask	As per Tender Document
417	IPS/IDS	83	**Suggestion for addition** Number of signatures supported by the offered product as "20000 or more".	**Justifcation for addition** "More numbers of signatures will provide better detection and prevention coverage capabilities against modern day attackers hence this will increase the effictiveness of NIPS	As per Tender Document
418	IPS/IDS	83	The appliance should have below port density:- 1. Fixed 8 - 1G copper ports with/without fail open. 2. 4 - 10G SFP+ ports with/without internal fail open. 3. Fixed 2 - 10G SFP+ ports. 4 All the ports shall be fully populated with its transceivers only	Please add more 10G ports from future scalability and **modify clause as below** The appliance should have below port density:- 1. Fixed 8 - 1G copper ports with/without fail open. 2. 8 - 10G SFP+ ports with/without internal fail open. 3. Fixed 2 - 10G SFP+ ports. 4 All the ports shall be fully populated with its transceivers only	As per Tender Document
419	IPS/IDS	35/83	**Add clause** Proposed solution should participated in Miercom security assessment test of IPS and score more then 99% in IPS exploit detection test.	**Justification** It is highly advisable to have 3rd Party independent like Miercom which is industry leading report for security effictiveness proof so to proof the NIPS have negligable false positives detection and unnecessary alerting	As per Tender Document
420	IPS/IDS	83	Solution must support SSL throughput of 5 Gbps from day 1.	Please increase the SSL throughput tom 8 Gbps from a future scalability standpointm of 5 years ,**Modify the clause as below** Solution must support SSL throughput of 5 Gbps and scalable upto 8 Gbps on the same appliance	As per Tender Document
421	IPS/IDS	83	**Suggestion for addition** Solution must do emaulation for embedded malware for PDF and Javascipts on the same appliance	**Justification of addition** As most of the hidden malwares are propagated using Javascript and PDF files hence **it is requested to add** "Solution must do emulation of PDF and Javascript to introspect hidden threatson the same appliance "	As per Tender Document
422	SSL VPN	Annexure-1 (Technical Specifications) SSL VPN Gateway	The device should support on demand provisioning of L3 VPN client using ActiveX or JAVA applet, standalone and command line L3 VPN client support	Justification: Both ActiveX by Microsoft and Java applet from Oracle have been deprecated due serious security issues. The Browser based clients should not be built using ActiveX or JAVA applet. Suggestive Clause: The device should support browser based VPN access, standalone and command line L3 VPN client for Windows, Mac, Linux, iOS and Android.	The device should support on demand provisioning of L3 VPN client using standalone and command line L3 VPN client support

423	Load balancer with WAF	Annexure-1 (Technical Specifications) Load balancer with WAF (ADC)	The solution must be appliance based, 1U rack mountable and it should be having internal redundant Power Supply from day one.	**Justification:** The clause specifies a 1U rack-mountable appliance with internal redundant power supply. However, the problem highlights the need for a high number of ports and high throughput, which may require more space and better cooling. A 2U rack is suggested to accommodate these requirements without compromising performance or reliability. **Suggestive Clause:** The solution must be a 2U rack-mountable appliance with internal redundant power supply, ensuring support for high port density and throughput requirements from day one.	Kindly refer Revised Technical specification
424	Load balancer with WAF	Load balancer with WAF (ADC)	Suggestive Clause	**Justification:** the proposed solution should offers flexibility and adaptability, enabling custom traffic management decisions based on real-time events. By supporting a scripting language, it allows for the creation of tailored rules to optimize application performance, handle dynamic scenarios, and meet specific operational requirements effectively. **Suggestive Clause:** The proposed solution should support scripting language for events based rules creation to make traffic management decision using scripting language.	As per Tender Document
425	Load balancer with WAF	Load balancer with WAF (ADC)	Suggestive Clause	**Justification:** The proposed solution should support limiting user sessions (cookies) per application or virtual server. This feature ensures that when the number of active sessions reaches the configured limit, new users are blocked from accessing the application. This helps maintain the availability and performance of web/app servers, allowing already logged-in users to complete their transactions without degradation in service. **Suggestive Clause:** The proposed solution should support limitation of users sessions (cookies) per application/vserver. Through this feature, SLB shall insure that new user (beyond the configured threshold limit) get blocked, so as to insure availability of resources on WEB / APP servers already logged in users to complete their transactions.	As per Tender Document
426	Load balancer with WAF	Load balancer with WAF (ADC)	Suggestive Clause	**Justification:** Including an anti-bot SDK for mobile applications ensures comprehensive protection for both mobile apps and Web APIs, safeguarding against automated attacks like credential stuffing and data scraping. By using an SDK from the same OEM as the WAF, seamless integration and consistent threat intelligence across platforms are achieved, enhancing security efficacy while simplifying deployment and management. **Suggestive Clause:** The solution should support anti-bot SDK for mobile application for protecting mobile apps and Web APIs. The anti-bot mobile SDK should be available for Android and iOS and should be from same OEM as WAF	As per Tender Document

427	Anti DDOS	Anti-DDoS	Suggestive Clause	**Justification:** Anti-DDoS solution with advanced score-based traffic shaping leverages machine learning, built-in signatures, and user-defined rules to provide dynamic, adaptive protection. Machine learning enables real-time detection and mitigation of both known and emerging threats, while score-based traffic shaping prioritizes legitimate traffic and limits malicious traffic, ensuring minimal disruption. The combination of these elements enhances threat intelligence, resource efficiency, and customization, making the solution effective against increasingly sophisticated DDoS attacks and adaptable to future challenges. **Suggestive Clause:** The proposed solution should have advanced score based traffic shaping where score is computed from machine-learning, built-in signatures and user defined rules	As per Tender Document
428	L4 Load balancer	L4 Load balancer in HA	Suggestive Clause	**Justification:** Link load balancing solution with a DNS firewall feature enhances network security by blocking access to known malicious domains. This helps prevent threats such as phishing, malware downloads, and command-and-control communications, protecting users and infrastructure while maintaining optimal network performance. Integrating a DNS firewall ensures proactive threat prevention and improves overall network resilience. **Addditional Clause:** The proposed solution should have DNS firewall feature to block malicious domains	As per Tender Document
429	L4 Load balancer	L4 Load balancer in HA	Suggestive Clause	**Justification:** The proposed solution supports caching (static and dynamic) to store frequently accessed content closer to users, reducing server load and improving response times. It also enables gzip and deflate compression to shrink data sizes, saving bandwidth and speeding up content delivery. Together, these features optimize application performance and user experience. **Suggestive Clause:** The proposed solution should support caching (static & dynamic) and compression (gzip & deflate) for improving application performance and saving bandwidth	As per Tender Document
430	SIEM	44	2) Training: Contractor Shall provide the training for installation, operation and maintenance of supplied equipment(s) as detailed in Section-VII/ BoM. Note: OEM based training is required on each of the supplied products/equipment /solutions, Further, on overall solution, contractor's Subject Matter Experts may provide the training.	Please clarify the training scope of work is inline with Training section mentioned @ page # 98	Product training after installation will be given by the OEM as per tender document
431	SIEM	68	2 OEM Security Specialist	You have asked for OEM security speclist in New DC & DR Please clarify, Which solutions is OEM security specialist required? Does solution listed at serial#46 in Bill of material also need to be supplied with OEM sedurity specialist?	The Three (03) OEM Security Specialist each at DC & DR asked in the bid should be supplied as follows . One each OEM Security Specialist for respective OEMs of the following solution/hardware : 1. " Enterprise Data Log Analytics Management with Application & Infrastructure Monitoring Solution " , 2. Internal Firewall 3. IPS/IDS

432	SIEM	79	Training with Certification from Authorized Certification Bodies	Training asked is for generic industry certifications. Is there any OEM Product specific training required to be delivered.	As per tender document
433	SIEM	86-87	Following equipment(s) OEMs whose products have been offered in the bid shall have Technical Assistance Centre (TAC) in India. OEM shall have dedicated / Toll Free Number for TAC to support the equipment. OEM(s) should have direct presence with their own office in India. Relevant documentary proof (i.e. Registration/Incorporation Certificate, Self-certification of TAC availability and Dedicated/Toll free number) should be submitted.	Different OEM's have their distinct ways of support. We understand the requirements of TAC center and support staff based out if India. Due to the global nature of product support and timezones, organization typically adhere to the "Follow the Sun" approach supporting customers globally. This appriach is successfull as there is seamless coverage across 24x7x365 without any dependence on one support person. Escalation path also becomes easier. In this regards, we would like to request for a change in clause to ensure the clause to ensure the OEM's are given flexibility to provide a high quality skilled support across 24 hours without any issues	Following equipment(s) OEMs whose products have been offered in the bid shall have Technical Assistance Centre (TAC)/Support Center in India. OEM(s) should have direct presence with their own office in India. Relevant documentary proof (i.e. Registration/Incorporation Certificate, Self-certification of TAC/Support Center availability) should be submitted.
434	Anti DDoS	285	10 Gbps of L7 Throughput	We request to you to change the Clause as - **10 Gbps of L7 Throughput and upgradable to 20 Gbps on the same platform without changing H/w and should be stateless in architecture supporting 80 Million packet per seconds flood prevention rate on the same appliance.. Device should not have any limit in storing L4 and L7 connections and should not be part of LB, LLB, WAF, IPS or Proxy to prevent state exaustion attacks**	Kindly refer Revised Technical specification
435	Anti DDoS	285	8 x 10G SFP+ from day 1. 8 x 10Gig SR populated from day one and should be upgradeable to 25gig by changing transceivers only. The appliance should also support 40G ports for future use.	We request to you to change the Clause as - "**8 x 10G SFP+ SR populated with internal bypass support from day . The appliance should also support replacement/upgrade of NIC to 40G and 100 G ports for future use**."	Kindly refer Revised Technical specification
436	Anti DDoS	285	SSL TPS 50K with RSA 2k keys and 25K TPS with ECC with SSL throughput of 25 Gbps	We request to change clause as **" SSL TPS of 25K TPS with ECC and should support capability to consume and integrate with 3rd Party feeds (IOCs) via STIX/TAXII inbuilt integration capability along with its own internal feeds(no third party). The Appliance should support more then 3 million IOCs blocking combined and should block such threats at the entry itself being at the extreme parimeter not allowing such malicious IPs to come inside the DC network."**	Kindly refer Revised Technical specification
437	Anti DDoS	286	The traffic Auto learning threshold can be apply automatically after auto learning completed.	We request you to change the clause as **" The traffic Auto learning threshold should be applied manually post understanding its impact on the production traffic after auto learning completed.**	The traffic Auto learning threshold can be applied manually/ automatically after auto learning completed.
438	Anti DDoS	286	Must have full Authoritative DNS capability to understand records like A, AAAA, CNAME, DNAME, HINFO, MX, NAPTR, NS, PTR, SOA, SRV, Should be able to do on the fly DNSSec.	**We request you to remove these points as they are part of LLB**	Kindly refer Revised Technical specification
439	Anti DDoS	286	the product should convert DNS requests to DNSSec on the fly, should support 1) Delegated DNS and 2) Proxy DNS, supports an GUl integrated zone file management tool that simplifies.	**We request you to remove these points as they are part of LLB**	Kindly refer Revised Technical specification
440	Anti DDoS	286	DNS Zone file management and reduce the risk of misconfiguration	**We request you to remove these points as they are part of LLB**	Kindly refer Revised Technical specification
441	Anti DDoS	286	It shall provide a secure environment to manage DNS infrastructure while validating and error- checking zone files. It shall be built on the latest version of BIND.	**We request you to remove these points as they are part of LLB**	Kindly refer Revised Technical specification
442	Anti DDoS	286	Should be able to define amount of memory for use of DNS caching	**We request you to remove these points as they are part of LLB**	Kindly refer Revised Technical specification
443	Anti DDoS	286	The solution shall have built-in high availability (HA) features in the following mode: Active- Passive, Active-Active using standard VRRP or equivalent	Request you to change the clause as **" The solution should be deployed in the Active Active or Active passive design and should be stateless along with should support capability to consume and integrate with 3rd Party feeds (IOCs) via STIX/TAXII inbuilt integration capability along with its own internal feeds(no third party). The Appliance should support more then 3 million IOCs blocking combined and should block such threats at the entry itself being at the extreme parimeter not allowing such malicious IPs to come inside the DC network."**	Kindly refer Revised Technical specification

444	Anti DDoS	287	The solution shall be able to support IPv4 & IPv6 routing protocols for traffic mitigation: Static Routing, OSPF Routing, BGPv4 Routing and Policy Based routing.	We request you to remove this point as DDoS are stateless and do not support routing protocols	Kindly refer Revised Technical specification
445	Anti DDoS	287	Active-Active and Active- Passive Mode configuration, when deployed in dual mode and should have seamless takeover in- case if one device fails. Support in transparent failover between the devices, and support session mirroring, SSL mirroring, persistence mirroring, connection mirroring and heartbeat check.	Request you to change the clause as **" The solution should be deployed in the Active Active or Active passive design and should be stateless along with should support capability to consume and integrate with 3rd Party feeds (IOCs) via STIX/TAXII inbuilt integration capability along with its own internal feeds(no third party). The Appliance should support more then 3 million IOCs blocking combined and should block such threats at the entry itself being at the extreme parimeter not allowing such malicious IPs to come inside the DC network."**	Kindly refer Revised Technical specification
446	Anti DDOS	288	Solutions Operating System should be tested and certified for EAL 2 / NDPP (Network Device Protection Profile)/NDcPP (Network Device collaborative Protection Profile)/ or above under Common Criteria Program for security related functions	Request you to change the clause as **" Solutions Operating System should be tested and certified for EAL 2 / NDPP (Network Device Protection Profile)/NDcPP (Network Device collaborative Protection Profile)/ or above under Common Criteria Program for security related functions or The OEM should provide 3 Govt/BFSI customer references in India**	As per Tender Document
447	Anti DDOS		Missing critical function of Anti DDOS	**DDoS solution should be stateless to mitigate TCP / Protocol Exhaustion attacks and should support capability to consume and integrate with 3rd Party feeds (IOCs) via STIX/TAXII inbuilt integration capability along with its own internal feeds(no third party). The Appliance should support more then 3 million IOCs blocking combined and should block such threats at the entry itself being at the extreme parimeter not allowing such malicious IPs to come inside the DC network."**	As per Tender Document
448	Anti DDOS		Missing critical availability funciton of Anti DDOS	**The appliance should support Hardware and Software Bypass Capability with both fail open and fail closed modes in all protection ports (including Copper and Fiber). The hardware bypass for all protection interface types (Copper and Fiber) should have In-Built in the Appliance without the need of any external bypass switch**	As per Tender Document
449	Anti DDOS		Missing critical sizing parameter of Anti DDOS appliance which is flood prevention rate	**Proposed appliance should support minimum of 80 Million packet per seconds flood prevention rate on the same appliance. This performance figure must be mentioned in public facing datasheet.**	As per Tender Document
450	Anti DDOS		Missing critical function of Anti DDOS	**OEM Anti-DDoS Solution should be deployed and used by at least 4 Gov/PSU/BFSI customer in India to protect their own Core infrastructure from DDoS attacks and proposed solution should support native Integration with ISP clean pipe for preventing the volumetric attacks. In case of volumetric attack on premise DDos solution should send signal to the ISP Scrubbing centre for automated scrubbing at the ISP level . Auto signalling should be supported with atleast 4 Tier 1 ISPs Clean pipe services in India**	As per Tender Document
451	Anti DDOS		Missing critical function of Anti DDOS	**Supports over 3 Million IOC Blocking via integration with 3rd Party TIP using STIX/TAXII protocols without any API integration**	As per Tender Document
452	Anti DDOS		Missing critical function of Anti DDOS	**DDoS Appliance must not have any limitations in handling the number of concurrent session for DDoS attack traffic - Knowing nature of solution and should be clearly mentioned in public facing datasheet. It should not maintain session table for authenticated / legitimate sessions.**	As per Tender Document
453	Anti DDOS		Missing critical function of Anti DDOS	**System must have an In-Built and In House updated IP reputation feed that has IOC for Active DDoS vectors, Botnets, etc. that are actively propagating DDoS attack vectors anywhere in the world. It should be automatically updated at a configurable interval of 15 minutes to block and protect network against active attackers**	As per Tender Document

454	Anti DDOS		Missing critical function of Anti DDOS	**The proposed OEM should provide online portal access to get visibility of global DDOS attack trends along with yearly/half yearly reports on global attack trends for the team to define their stretegies for future.**	As per Tender Document
455	ASM	122	The solution should be bundled with a network decoy to provide real-time visibility into malicious insider activity.	Use Language as: Solution should have private honey pot deployments	As per Tender Document
456	ASM	123	The solution should highlight Wi-Fi enabled devices at risk owing to their connections with unsanctioned devices.	If those devices have Public Ips tagged to the company then they can be picked up	As per Tender Document
457	ASM	123	The solution should have an inbuilt response mechanism wherein it should be able to implement a kill-switch to disrupt network communication originating from offending nodes in the network without the need for any L2/L3 switch/router or security device integration.	ASM tools are part of outside environement of client. So they don't touch any infra of client at any time and don't make any changes to the network. Request you to remove this point as Internal tools like IPS etc should be doing this activity.	As per Tender Document
458	ASM	122		"Platform should discover & then monitor the complete Tech Inventory of customer, including but not limited to: — Cloud Buckets — Domains — IPs — IP Ranges — Subdomains — DNS Records (A, AAAA, CNAME, SOA, MX, NS, TXT etc.) — Digital Certificates — Trackers — Keywords — Technologies — Emails — Executives (Cxx / VPs)	As per Tender Document
459	ASM	122		Vendor should provide Vulnerability Intelligence which will include: a) Vulnerability source information, extensive references, links to Proof of Concept code and solutions b) Vulnerability Intel on 3rd party software products c) Vulnerability Prioritisation"	As per Tender Document
460	ASM	122		The Platform must monitor all of Customer's Public Infrastructure continuously and provide report on •Exploitable Vulnerabilities from known & Unknown assets •CVE/ SSL Expiry •Shadow IT •Sensitive Open Port •Certificate Issues •Misconfigured Devices •The platform must scan the internet for finding RDP, VNC, xserver"	As per Tender Document
461	ASM	122		Platform should also monitor cloud infrastructure of the customer & provide the visibility of the issues & vulnerabilities. Tool should maintain the dynamic cloud inventory "Platform should also provide: •DNS Zone Transfer monitoring •DMARC monitoring. •SPF Monitoring •DKIM Monitoring •BIMI Monitoring"	As per Tender Document
462	ASM	122		The Platform must monitor misconfigured cloud repositories, public folders and peer-to-peer networks for data that could represent leaked confidential or sensitive information.	As per Tender Document
463	ASM	122		Platform should monitor exposed sensitive codes on all of the platforms listed below: Github BitBucket Postman Docker Hub"	As per Tender Document

464	ASM	122		Bidder should have it's own Internet Scanner & data pipeline to monitor the Attack Surface exposure of the customer, it should not be dependent on any 3rd party to provide this service	As per Tender Document
465	ASM	122		Platform should support application security scanning of web applications (OWASP Top 10 vulnerabilities) & should provide visibility into Botnet Detection	As per Tender Document
466	Anti DDoS	285	10 Gbps of L7 Throughput	We request to you to change the Clause as - **10 Gbps of L7 Throughput and upgradable to 20 Gbps on the same platform without changing H/w and should be stateless in architecture supporting 80 Million packet per seconds flood prevention rate on the same appliance.. Device should not have any limit in storing L4 and L7 connections and should not be part of LB, LLB, WAF, IPS or Proxy to prevent state exaustion attacks**	Kindly refer Revised Technical specification
467	Anti DDoS	285	8 x 10G SFP+ from day 1. 8 x 10Gig SR populated from day one and should be upgradeable to 25gig by changing transceivers only. The appliance should also support 40G ports for future use.	We request to you to change the Clause as - "**8 x 10G SFP+ SR populated with internal bypass support from day . The appliance should also support replacement/upgrade of NIC to 40G and 100 G ports for future use**."	Kindly refer Revised Technical specification
468	Anti DDoS	285	SSL TPS 50K with RSA 2k keys and 25K TPS with ECC with SSL throughput of 25 Gbps	We request to change clause as **" SSL TPS of 25K TPS with ECC and should support capability to consume and integrate with 3rd Party feeds (IOCs) via STIX/TAXII inbuilt integration capability along with its own internal feeds(no third party). The Appliance should support more then 3 million IOCs blocking combined and should block such threats at the entry itself being at the extreme parimeter not allowing such malicious IPs to come inside the DC network."**	Kindly refer Revised Technical specification
469	Anti DDoS	286	The traffic Auto learning threshold can be apply automatically after auto learning completed.	We request you to change the clause as **" The traffic Auto learning threshold should be applied manually post understanding its impact on the production traffic after auto learning completed.**	Kindly refer Revised Technical specification
470	Anti DDoS	286	Must have full Authoritative DNS capability to understand records like A, AAAA, CNAME, DNAME, HINFO, MX, NAPTR, NS, PTR, SOA, SRV, Should be able to do on the fly DNSSec.	**We request you to remove these points as they are part of LLB**	Kindly refer Revised Technical specification
471	Anti DDoS	286	the product should convert DNS requests to DNSSec on the fly, should support 1) Delegated DNS and 2) Proxy DNS, supports an GUI integrated zone file management tool that simplifies.	**We request you to remove these points as they are part of LLB**	Kindly refer Revised Technical specification
472	Anti DDoS	286	DNS Zone file management and reduce the risk of misconfiguration	**We request you to remove these points as they are part of LLB**	Kindly refer Revised Technical specification
473	Anti DDoS	286	It shall provide a secure environment to manage DNS infrastructure while validating and error- checking zone files. It shall be built on the latest version of BIND.	**We request you to remove these points as they are part of LLB**	Kindly refer Revised Technical specification
474	Anti DDoS	286	Should be able to define amount of memory for use of DNS caching	**We request you to remove these points as they are part of LLB**	Kindly refer Revised Technical specification
475	Anti DDoS	286	The solution shall have built-in high availability (HA) features in the following mode: Active- Passive, Active-Active using standard VRRP or equivalent	Request you to change the clause as **" The solution should be deployed in the Active Active or Active passive design and should be stateless along with should support capability to consume and integrate with 3rd Party feeds (IOCs) via STIX/TAXII inbuilt integration capability along with its own internal feeds(no third party). The Appliance should support more then 3 million IOCs blocking combined and should block such threats at the entry itself being at the extreme parimeter not allowing such malicious IPs to come inside the DC network."**	Kindly refer Revised Technical specification
476	Anti DDoS	287	The solution shall be able to support IPv4 & IPv6 routing protocols for traffic mitigation: Static Routing, OSPF Routing, BGPv4 Routing and Policy Based routing.	We request you to remove this point as DDoS are stateless and do not support routing protocols	Kindly refer Revised Technical specification

477	Anti DDoS	287	Active-Active and Active- Passive Mode configuration, when deployed in dual mode and should have seamless takeover in- case if one device fails. Support in transparent failover between the devices, and support session mirroring, SSL mirroring, persistence mirroring, connection mirroring and heartbeat check.	Request you to change the clause as **" The solution should be deployed in the Active Active or Active passive design and should be stateless along with should support capability to consume and integrate with 3rd Party feeds (IOCs) via STIX/TAXII inbuilt integration capability along with its own internal feeds(no third party). The Appliance should support more then 3 million IOCs blocking combined and should block such threats at the entry itself being at the extreme parimeter not allowing such malicious IPs to come inside the DC network."**	Kindly refer Revised Technical specification
478	Anti DDoS	288	Solutions Operating System should be tested and certified for EAL 2 / NDPP (Network Device Protection Profile)/NDcPP (Network Device collaborative Protection Profile)/ or above under Common Criteria Program for security related functions	Request you to change the clause as **" Solutions Operating System should be tested and certified for EAL 2 / NDPP (Network Device Protection Profile)/NDcPP (Network Device collaborative Protection Profile)/ or above under Common Criteria Program for security related functions or The OEM should provide 3 Govt/BFSI customer references in India**	Kindly refer Revised Technical specification
479	Anti DDoS		Missing critical function of Anti DDOS	**DDoS solution should be stateless to mitigate TCP / Protocol Exhaustion attacks and should support capability to consume and integrate with 3rd Party feeds (IOCs) via STIX/TAXII inbuilt integration capability along with its own internal feeds(no third party). The Appliance should support more then 3 million IOCs blocking combined and should block such threats at the entry itself being at the extreme parimeter not allowing such malicious IPs to come inside the DC network."**	As per Tender Document
480	Anti DDoS		Missing critical availability funciton of Anti DDOS	**The appliance should support Hardware and Software Bypass Capability with both fail open and fail closed modes in all protection ports (including Copper and Fiber). The hardware bypass for all protection interface types (Copper and Fiber) should have In-Built in the Appliance without the need of any external bypass switch**	As per Tender Document
481	Anti DDoS		Missing critical sizing parameter of Anti DDOS appliance which is flood prevention rate	**Proposed appliance should support minimum of 80 Million packet per seconds flood prevention rate on the same appliance. This performance figure must be mentioned in public facing datasheet.**	As per Tender Document
482	Anti DDoS		Missing critical function of Anti DDOS	**OEM Anti-DDoS Solution should be deployed and used by at least 4 Gov/PSU/BFSI customer in India to protect their own Core infrastructure from DDoS attacks and proposed solution should support native Integration with ISP clean pipe for preventing the volumetric attacks. In case of volumetric attack on premise DDos solution should send signal to the ISP Scrubbing centre for automated scrubbing at the ISP level . Auto signalling should be supported with atleast 4 Tier 1 ISPs Clean pipe services in India**	As per Tender Document
483	Anti DDoS		Missing critical function of Anti DDOS	**Supports over 3 Million IOC Blocking via integration with 3rd Party TIP using STIX/TAXII protocols without any API integration**	As per Tender Document
484	Anti DDoS		Missing critical function of Anti DDOS	**DDoS Appliance must not have any limitations in handling the number of concurrent session for DDoS attack traffic - Knowing nature of solution and should be clearly mentioned in public facing datasheet. It should not maintain session table for authenticated / legitimate sessions.**	As per Tender Document
485	Anti DDoS		Missing critical function of Anti DDOS	**System must have an In-Built and In House updated IP reputation feed that has IOC for Active DDoS vectors, Botnets, etc. that are actively propagating DDoS attack vectors anywhere in the world. It should be automatically updated at a configurable interval of 15 minutes to block and protect network against active attackers**	As per Tender Document
486	Anti DDoS		Missing critical function of Anti DDOS	**The proposed OEM should provide online portal access to get visibility of global DDOS attack trends along with yearly/half yearly reports on global attack trends for the team to define their stretegies for future.**	As per Tender Document
487	Anti DDoS	285	Anti DDOS Solution	Current RFP specs will allow only specific set of vendor(s) to participate and which might avoid competition.	Kindly refer Revised Technical specification

488	Anti DDoS	285	Appliance:	We recommend LLB and DNS SECURITY/Anti DDOS feature should be different solution and vendor with respective features and specialized capabilities.	Kindly refer Revised Technical specification
489	Anti DDoS	285	Anti DDOS and LLB functionalities. The solution must not be part of any UTM or NGFW or any white labelled or virtual solution running on third party hardware.	We recommend DNS DDOS is a specialised DDoS which will ensure DNS functioning under various type of inbound and outbound DNS attacks.	Kindly refer Revised Technical specification
490	Remote Firewall	224	Should be supplied on day 1 with 18 x Gigabit Ethernet (10/100/1000 Base T) ports, 2 X 1000Base-LX Single Mode SFP transceivers and 2x 10G Base SR Transceivers. All mentioned SFP should be fully populated from day one (1).	Considering this to be remote firewall port popuation seems to be highger, request to reduce the interface count of Gigabit Ethernet port count to 8. Should be supplied on day 1 with 8 x Gigabit Ethernet (10/100/1000 Base T) ports, 2 X 1000Base-LX Single Mode SFP transceivers and 2x 10G Base SR Transceivers. All mentioned SFP should be fully populated from day one (1).	Should be supplied on day 1 with 8 x Gigabit Ethernet (10/100/1000 Base T) ports, 2 X 1000Base-SX Single Mode SFP transceivers and 2x 10G Base LR Transceivers. All mentioned SFP should be fully populated from day one (1).
491	Remote Firewall	224	Suggested Add-on point	A firewall with adequate concurrent connection capacity ensures seamless handling of high traffic volumes, preventing performance degradation and service interruptions. It also supports future scalability to accommodate organizational growth and evolving network demands. Request to add below points to ensure right fit appliance to handle the traffic. It is suggested that the Concurrent Connections Supported : 16 Million	As per Tender Document
492	Remote Firewall	226	Should be supplied on day 1 with 12 x Gigabit Ethernet (10/100/1000 Base T) ports, 2 X 1000Base-LX Single Mode SFP transceivers and 2x 10G Base SR Transceivers. All mentioned SFP should be fully populated from day one (1).	Considering this to be remote firewall port popuation seems to be highger, request to reduce the interface count of Gigabit Ethernet port count to 8. Should be supplied on day 1 with 8 x Gigabit Ethernet (10/100/1000 Base T) ports, 2 X 1000Base-LX Single Mode SFP transceivers and 2x 10G Base SR Transceivers. All mentioned SFP should be fully populated from day one (1).	Should be supplied on day 1 with 8 x Gigabit Ethernet (10/100/1000 Base T) ports, 2 X 1000Base-SX Single Mode SFP transceivers and 2x 10G Base LR Transceivers. All mentioned SFP should be fully populated from day one (1).
493	Remote Firewall	226	Suggested Add-on point	A firewall with adequate concurrent connection capacity ensures seamless handling of high traffic volumes, preventing performance degradation and service interruptions. It also supports future scalability to accommodate organizational growth and evolving network demands. Request to add below points to ensure right fit appliance to handle the traffic. It is suggested that the Concurrent Connections Supported : 16 Million	As per Tender Document
494	Internal Firewall	256	Onboard Storage : 4 TB SSD or higher	Is this 4 TB storage requirement is for logs? For this type of setup centralized management and logger should be commisioned with adequate storage to manage and maintain logs.	Kindly refer Revised Technical specification
495	Solution Firewall	259	NG IPS Signature supported excluding custom IPS signatures : 20000 or higher	As in RFP dedicated IPS/IDS appliance is already asked seperately as a solution and IPS Signature count in internal firewall asked as 15000 or higher, Suggest/request you to modify the signature count on solution firewall as well to 15000 or higher.	NG IPS Signature supported excluding custom IPS signatures : 15000 or higher
496	Internet Firewall	259		We assume internet firewall will have separate centralized management. Please suggest what is the envisaged logs per day and the log retention days to be considered for internet firewall.	As per Tender Document
497	Internet Firewall	269	NG IPS Signature supported excluding custom IPS signatures : 20000 or higher	As in RFP dedicated IPS/IDS appliance is already asked seperately as a solution and IPS Signature count in internal firewall asked as 15000 or higher, suggest/ request you to modify the signature count on solution firewall as well to 15000 or higher.	NG IPS Signature supported excluding custom IPS signatures : 15000 or higher

498	IPS/IDS	Page No. 84	The IPS Solution should support Anti-malware protection through various engines as part of solution offerings.	Malware protection should be part of dedicated solution, it can't be clubbed with network protection device like NIPS. Known and unknown attacks like zero-day should be asked to provide wide protection against next gen attacks. **Suggested Clause:** **The IPS Solution should provide protection against zero-day attack without any manual intervention in less than 20 seconds.**	As per Tender Document
499	IPS/IDS	Page No. 84	The IPS Solution should have real time emulation techniques for embedded malware protection.	Malware protection should be part of dedicated solution, it can't be clubbed with network protection device like NIPS. Known and unknown attacks should be asked to provide wide protection against next gen attacks. **Suggested Clause:** **The IPS Solution should provide protection known as well as unknown attacks.**	Kindly refer Revised Technical specification
500	IPS/IDS	Page No. 86	NIPS should support High Availability. It should support stateful HA such that state information is shared between the HA appliance. In case one of the appliances fails state is maintained.	IPS should be transparent in network so that attacker should not be able to identify its presence, state tabel information is relevant for statefull device not stateless. It should also have sufficient capacity to handle large attack request without any performance degradation. **Suggested Clause:** **NIPS should support High Availability. It should be stateless appliance with unlimited attacks concurrent sessions handling.**	Kindly refer Revised Technical specification
501	IPS/IDS	Page No. 86	NIPS should support Active-Active high availability. The HA should be out of the box solution and should not require any third party or additional software for the same	Transparent appliance achieve failover by combining with other routing solution like router or firewall. Dual MNG port should be considered. **Suggested Clause:** **NIPS should support Active-Active high availability. 2x1G RJ45 MNG port should be out of the box**	Kindly refer Revised Technical specification
502	IPS/IDS	Page No. 87	NIPS solution should provide Intelligent security management: ■ Intelligent alert correlation and prioritization ■ Robust malware investigation dashboards ■ Preconfigured investigation workflows ■ Scalable web-based management	Malware protection should be part of dedicated solution, it can't be clubbed with network protection device like NIPS. Known and unknown attacks should be asked to provide wide protection against next gen attacks. **Suggested Clause:** **NIPS solution should provide Intelligent security management:** **■ Intelligent alert** **■ Web-based management**	Kindly refer Revised Technical specification
503	L4 Load	Page No. 104	Each Load balancer must have minimum 6 X 100G Ports and should be fully populated with associated MPO based multimode QSFPs. Ports should be usable as 4x10G ports or 4x25G or 1x40G or 1x50G using breakout cables	The asked port requirement is not inline with the throughput requirement. It can be catered with the cost effective solution, As per the asked throughput, 100G interfaces will unnecessary increase the cost of the solution. **Suggested Clause:** **The solution should be able to provide at least 6 x 40G QSFP+ interfaces and 12 x 10G SFP+ interfaces from day 1 . Dedicated 2x1G RJ45 Management Port and RJ45 Console Port.**	Kindly refer Revised Technical specification
504	L4 Load	Page No. 105	The proposed appliance should support minimum 595 Million packets per second (400X1.488) L4 concurrent connections at line rate, considering minimum packet size of 1500 Bytes.	Appliance should not be oversized, it will unnecessary increase the overall cost of the solution without any requirement. Almost OEMs publish concurrent data, pls consider the same. **Suggested Clause:** **The proposed appliance should support minimum 180 Million L4 concurrent connections**	Kindly refer Revised Technical specification

505	L4 Load	Page No. 105	New Clause Request	Next gen features like virtualization is missing, it must be added to create isolated environment from application and management perspective. **Suggested Changes:** **The proposed device should have Hypervisor Based Virtualization feature(that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. Should be capable of virtualization and support minimum 10 and scalable up to 50 virtual instances each virtual instance having dedicated resources including Management, Operating system and resources from day1**	As per Tender Document
506	L4 Load	Page No. 105	New Clause Request	Certification like EAL should be considered to choose right and reliable product for such critical data centre. **Suggested Clause:** **Appliance's software should be EAL2 certified**	As per Tender Document
507	Anti DDOS	Page No. 107	Anti DDOS and LLB functionalities. The solution must not be part of any UTM or NGFW or any white labelled or virtual solution running on third party hardware.	DDOS should always be a stateless appliance to effectively mitigate large attacks whereas LLB is a statefull appliance, both can't be clubbed together. **Suggested Clause:** **Anti DDOS functionalities. The solution must not be part of any UTM or NGFW or any white labelled or virtual solution running on third party hardware or any statefull appliance.** **Attack Concurrent Sessions: Unlimited**	Kindly refer Revised Technical specification
508	Anti DDOS	Page No. 107	10 Gbps of L7 Throughput	DDoS should be sized based on legit and attack throughput. **Suggested Clause:** **Legit Throughput: 10Gbps and scalable upto 40Gbps** **Attack Mitigation Throughput: 60Gbps**	Kindly refer Revised Technical specification
509	Anti DDOS	Page No. 107	8 x 10G SFP+ from day 1. 8 x 10Gig SR populated from day one and should be upgradeable to 25gig by changing transceivers only. The appliance should also support 40G ports for future use.	Appliance should have sufficient port to cater current as well as future requirement, asking the 25G or 40G port is of no use as per throughput requirement. **Suggested Clause:** **12 x 10G SFP+ from day 1. 12 x 10Gig SR populated from day one and should be upgradeable to in total 24 x 10G SFP+ for future only.**	Kindly refer Revised Technical specification
510	Anti DDOS	Page No. 107	Dedicated1 x 1G RJ45 Out-of-band Management Port and RJ45 Console Port	As DDOS is a stateless appliance, it has only MNG port for management and reporting which should be redundant in nature. **Suggested Clause:** **Dedicated 2x1G RJ45 Management Port and RJ45 Console Port.**	As per Tender Document
511	Anti DDOS	Page No. 107	SSL TPS 50K with RSA 2k keys and 25K TPS with ECC with SSL throughput of 25 Gbps	SSL and PPS sizing should be sufficient to handle all technical requirements.Hence, request to ammend the clause. **Suggested Clause:** **Should support minimum 25 MPPS & minimum 90K TPS on RSA 2K Key**	Kindly refer Revised Technical specification
512	Anti DDOS	Page No. 107	Must have full Authoritative DNS capability to understand records like A, AAAA, CNAME, DNAME, HINFO, MX, NAPTR, NS, PTR, SOA, SRV, Should be able to do on the fly DNSSec.	Record resolution should be part of DNS server not DDOS.It can protect from DNS attacks as well as zero-day attacks. **Suggested Clause:** **Must protect from DNS attacks. Solution should also protect from zero-day using real time signature within 20sec automatically.**	Kindly refer Revised Technical specification

513	Anti DDOS	Page No. 107	the product should convert DNS requests to DNSSec on the fly, should support 1) Delegated DNS and 2) Proxy DNS, supports an GUl integrated zone file management tool that simplifies.	Appliance should not work like DNS server, it is meant for DDoS protection. **Suggested Clause:** **Delete the clause**	Kindly refer Revised Technical specification
514	Anti DDOS	Page No. 107	DNS Zone file management and reduce the risk of misconfiguration	Appliance should not work like DNS server, it is meant for DDoS protection. **Suggested Clause:** **Delete the clause**	Kindly refer Revised Technical specification
515	Anti DDOS	Page No. 107	It shall provide a secure environment to manage DNS infrastructure while validating and error- checking zone files. It shall be built on the latest version of BIND.	Appliance should not work like DNS server, it is meant for DDoS protection. **Suggested Clause:** **Delete the clause**	Kindly refer Revised Technical specification
516	Anti DDOS	Page No. 107	Should be able to define amount of memory for use of DNS caching	Appliance should not work like DNS server, it is meant for DDoS protection. **Suggested Clause:** **Delete the clause**	Kindly refer Revised Technical specification
517	Anti DDOS	Page No. 108	The solution shall have built-in high availability (HA) features in the following mode: Active- Passive, Active-Active using standard VRRP or equivalent	VRRP is not relevant for stateless appliance like DDoS, DDoS should support clustering. **Suggested Clause:** **The solution shall have clustering features for HA**	Kindly refer Revised Technical specification
518	Anti DDOS	Page No. 109	The solution shall be able to support IPv4 & IPv6 routing protocols for traffic mitigation: Static Routing, OSPF Routing, BGPv4 Routing and Policy Based routing.	Routing is not relevant for stateless appliance like DDoS. **Suggested Clause:** **The solution shall be able to support IPv4 & IPv6 traffic mitigation along with L3-L7 mitigation.**	Kindly refer Revised Technical specification
519	Anti DDOS	Page No. 109	Active-Active and Active- Passive Mode configuration, when deployed in dual mode and should have seamless takeover in- case if one device fails. Support in transparent failover between the devices, and support session mirroring, SSL mirroring, persistence mirroring, connection mirroring and heartbeat check.	Should be transparent in network so that attacker should not be able to identify its presence, state tabel information is relevant for statefull device not stateless. It should also have sufficient capacity to handle large attack request without any performance degradation. **Suggested Clause:** **Should support High Availability.**	Kindly refer Revised Technical specification
520	Anti DDOS	Page No. 109	The solution should provide online troubleshooting and traffic analysis tool where the administrator can take a snapshot of the config and upload it on web based diagnostic tool to check the health and vulnerability of the solution with the recommended solution provided on the knowledge base link.	Clause should be generic, using single OEM terminology is restrictive. **Suggested Clause:** **The solution should provide troubleshooting and traffic analysis as well as recommendation using knowledge base link.**	Kindly refer Revised Technical specification

521	Load Balancer with WAF	Page No. 145	Must display a visual representation of authentication in the GUI. The Appliance must support minimum two 40/100Gig SFP Slots and 8 * 10G SFP+ slots populated with 10Gig SR and same should be upgradeable to 25Gig by changing transceivers only. The solution must be appliance based, 1U rack mountable and it should be having internal redundant Power Supply from day one.	Visual representation of authentication is of no use, system should alert admin. 100G port will unneccessary increase overall cost without any requirement. 1U is restrictive clause and does not create any advantages. **Suggested Clause:** **Must alert administrator.** **The Appliance must support minimum six 40 SFP+ Slots and 12 * 10G SFP+ slots populated with 10Gig SR.** **The solution must be appliance based, 1U/2U rack mountable and it should be having internal redundant Power Supply from day one.** **Dedicated 2x1G RJ45 Management Port and RJ45 Console Port.**	Kindly refer Revised Technical specification
522	Load Balancer with WAF	Page No. 148	New Clause Request	Next gen features like virtualization is missing, it must be added to create isolated environment from application and management perspective. **Suggested Changes:** **The proposed device should have Hypervisor Based Virtualization feature(that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. Should be capable of virtualization and support minimum 10 and scalable up to 50 virtual instances each virtual instance having dedicated resources including Management, Operating system and resources from day1**	As per Tender Document
523	EMS	374	EMS should provide the compliance management report in the integrated view showing network topologies. Proposed EMS should adhere to guidelines so that the CERT can stay compliant with its current day industry standards .The minimum security guidelines to be adhered are: a.) All the data stored or getting communicated over LAN should be encrypted as per encryption level mentioned in detailed technical specifications. b.) Malicious code test certificate to be provided. Solution should be OWASP & SANS certified by CERT-In empanelled vendor. c.) VAPT – Ensure VAPT is done immediately after the software is deployed but before taking the system into production. d.) To provide regular hot fixes/updates to ensure the system security. e.) The Software to be integrated with AD and AAA as well to ensure the strong access control measures. The SI is required to provide a clean VAPT report of the complete solution (i.e. including all modules) at the time of acceptance testing, where all categories of vulnerabilities are fixed in the deployed solution. Additionally, periodic VAPTs must be done yearly from the date of acceptance and additional VAPT should be done, upon any major upgrade in solution or solution's respective modules.	OWASP and SAN 25 Security Assessment certificates, are overlapping standards wherein most of the testing is similar. So we request that either of these certification to be asked and amend this clause as below: "EMS should provide the compliance management report in the integrated view showing network topologies. Proposed EMS should adhere to guidelines so that the CERT can stay compliant with its current day industry standards .The minimum security guidelines to be adhered are: a.) All the data stored or getting communicated over LAN should be encrypted as per encryption level mentioned in detailed technical specifications. b.) Malicious code test certificate to be provided. Solution should be OWASP/SANS certified by CERT-In empanelled govt vendor. c.) VAPT – Ensure VAPT is done immediately after the software is deployed but before taking the system into production. d.) To provide regular hot fixes/updates to ensure the system security. e.) The Software to be integrated with AD and AAA as well to ensure the strong access control measures. The SI is required to provide a clean VAPT report of the complete solution (i.e. including all modules) at the time of acceptance testing, where all categories of vulnerabilities are fixed in the deployed solution. Additionally, periodic VAPTs must be done yearly from the date of acceptance and additional VAPT should be done, upon any major upgrade in solution or solution's respective modules."	The clause may be read as EMS should provide the compliance management report in the integrated view showing network topologies. Proposed EMS should adhere to guidelines so that the CERT can stay compliant with its current day industry standards .The minimum security guidelines to be adhered are: a.) All the data stored or getting communicated over LAN should be encrypted as per encryption level mentioned in detailed technical specifications. b.) Malicious code test certificate to be provided. Solution should be**OWASP / SANS** certified by CERT-In empanelled vendor. c.) VAPT – Ensure VAPT is done immediately after the software is deployed but before taking the system into production. d.) To provide regular hot fixes/updates to ensure the system security. e.) The Software to be integrated with AD and AAA as well to ensure the strong access control measures. The SI is required to provide a clean VAPT report of the complete solution (i.e. including all modules) at the time of acceptance testing, where all categories of vulnerabilities are fixed in the deployed solution. Additionally, periodic VAPTs must be done yearly from the date of acceptance and additional VAPT should be done, upon any major upgrade in solution or solution's respective modules.
524	EMS	389	OEM of EMS Solution should be SOC2, CMMI Level 3, ISO 27001&ISO 27034 certified	SOC2 certification is not typically a standard requirement for EMS solutions, as it is more relevant for service organizations handling sensitive data. To ensure the certification aligns with the qualifications needed for EMS applications, we, request to ammend this clause as below: "OEM of EMS Solution should be SOC2/CMMI Level 3, ISO 27001&ISO 27034 certified."	Kindly refer Revised Technical specification

525	EMS	367	The overall solution should be provided in local High Availability mode. There should be seamless automatic successful switchover/handover (in failure cases) between the two instances. The each instance of applications / modules should execute at different physical servers. The servers should be of industry standard and data center compatible. Each instance should be able to manage & monitor complete infrastructure at DC, DR & Remote Locations.	We understand that the proposed solution will include one instance at the DC with HA and one instance at the DR with HA,. Additionally, the DC and DR instances will operate in an active-standby mode, Kindly confirm if our understanding is correct.	Instances at DC shall be able to monitor and manage DC / DR &/or Remote Sites. Instances at DR shall be able to monitor and manage DR / DC &/or Remote Sites. Remote Sites shouldnt go unmonitored . When the DC instances are down / don't have MPLS connectivity at DC ; DR instances should be able to manage & monitor Remote Sites; Data generated/updated during this period at DR should be able to synced up to DC. & Vice Versa is applicable when DR connectivity is down. The clause "Each instance should be able to manage & monitor complete infrastructure at DC, DR & Remote Locations." may be read as "Each instance should be able to manage & monitor complete infrastructure at DC / DR &/or Remote Locations."
526	EMS	368	The OEM/OEM(s) should have their own IP rights on the solution being supplied, so as any customization required in solution may be possible by them. This will include integration with third-party Non-EMS / EMS applications over REST APIs /any other interface. The integration should be bi-directional in nature.	We understand that the required integration with proposed solution includes AIM and PATS systems. Kindly confirm if this understanding is correct. If additional integrations are required, please provide detailed information about that systems, including functionalities and the quantity for each integration.	For detailed information about the integrations pls refer to the Tech Specs & Scope of work Section w.r.t EMS
527	EMS	370	The scripts may be used for upgrading the Firmware in NEs for any relevant issues such as fixing vulnerabilities.	Fixing vulnerabilities does not fall under the scope of EMS and is generally managed by security solutions. The EMS is primarily responsible for network equipment management and monitoring . So, we kindly request amending the clause as below: "The scripts may be used for upgrading the Firmware in NEs for any relevant issues."	The clause may be read as "The scripts may be used for upgrading the Firmware in NEs ."
528	EMS	372	Should provide option to provide standard compliance checks w.r.t Configuration, OS version, software process/services running state across all target devices, etc.	We understand that the requirement for standard compliance checks related to configuration, OS version, and software processes/services running state is specific to network switches and routers. Kindly confirm if our understanding is correct.	This will be for other IT Infra as well which provide the relevant data over SNMP
529	EMS	377	The solution must support custom dashboards for different role users such as Management, admin and report users	Based on industry standards, user roles are typically defined as Management, Admin, and View-Only users. Report generation is generally an inherent functionality, often with a drill-down feature set. To align with this standard practice, we kindly request amend the clause as below: "The solution must support custom dashboards for different role users such as Management, admin and view only users."	The clause may be read as The solution must support custom dashboards for different role users such as Management, admin and View-Only/other users
530	EMS	379	The proposed management solution's network configuration module, should be able to automatically backup configurations (for both text based and binary configuration files etc.) on routers, switches, and other network devices. The trigger to automatic back up may be setup in EMS such trigger could be upon a detection of a configuration change and/or an automatic timer based. The configuration change should be recorded with the date-time stamp along with the user info. The EMS must integrate with Firewall and Access point OEM's EMS to bring the backup of these configuration files for Firewall and Access Point, provided OEM's Element Management System allows a automatic mechanism and a standard interface for backup of configuration files from Access Points and Firewall, then these files must be brought to proposed EMS.	We understand that configuration backups for Access Points and Firewalls are typically managed through their respective specific EMS systems, as these devices often do not extend such functionality directly to third-party EMS solutions. To align with standard industry practices and avoid operational challenges, we kindly request to relax this clause and amend it as below: "The proposed management solution's network configuration module, should be able to automatically backup configurations (for both text based and binary configuration files etc.) on routers, switches, and other network devices. The trigger to automatic back up may be setup in EMS such trigger could be upon a detection of a configuration change and/or an automatic timer based. The configuration change should be recorded with the date-time stamp along with the user info. "	The clause may be read as : The proposed management solution's network configuration module, should be able to automatically backup configurations (for both text based and binary configuration files etc.) from routers, switches, firewalls and other network devices to EMS. The trigger to automatic back up may be allowed to be setup in EMS , such trigger could be upon a detection of a configuration change and/or an automatic timer based. The configuration change should be recorded with the date-time stamp along with the user info. All configuration data needs to maintained as encrypted. The EMS should bring the backup of these configuration files for Firewall and Access Point or other networking equipment, provided the OEM / OEM's Element Management System allows an automatic mechanism and a standard interface for backup of configuration files from these devices.
531	EMS	368	Solution be bundled with Data base /Data store encryption for Documents encryption and decryption using AES 256 bit cipher.	We understand that the clause refers to documents related to knowledge management, which are intended to be stored in the database in an encrypted format using AES 256-bit cipher. Kindly confirm if our understanding is correct.	The clause may be read as "Solution be bundled with Data base Encryption & (optional feature) Documents encryption and decryption using AES 256 bit cipher."
532	EMS	373	Should be scalable to allow the addition/integration of new instances of devices to be added in future	Kindly provide information on the new instances of devices expected to be added or integrated in the future, along with the approximate quantities for each category.	Refer to maximum change clause allowed in the bid, for identifying the percentage of devices allowed to be increased.

533	EMS	378	5. Database Monitoring parameters such as a Database Availability b Database Process and Logs c Locks and Buffers d Tablespace/Database e Sessions/Connections f Database Memory h SQL Statistics i Database Jobs etc.	kindly provide details and quantity regarding the specific databases/application that need to be monitored, including their types and versions. to ensure accurate planning and implementation	Latest data bases such as sql, postgres , elastic , mongo etc.
534	EMS	366	The proposed EMS solution and all modules (e.g. Configuration Management, network monitoring, server monitoring, asset management, IT Helpdesk, Change Management etc.) must be from a single OEM to fulfill the sought requirements & functionality. Bidder holds the responsibility to ensure of testing the functionality of these components/modules before proposing a solution in the bid.	We understand that the EMS modules should be from the same OEM((e.g. Configuration Management, network monitoring, server monitoring, asset management, IT Helpdesk, Change Management etc.) to ensure seamless integration and functionality. However, IPAM can provided as a third-party tool that is integrated with the proposed EMS. Kindly Confirm!	The proposed EMS solution and all modules (e.g. Configuration Management, network monitoring, server monitoring, asset management, IT Helpdesk, Change Management etc.) must be from a single OEM to fulfill the sought requirements & functionality. The final EMS solution with IPAM & Switch Port Management may be an integration of OEMs to fulfill the sought requirements. In case the IPAM solution is from other OEM, the EMS OEM holds the responsibility along with bidder to accomplish the end to end integrated requirements of IPAM in EMS. Bidder holds the responsibility to ensure testing of complete functionality of these components / modules before proposing a solution in the bid.
535	EMS	386	The solution must be agentless can be an pre-integrated module of EMS or it could be a separate module . It may be noted that the functionality and specifications sought via IPAM and Switch Port Management Module may be fulfilled as an integrated module of EMS.In either cases , it must allow the secured access via the browsers using SSL certificates(128 bit &/or 256 bit encryption)	We understand that the EMS modules should be from the same OEM((e.g. Configuration Management, network monitoring, server monitoring, asset management, IT Helpdesk, Change Management etc.) to ensure seamless integration and functionality. However, IPAM can provided as a third-party tool that is integrated with the proposed EMS. Kindly Confirm!	The clause may be read as : The proposed EMS solution and all modules (e.g. Configuration Management, network monitoring, server monitoring, asset management, IT Helpdesk, Change Management etc.) must be from a single OEM to fulfill the sought requirements & functionality. The final EMS solution with IPAM & Switch Port Management may be an integration of OEMs to fulfill the sought requirements. In case the IPAM solution is from other OEM, the EMS OEM holds the responsibility along with bidder to accomplish the end to end integrated requirements of IPAM in EMS. Bidder holds the responsibility to ensure testing of complete functionality of these components / modules before proposing a solution in the bid.
536	EMS	371	Users must be able to choose the thresholds (high and low) for when an alarm and/or warning will activate, along with the points for the severity level. Users must be able to acknowledge and filter alarms. Alarms should have a way to prioritize more important alarms. The solution shall include an alarm history page where all system alarms are stored. Users should be able to search for previous alarms by site, device, or point. Should be able to manage and display alarms/events/alerts, store them and should allow creation of new alarms/events/alerts from scratch with customizable threshold limits. The threshold may be applied to any valid parameters which are being monitored per device.	Since alarms are based upon the events generated at devices and not created manually, we understand that here the term "scratch" implies the ability to create new tickets based on threshold settings, with notifications sent to users upon thresholds, Kindly confirm if our understanding is correct.	Yes
537	SFTP Solution	133	The solution should be able integrated using SAML for SSO	Requesting you to please share the vender name of SSO provider.	As per Tender Document
538	SFTP Solution	132	It should recursively sanitize/scan embedded file in docx, pptx ,xlsx etc.	Requesting you to please consider the clouse as**" It should recursively sanitize and scan embedded file in docx, pptx ,xlsx etc."**	As per Tender Document
539	NAC (Included AAA) Server	153	Ability to create playbooks to run specific tasks on endpoint and assign compliance status	Requesting you to please delete this clouse . This is endpoint management feature.	As per Tender Document
540	NAC (Included AAA) Server	152	The solution should support authentication protocols including PAP,MS-CHAP,PEAP and EAP-TLS and 802.1X Single Sign-On (SSO)	Requesting you to please share the vender name of SSO provider.	As per Tender Document
541	Security Kiosk	111	The solution should be able to support whitelisted USB Drives	Requesting you to please consider the clouse as**" The solution should be able to support whitelisted USB Drives and Defending a range of BadUSB devices, including RubberDucky and BashBunny,"**	As per Tender Document

542	EMS	Page No. 371	222. The solution should have its own IT Service Management (ITSM) / IT helpdesk solution which is certified on ITIL v4 atleast 5 practices.Should provide an GUI interface w.r.t emails.	We recommend the authority to kindly update the requirements and replace this clause as follows to ensure selection of a proven Helpdesk solution: **"The proposed Helpdesk solution must be ITIL-certified across at least 12 key ITIL processes, such as Incident Management, Request Management, Problem Management, Change Management, Availability Management, and Event Management. Documentary proof of the ITIL certification, covering these processes, should be provided at the time of bidding to verify compliance and ensure the solution's adherence to ITIL best practices."**	The Clause#222 in EMS sepcs may be read as below : The solution should have its own IT Service Management (ITSM) / IT helpdesk solution which is certified on ITIL v4 atleast 5 practices.Should provide an GUI interface w.r.t emails. Documentary proof of the ITIL certification, for the covered processes, should be provided at the time of bidding to verify compliance and ensure the solution's adherence to ITIL best practices."
543	EMS	Page No. 371	59. Reports shall contain visualizations utilizing the applicable graphic types such as Bar Chart, Gauge , Pie Chart, Scatter Plot, Simple Value, Table, Time Series, User Image, User Text etc.	Requesting clarification from the authority regarding the specific requirements for user images and user text in the report. Could you please elaborate on what exactly is expected and how these elements should be presented in the report?	Few of use cases using User Images & User Text include Logo & Special Text insertion in reports ; These will be required in other such customized reports.
544	EMS	Page No. 377	131. The platform must consolidate monitoring events from across layers such as Network, Server, Database, 3rd party tools (monitoring solutions to monitor key DC elements like wires / cables etc.)	Passive components cannot be monitored using NMS. Kindly exclude them from the scope of NMS/EMS.	No Change; Monitoring here is via integration with 3rd Party tools such as AIM
545	EMS	NA	clause addition	In order to select proven EMS/NMS (Enterprise Monitoring System/Network Monitoring System) solution with deployment experience in projects with similar magnitude, we recommend the authority to consider following clause in the NMS specification: **"The proposed NMS solution should have been successfully implemented in at least two State Data Centers or should be monitoring a minimum of 10,000 nodes across three deployments within State/Central Government or PSU projects in India. Documentary proof, such as Purchase Order (PO) copies and project sign-off/completion certificates, must be submitted at the time of proposal submission."**	As per Tender Document
546	EMS	NA	clause addition	In order to select solution with in-built database for ensuring better control and flexibility along with lower TCO, we recommend the authority to incorporate the below clause: **"The monitoring module of proposed solution must not use any third party database (including RDBMS and open source) to store data in order to provide full flexibility and control on collected data."**	As per Tender Document

547	EMS	NA	clause addition	In order to provide complete visibility of IT infrastructure including servers with micro level monitoring (on need basis) through which granular level details can be captured along with flexibility of monitoring through agent and agentless approach. Hence, we request the authority to add the following clause in the EMS specification: **"The proposed NMS solution must provide agentless as well as agent based monitoring for server infrastructure. The agents should be able to set polling interval as low as 1 second with low overhead on target server infrastructure."**	As per Tender Document
548	EMS	NA	clause addition	ISO and CIS standards are a set of security guidelines and best practices developed by the nonprofit organizations such as ISO and CIS. These standards provide detailed configuration recommendations and benchmarks for securing your enterprise network. The purpose of these benchmarks is to provide industry-recognized guidelines for secure system configuration. These benchmarks help the authority to enhance their security posture, mitigate risks, and ensure compliance with industry standards and regulatory requirements. Hence we request you to add the following cluase in the RFP **"The OEM of the proposed solution should possess Quality certifications ISO 9001, Information security certificate ISO 27001, Application security certificate ISO 27034 and CIS benchmark certificate. Documentary proof must be provided at the time of submission."**	As per Tender Document
549	Non Smart Rack	Annexure-1 (Technical Specifications) Page 161	Rear 19" mounting angles supplied as split pairs to allow easy adjustments for equipment of different depths.	Please accept to delete this clause for broader level of participation.	As per Tender Document
550	Non Smart Rack	Annexure-1 (Technical Specifications) Page 161	Side panels with Slam latches and Indents for improved strength and aesthetics	Please accept to revise this clause as "Side Panel shall be lockable and horizontally split for ease of operation and aesthetics".	As per Tender Document
551	Non Smart Rack	Annexure-1 (Technical Specifications) Page 161	Component Shelf 720mm Depth - 2 Nos	Please accept to revise this clause as "Component Shelf shall be with depth adjustable of minimum 620mm deep"	As per Tender Document
552	Non Smart Rack	Annexure-1 (Technical Specifications) Page 162	Each rack should have 2 PDUs The 2 PDUs in each rack should have different chassis color for identification of UPS source. Electrical rating – Input – 230V, 32A, 1 Phase, 3-meter-long input cable with Splash proof IEC60309 input plug. For all 3Ph PDU it must have the color-coded alternating outlets based on the circuit color to identify the phase and help phase balancing when used as a three phase PDU. High temperature grade, operating temperature up to 60°C.	Please accept for single black coloured chassis.	Each rack should have 2 PDUs The 2 PDUs in each rack should have different chassis color / single black coloured chassis for identification of UPS source. Electrical rating – Input – 230V, 32A, 1 Phase, 3-meter-long input cable with Splash proof IEC60309 input plug. For all 3Ph PDU it must have the color-coded alternating outlets based on the circuit color to identify the phase and help phase balancing when used as a three phase PDU. High temperature grade, operating temperature up to 60°C.
553	KVM Console	Annexure-1 (Technical Specifications) Page 163	Proposed 18.5” or higher LCD console tray and 16 port IP KVM switch should be built in design and should occupy 1U space together in 19” standard rack. KVM Console should have provision to integrate with existing/deployed centralized monitoring software to monitor all KVMs.	Please accept for separate unit as well for both KVM & LCD.	As per Tender Document

554	KVM Console	Annexure-1 (Technical Specifications) Page 163	It should have cable management arm(CMA) and the 16x RJ45 port KVM switch built in at the rear side of the LCD console tray to save the U space in Rack.	Please accept to revise this clause by removing Cable management arm (CMA) from rear.	As per Tender Document
555	KVM Console	Annexure-1 (Technical Specifications) Page 163	Both LCD console tray and the built-in KVM switch should have single/ separate power supply.	Please accept for separate power supply as well for both KVM & LCD	As per Tender Document
556	KVM Console	Annexure-1 (Technical Specifications) Page 163	Vendor should supply 16 number of KVM cables with VGA, USB connectors.	Please accept to revise this clause as "Vendor should supply 16 number of Dongles / KVM cables with VGA, USB connectors."	As per Tender Document
557	KVM Console	Annexure-1 (Technical Specifications) Page 163	Built-in KVM switch should have 16 RJ45 port to connect KVM cable/dongle with CAT cable to extension at least up to 30Mt	Please accept to revise this clause as "KVM switch should have 16 RJ45 port to connect KVM cable/dongle with CAT cable to extension at least up to 30Mt"	As per Tender Document
558	KVM Console	Annexure-1 (Technical Specifications) Page 163	Built it KVM switch should have encryption 128-bit AES for keyboard, mouse and video signals and virtual media sessions, internal and LDAP external authentication.	Please accept to revise this clause as "KVM switch should have encryption for keyboard, mouse and video signals and virtual media sessions, internal and LDAP external authentication."	As per Tender Document
559	KVM Console	Annexure-1 (Technical Specifications) Page 163	Built-in KVM switch should be cascaded with another KVM switch with max 30Mt CAT cable.	Please accept to revise this clause as "KVM switch should be cascaded with another KVM switch with max 30Mt CAT cable."	As per Tender Document
560	KVM Console	Annexure-1 (Technical Specifications) Page 163	Built-in KVM switch should have min. two VGA local console ports.	Please accept to revise this clause as "KVM switch should have min. one VGA local console ports."	The clause may be read as : Built-in KVM switch should have min. one VGA/DVI local console ports.
561	KVM Console	Annexure-1 (Technical Specifications) Page 163	LCD KVM console should support min. resolutions up to 1366 x 768 @ 60Hz; & KVM switch to support Local VGA up to 1920 x 1080 & Remote support up to 1600 x 1200	Please accept to revise this clause as "Minimum LCD Resolution as 1280 x 1024 & KVM Resolution as 1600 x 1200.	As per Tender Document

562	KVM Console	Annexure-1 (Technical Specifications) Page 163	Operating temperature and Humidity of LCD console tray should be 0°C to 50°C and 10% to 80%	Please accept to revise this clause as "Operating temperature and Humidity of LCD console tray should be 0°C to minimum 40°C and 10% to 80%	As per Tender Document
563	KVM Console	Annexure-1 (Technical Specifications) Page 163	LCD console tray should be global certified by most of the agencies like UL, CE, BSMI, cUL, IC, UKCA, NOM, FCC Class A	Please accept to revise this clause as "LCD console tray should be global certified by most of the agencies like C-Tick, CE, Industry Canada, KCC, NOM, UL listed, VCCI class A, VDE, TAA compliance"	LCD console tray should be global certified by most of the agencies like UL/, CE/, BSMI/, cUL/, IC/ , UKCA / , NOM/, FCC Class A
564	RLPAT	Technical Specifications, Page#9	OEM should have atleast 03 projects i.e. three Purchase Orders/commissioning(s) with PAT Solution & atleast 1000 nodes in each Project	**Technical Specifications, Page#9,** Please accept to revise the clause as follow: "OEM should have atleast **02** projects i.e. **two** Purchase Orders/**Commissioning(s) Certificate/successful DCIM Integration experience** with PAT Solution & atleast 1000 nodes in **1x** Project"	The clause may be read as : "OEM should have atleast 01 project i.e. one Purchase Order / Commissioning(s) Certificate of PAT Solution with atleast 1000 nodes in a Project / a successful DCIM / PAT Solution integration experience with atleast 1000 nodes in a single Project ."
565	EMS	94	Setting up, configuring and integrating requested software modules such as AAA, Active Directory, EMS, PATS, IT Helpdesk, Asset Management etc. (its complete list as per BoM & specifications) in a High Availability (HA) mode for administration, monitoring and management of infrastructure and established Network. EMS OEM holds the responsibility to perform integration of overall EMS solution & PATS (with all their respective sought modules). Contractor must ensure that the integration of EMS with all IT equipment commissioned as a part of this bid. Contractor must ensure that all this equipment is discoverable and manageable via the EMS.	We understand that in EMS solution we have to capture the alarms from PATS solution and convert them into tickets. Kindly confirm.	Clause is self explanatory
566	EMS	94	Installing & configuring AIM solution at DC and DR. Integrating AIM solution at new DC&DR with EMS.	We understand that in EMS solution we have to capture the alarms from AIM solution and convert them into tickets. Kindly confirm.	Clause is self explanatory
567	EMS	94	ERNET India/CERT-In intends to procure the DCIM solution in another bid, Integration of DCIM and EMS using REST APIs/SNMP and / or any other available non – proprietary interfaces available for integration between modules for accomplishing requirements and complete functionality will be in scope of the EMS OEM & Contractor. Integration of EMS's IT Helpdesk & Change Management Solution with PATS solution , Integration of EMS with the additionally planned security components via standard interfaces such as SNMP,REST etc.	We understand that in EMS solution we have to capture the alarms from DCIM solution and convert them into tickets. Kindly confirm.	Clause is self explanatory

568	EMS	95	Installation, configuration of a syslog server, its integration with EMS (in case syslog server is not built-In EMS) and integrating it with all network devices & servers to aggregate syslog(s) at this server	Request you to specify the Events per Second (EPS) rate to size the solution accordingly. Also, request you to specify the data retention period for logs.	Back up Data Retention Period is 1 year. Consider 1x the Logs from all solutions & IT equipment being procured in this bid for caluclation of EPS rate.
569	EMS	95	11) Installation and commissioning of IP Address Management and Switch Port Management solution to allow management of available and used IP addresses. i.e. it must support Network inventory management with IP address and Switch port management.	We request you that IPAM solution should be provided from same OEM as EMS solution. Thus providing a unified offering to the end customer with less complexity.	EMS needs to contain IPAM & Switch Port Management functionality ; May refer to revised respective updated clause
570	EMS	27	Solution should have its own application and data base . It should be a web based portal hosted in an on premise manner.	The change management solution is an integrated module of EMS solution so we understand that change management can share the centralized database of EMS soltuion. Kindly confirm.	Yes provided that Change Management Module is an integrated module of EMS.
571	EMS	28	It should be able to use IMAP, POP3 ,SMTP protocols to provide email integration and able to send emails for CRs status as configured . The solution must be able to use IMAP, POP, protocols & should be able to automatically convert service request emails into help desk tickets.	We request you to remove POP3 protocol.	As per Tender Document
572	EMS	32	Uses the communications channel with enhanced security features, audit logs, and access control policies to provide direct connections to servers in any location	We understand that here access of EMS server has to provided using secure protocol such as HTTPS. Kindly confirm.	Clause is self explanatory
573	EMS	33	Document Management/Collaboration / Knowledge-based module - The system should also have knowledge-based module built in for the operators for quick issue identifications and resolution, thus minimizing the time and efforts. This will should server as a historical database of documents and can be used for training of new recruits, resolution of alarms, resolution of certain specific issues. Users should be able to add information, categorize it, add files to it. The proposed storage for Collaboration and Knowledge-based module artifacts should be scalable. It must sufficient enough by default to store data for the complete contract period. In case of any shortage of storage , SI will be required to immediately(within 1week notice) provide the double the original capacity storage base.	Request you to specify the storage required as it will be very diffcult to assume the amount of data that will be uploaded into the system for an entire contract period.	The details about types of information to be stored is already detailed in the clause; Duration for which its to be stored is already mentioned; Now the total size will depend upon how the OEM is performing the storage.
574	EMS	33	OEM of EMS Solution should be SOC2, CMMI Level 3, ISO 27001&ISO 27034 certified	SOC3 is now the latest certification. Request you to modify the clause as "OEM of EMS Solution should be SOC2/SOC3, CMMI Level 3, ISO 27001&ISO 27034 certified "	May refer to respective revised clause

575	EMS	33	OEM should have performed the installation / commissioning at 5 projects with minimum 2500 nodes in each project.	Kindly clarify whether enterprise or global customer experience can be used here or only indian government customer references can be provided here.	The clause may be read as : OEM should have performed the installation / commissioning of atleast 2 projects with minimum 2000 nodes in each project in India.
576	Intelligent cabling	54	Intelligent Cabling is required at DC for 100 Racks & at DR for 50 Racks.	Please share the rack layout for both DC (100 Racks) and DR (50 Racks). This will be required for the preparation of the Passive Structured Cabling BoQ.	Kindly refer Revised Technical specification
577	Intelligent cabling	165	2 X 16 LC Duplex connections will be extended to each Server/Storage via fiber shelf to enable intelligent solution.	Please confirm if any connectivity between two adjacent servers racks is required for Network 1	Self explanatory
578	Intelligent cabling	58	Flame Test Method: IEC 60332-3/ IEC 60332-1 , IEC 60754-2, IEC 61034-2	The fiber trunk cables and patch cords must strictly comply with IEC 60332-3, as IEC 60332-1 is not the appropriate flame test standard for cable bundles. Since all fiber trunk cables and patch cords will be installed along the same pathway, forming a cable bundle, permitting compliance with IEC 60332-1 would heighten the risk of significant fire spread in case of a fire. Therefore, the clause should be revised as follows: **Flame Test Method: IEC 60332-3, IEC 60754-2, IEC 61034-2**	As per Tender Document
579	Intelligent cabling	61	Connector type: LC/UPC to LC/UPC, Fiber patch cord 1.7mm / 3.5mm. Riser	In a Data Center environment, it is preferable to use small-diameter patch cords to effectively manage the high volume of patch cords within a rack. Therefore, we request that 1.6 mm diameter patch cords also be allowed. The clause should be revised as follows: **Connector type: LC/UPC to LC/UPC, Fiber patch cord 1.6mm / 1.7mm / 3.5mm. Riser**	Kindly refer Revised Technical specification
580	Intelligent cabling	61	Color: Lime Green color for cable and Gray color for connector	Typically, the connector color for an LC connector is Black or Beige. We request that Black connectors also be permitted, or that the connector color can be made color-independent. The clause should be revised as follows: **Color: Lime Green color for cable and connector color as per OEM**	Kindly refer Revised Technical specification
581	Intelligent cabling	61	Missing Clause: Insertion Loss and Return Loss value specifications missing for OM5 LC type fiber patch cords seem by mistake as these critical performance parameters are there for all other components such as OM5/0M4 trunk cable, OM4 Patch cords.	The insertion loss and return loss are the most critical performance specifications for any fiber cable or patch cord. These parameters are currently missing and must be included in the specifications to guarantee the supply of high-performance patch cords. The following clause should be added to the specifications: **Insertion Loss, maximum: 0.15 dB** **Return Loss, minimum: 35 dB**	As per Tender Document
582	Intelligent cabling	62	Flame Test Listing: NEC OFNR-LS (ETL) and c(ETL) or equivalent	Recent amendments to the standards have updated the classification from OFNR-LS to OFNR-ST1. We request that the standard mentioned be updated accordingly. The clause should be revised as follows:	Kindly refer Revised Technical specification

583	Intelligent cabling	62	Missing Security clause which was there is earlier project of ERNET vide Tender No. GEM/2023/B/3273791 dated 18.03.2023 vide Annexure-C Clarifications/Explanations dated 18.04.2023 page no. 165 Should detect standard MPO and LC patch cords from and OEM	The proposed solution panels (fiber or copper) should be able to detect standard and any type of proprietary patch cords that are inserted into the panel. This is highly critical from a security point of view, as any solution not supporting this feature can expose the network to external security threats. This is because if the panel should not detect a standard patch cord, then the user/network manager will not get an alert that a patch cord has been inserted in a port. The following clause should be included in the specifications: **Panel should be able to detect standard and proprietary patch cords with an alert of the event sent to the software. The same should be demonstrated by the OEM / Bidder.**	As per Tender Document
584	Intelligent cabling	67	Attenuation: 1.00 dB/km @ 1,300 nm | 2.20 dB/km @ 953 nm 3.00 dB/km @ 850 nm	We recommend that the specification should be removed as it provides no additional benefit. The important parameter that impacts the performance is the insertion loss value, which has been asked in the specification. Also OM4 which is a multimode fiber and governed by international standards specifies only 2 wavelengths, 1300 nm and 850 nm. Hence 953 nm is not a defined wavelength for OM4 multimode fiber. The clause could be amended as well: Attenuation: 1.00 dB/km @ 1,300 nm | 3.00 dB/km @ 850 nm	Kindly refer Revised Technical specification
585	Intelligent cabling	67	Insertion Loss, maximum: 0.47 dB	The asked insertion loss value of 0.35 dB is very high for a high quality and high performance module. Insertion loss is the most critical performance parameter in a fiber component. To ensure that high speed applications, today or in the future, should be supported, the insertion loss should not be more than 0.35 dB. The clause should be ammended to the following: **Insertion Loss, maximum: 0.35 dB**	As per Tender Document
586	Intelligent cabling	68	Connector type: LC/UPC to LC/UPC, Fiber patch cord 1.7mm / 3.5mm. Riser	It is prefered in a Data Center enviornment to have a small diameter patch cord to manage the large volumn of patch cords inside a rack. Therefore request you to allow 1.6 mm diameter as well. The clause should be ammended to the following: **Connector type: LC/UPC to LC/UPC, Fiber patch cord 1.6mm / 1.7mm / 3.5mm. Riser**	Kindly refer Revised Technical specification
587	Intelligent cabling	68	Color: Aqua color for cable and Beige color for connector	Typically, the connector color for an LC connector is Black or Beige. We request that Black connectors also be permitted, or that the connector color be made color-independent. The clause should be revised as follows: Color: Lime Green color/Aqua color for cable and connector color as per OEM	Kindly refer Revised Technical specification
588	Intelligent cabling	68	Flame Test Listing: NEC OFNR-LS (ETL) and c(ETL) or equivalent	Recent amendments to the standards have updated the classification from OFNR-LS to OFNR-ST1. We request that the standard mentioned be updated accordingly. The clause should be revised as follows: Flame Test Listing: NEC OFNR-ST1 (ETL) / NEC OFNR-LS (ETL) and c(ETL) or equivalent	NEC OFNR-ST1 (ETL) / NEC OFNR-LS (ETL) and c(ETL)/ UL 60950-1 or equivalent
589	Intelligent cabling	68	Insertion Loss, maximum: 0.3 dB	The asked insertion loss value of 0.30 dB is very high for a high quality and high performance fiber patch cord. Insertion loss is the most critical performance parameter in a fiber component. To ensure that high speed applications, today or in the future, should be supported, the insertion loss should not be more than 0.15 dB for fiber patch cords. The clause should be ammended to the following: **Insertion Loss, maximum: 0.15 dB**	As per Tender Document

590	Intelligent cabling	68	Return Loss, minimum: 27 dB	The asked return loss value of 27 dB is very low for a high quality patch cord connector. Return loss along with Insertion loss is one of the most critical performance parameters in a fiber component. To ensure that high speed applicatoins, today or in the future, should be supported, the return loss value should not be lower than 35 dB for fiber patch cords. The clause should be ammended to the following: **Return Loss, minimum: 35 dB**	As per Tender Document
591	Intelligent cabling	73	4) The AIM System Monitor shall be able to display live end-to-end tracing information on its screen during patching activities. The screen may be a fixed unit or portable unit fixed in the racks using suitable mount/brackets. Both network rack should have one dedicated (AIM) Intelligent system monitor. Bidder shall configure one Intelligent system monitor two Server racks. 9) AIM monitor display system should have the capacity to monitor three RACKs	Please clarify whether the AIM system monitor should monitor two (2) server racks or three (3) server racks as clause 4 and 9 specify different quantity.	Kindly refer Revised Technical specification
592	Intelligent cabling	74	Missing Clause: Each individual copper and fiber port must have a push / membrane button to trace the circuit from end to end. The circuit trace must also appear on the AIM system monitor display.	This is an essential feature that must be included in the AIM system. The trace button on the panel enables users to quickly access end-to-end circuit details for a specific port. Upon pressing the button, the user should be able to view the complete circuit details on the AIM system monitor, along with additional information such as VLAN details. This functionality must be part of the standard AIM solution offering. Without it, users would be forced to rely solely on the software, which may be located remotely.	As per Tender Document
593	Intelligent cabling	97	The bid should include OEM professional services for the successful implementation of project. The OEM professional services shall include but not limited to solution architecture, design, installation, preparation of acceptance test plan & procedure with expected results and end user training leading to OEM Certification. The above activities should be jointly done by the Contractor and the OEM, as per the best security practices for the final acceptance.	Installation of the passive structured cabling and AIM system is implemented by OEM certified system integrators for most OEMs if not all. Therefore passive OEMs do not provide professional services as part of their offerings. OEMs can help and offer technical guidance to the system integrators. It is requested that Passive Structured Cabling and AIM OEMs be exempted from this clause. The clause should be amended to the following: The bid should include OEM professional services (except for Passive Structured Cabling and AIM) for the successful implementation of project. The OEM professional services shall include but not limited to solution architecture, design, installation, preparation of acceptance test plan & procedure with expected results and end user training leading to OEM Certification. The above activities should be jointly done by the Contractor and the OEM, as per the best security practices for the final acceptance. For Passive OEMs, regular Site audit clause can be added to ensure smooth implmentation.	In Case of Intelligent cabling, OEM Shall issue undertaking that OEM doesn't provide professional services. Accordingly implementation may be done by OEM certified agency.
594	SSL VPN	134	The device should support on demand provisioning of L3 VPN client using ActiveX or JAVA applet, standalone and command line L3 VPN client support	Justification: Both ActiveX by Microsoft and Java applet from Oracle have been deprecated due serious security issues. The Browser based clients should not be built using ActiveX or JAVA applet. Suggestive Clause: The device should support browser based VPN access, standalone and command line L3 VPN client for Windows, Mac, Linux, iOS and Android.	Kindly refer Revised Technical specification

595	l balancer with	145	The solution must be appliance based, 1U rack mountable and it should be having internal redundant Power Supply from day one.	**Justification:** The clause specifies a 1U rack-mountable appliance with internal redundant power supply. However, the problem highlights the need for a high number of ports and high throughput, which may require more space and better cooling. A 2U rack is suggested to accommodate these requirements without compromising performance or reliability. **Suggestive Clause:** The solution must be a 2U rack-mountable appliance with internal redundant power supply, ensuring support for high port density and throughput requirements from day one.	Kindly refer Revised Technical specification
596	EMS	33, 286	OEM of EMS Solution should be SOC2, CMMI Level 3, ISO 27001&ISO 27034 certified	Changes: OEM of EMS Solution should be CMMI Level 3, ISO 27001&ISO 27034 certified **Justification for change:** **SOC 2 certification is currently limiting broader OEM participation, as only 2-3 OEMs possess this certification. We respectfully request the authority to consider an alternative approach. Instead of mandating SOC 2 certification, it could be required that products demonstrate vulnerability-free status through VAPT (Vulnerability Assessment and Penetration Testing) reports issued by CERT-IN empaneled vendors**	The Clause may be read as : OEM of EMS Solution should be SOC2 / SOC3 / CMMI Level 3, ISO 27001 & ISO 27034 certified
597	EMS	33, 287	EMS should have performed the installation / commissioning at 5 projects with minimum 2500 nodes in each project.	EMS should have performed the installation / commissioning at 3 projects with minimum 2500 nodes in each project. **Justification for change:** **This clause appears to favor specific OEMs. We kindly request the authority to provide relaxation by allowing consideration of experience in three projects. Additionally, given the nature of the project, you may require experience in monitoring 10,000+ nodes in each of these three projects**	Kindly refer Revised Technical specification
598	NAC (included AAA)	151,1	The solution must provide Authentication, Authorization and Accounting (AAA) services using TACACS, Profiling, Posturing, Guest Management from a single platform	The solution must provide Authentication, Authorization and Accounting (AAA) services using TACACS+, Profiling, Posturing, Guest Management from a single platform **Justification for change:** **TACACS is a Cisco proprietary protocol. To ensure broader OEM participation, we kindly request the authority to mandate the use of TACACS+, which is an industry-standard protocol."**	The solution must provide Authentication, Authorization and Accounting (AAA) services using TACACS/TACACS+, Profiling, Posturing, Guest Management from a single platform
599	NAC (included AAA)	151,9	The solution must support agent-based deployment and provide deep compliance check for Meeting regulatory compliance requirements such as GDPR, HIPAA, PCI DSS, SOX, or GLBA revolve around knowing “who, what, when and where” for devices and users on your network and controlling access to the data your company needs to keep secure.	The solution must support agent-based deployment revolve around knowing “who, what, when and where” for devices and users on your network and controlling access to the data your company needs to keep secure. **Justification for Change: Compliance checking is not a standard feature of NAC solutions. In this RFP, specific tools have been mentioned for compliance checking, making this clause OEM-specific. To ensure broader OEM participation, we kindly request the removal of the compliance check requirement**	The solution must support agent-based deployment should revolve around knowing “who, what, when and where” for devices and users on your network and controlling access to the data your company needs to keep secure.

600	EMS	ge No. 3	222. The solution should have its own IT Service Management (ITSM) / IT helpdesk solution which is certified on ITIL v4 atleast 5 practices.Should provide an GUI interface w.r.t emails.	We recommend the authority to kindly update the requirements and replace this clause as follows to ensure selection of a proven Helpdesk solution: **"The proposed Helpdesk solution must be ITIL-certified across at least 12 key ITIL processes, such as Incident Management, Request Management, Problem Management, Change Management, Availability Management, and Event Management. Documentary proof of the ITIL certification, covering these processes, should be provided at the time of bidding to verify compliance and ensure the solution's adherence to ITIL best practices."**	May refer to respective revised clause
601	EMS	ge No. 3	59. Reports shall contain visualizations utilizing the applicable graphic types such as Bar Chart, Gauge , Pie Chart, Scatter Plot, Simple Value, Table, Time Series, User Image, User Text etc.	Requesting clarification from the authority regarding the specific requirements for user images and user text in the report. Could you please elaborate on what exactly is expected and how these elements should be presented in the report?	Some of the common usage of User Images & User Text include Logo & Special Text insertion in reports ; These will be required in other such customized reports.
602	EMS	ge No. 3	131. The platform must consolidate monitoring events from across layers such as Network, Server, Database, 3rd party tools (monitoring solutions to monitor key DC elements like wires / cables etc.)	Passive components cannot be monitored using NMS. Kindly exclude them from the scope of NMS/EMS.	No Change; Monitoring here is via integration with 3rd Party tools such as AIM
603	Storage Server	3	Total 2TB or higher RAM, DDR5 5000+ MHz ECC REG DIMM	For such a huge memory capacity it is recommended to adopt a monolithic architecture for DRAM in datacenter, as it offers**lower power consumption**, enchanced performance and simpler design that **minimizes signal integrity issues**. This will not only optimise the TCO but also the department can leverage more robust architecture. Request you to kindly consider the same.	As per Tender Document
604	Storage Server	3	Total 2TB or higher RAM, DDR5 5000+ MHz ECC REG DIMM	The specifications provided only outline the total DRAM requirement. To ensure consistency across the proposal, we kindly request that you include the capacity details for each individual RAM module to be considered in the proposal.	As per Tender Document
605	Storage Server	3	Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS SSD/M.2 NVME SSD Each SSD spec: 960GB+ Capacity, Write Intensive, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size	The RFP specifies the use of SAS SSDs, which are increasingly becoming obsolete as market adoption shifts towards newer technologies. While NVMe is the Next-gen SSD solution, SAS SSD are based on older technology and their market share is steadily declining. For optimal server performance; faster boot times, OS loading - adopting NVMe not only aligns with current technological trends but also ensures long term scalability, better throughput and overall performance. This will enable the Upcoming datacenter to be more future ready and efficient solution not only for the current applications but also for the future applications. So Request you to kindly restrict the RFP to NVMe SSDs instead of both SAS and NVMe.	As per Tender Document

606	Storage Server	3	Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS SSD/M.2 NVME SSD Each SSD spec: 960GB+ Capacity, **Write Intensive**, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have **150K+/100K+** Random Read/Write IOPS at 4K block size	Since these drives are intended for boot purpose, they need to handle both read and write intensive opertions efficiently. To ensure optimal performance and reliability, we recommend increasing the ramdom read IOPS to be **atleast 1000K and Random writes IOPS to be atleast 250K and industry standard 3 DWPD**. This enhancement will significantly improve the responsiveness and overall throughput of boot operations, enabling faster system startup time and more reliable performance under heavy workloads. This in turn will not only i**mprove the performance but also in tern reduce the TCO.**	Kindly refer Revised Technical specification
607	Storage Server	4	Minimum Storage of 1440 TB With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	Recommend using 30TB TLC NVMe SSDs instead of high-capacity HDDs reduces server footprint and power consumptions, optimising TCO while enchaning data security and longevity. Request you to kindly consider the architecture based on SSDs rather than HDDs.	As per Tender Document
608	Storage Server	4	Minimum Storage of 1440 TB With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	QD for Random read/ write IOPS is recommended to be calculated at industry standard QD256.	As per Tender Document
609	Storage Server	4	Minimum Storage of 1440 TB With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	Request you to kindly modify the following as per current SSD standards in the industry: Random R/W IOPS (at 4KB, **QD256**): 1000+/400+ Sequential R/W speed for 64 KB blocks: 7000+/5900+, 120+ MB/s	As per Tender Document
610	Storage Server	4	Minimum Storage of 1440 TB With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s Note: 1. Single DAS expansion can be used. However, the effective I/O throughput of all the disks combined should not be impacted due to any DAS expansion connector limitations. 2. DAS and Server should be compatible and support of DAS to be provided by Server OEM only. Server OEM shall give undertaking for the support of DAS on their letterhead.	DAS based architecturess with high-capacity HDDs result in slow performances and are not suitable for high performance environments, potentially increasing TCO and adding a point of failure in the achritecture. For the industry standard recommendations request you to kindly refer to the following: Uptime Institute's Tier Standards Storage Networking Industry Association (SNIA) best practices And it would be recommended to use server-storage architecture without DAS expansions.	As per Tender Document
611	Storage Server	5	Dedicated Hardware Raid controller= RAID 0,1,5,6,10, 50, 60, SATA/SAS-3 connectivity, 4+ GB cache, battery or flash backed protection for all HDDs. All the HDDs in the server should be configurable under a single virtual drive with RAID 5,6,50,60. Storage management including raid configuration. Required support for SED (Self Encrypting Drive) and ISE (Instant Sanitise Erase) should be available in RAID controller	As per the datacenter optimal recommendation, sofware based RAID should be preffered for NVMe drives over SATA/SAS controllers, as it optimises TCO and boots performances.	As per Tender Document
612	Storage Server	5	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe Sequential read 6,200 MB/s, Sequential write 2,600 MB/s (Sequential performance 128KB block size with queue depth 32) - Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS (Random Performance 4K block size with queue depth 256) **Latency, read/write 120/20 µs (4KB transfer size with queue depth 1)** Endurance 3 DWPD with additional 2 free slots for populating additional cache drives.	Proprietry specs for latency, this is not industry standard. Request you to kindly remove these of specify industry standard latency specifications	As per Tender Document

613	Storage Server	5	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe **Sequential read 6,200 MB/s, Sequential write 2,600 MB/s** (Sequential performance **128KB block size with queue depth 32**) - **Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS** (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1) Endurance 3 DWPD with additional 2 free slots for populating additional cache drives.	Queue Depth 32 is not industry standard and all the potential players across the industry develop products based on industry standard of QD 128. Request you to kindly change the same as below: Sequential read 6,800 MB/s, Sequential write 5,300 MB/s (Sequential performance 128KB block size with queue depth 128) Random read (4K) Up to 1,100K IOPS, Random write (4K) Up to 390K IOPS	Kindly refer Revised Technical specification
614	Storage Server	5	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe Sequential read **6,200 MB/s, Sequential write 2,600 MB/s** (Sequential performance 128KB block size with queue depth 32) - Random read **(4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS** (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1) Endurance 3 DWPD with additional 2 free slots for populating additional cache drives.	Cache Drives are critical and should have industry standard optimal parameters for the sequenctial and ramdom read writes, hence, request you to kindly modify the following to current industry standards: Sequential read 6,800 MB/s, Sequential write 5,300 MB/s Random read (4K) Up to 1,100K IOPS, Random write (4K) Up to 390K IOPS	Kindly refer Revised Technical specification
615	Storage Server	5	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe Sequential read 6,200 MB/s, Sequential write 2,600 MB/s (Sequential performance 128KB block size with queue depth 32) - Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1) Endurance 3 DWPD with additional 2 free slots for populating additional cache drives.	By using NVMe drives instead of HDDs for storage, the need of separate cache drives will be eliminated, as NVMe's exceptional performance already delivers faster data access and will significantly increase the TCO.	Kindly refer Revised Technical specification
616	Application Server	6	Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS/M.2 SSD Each SSD spec: 960GB+ Capacity , Write Intensive, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block s size	The RFP specifies the use of SAS SSDs, which are increasingly becoming obsolete as market adoption shifts towards newer technologies. While NVMe is the Next-gen SSD solution, SAS SSD are based on older technology and their market share is steadily declining. For optimal server performance; faster boot times, OS loading - adopting NVMe not only aligns with current technological trends but also ensures long term scalability, better throughput and overall performance. This will enable the Upcoming datacenter to be more future ready and efficient solution not only for the current applications but also for the future applications. So Request you to kindly restrict the RFP to NVMe SSDs instead of both SAS and NVMe.	Kindly refer Revised Technical specification
617	Application Server	6	Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS/M.2 SSD Each SSD spec: 960GB+ Capacity , Write Intensive, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block s size	Since these drives are intended for boot purpose, they need to handle both read and write intensive opertions efficiently. To ensure optimal performance and reliability, we recommend increasing the ramdom read IOPS to be **atleast 1000K and Random writes IOPS to be atleast 250K and industry standard 3 DWPD**. This enhancement will significantly improve the responsiveness and overall throughput of boot operations, enabling faster system startup time and more reliable performance under heavy workloads. This in turn will not only i**mprove the performance but also in tern reduce the TCO.**	Kindly refer Revised Technical specification
618	Application Server	6	Storage Each Server With Minimum Storage of 200 TB,With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency : between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	Recommend using 30TB TLC NVMe SSDs instead of high-capacity HDDs reduces server footprint and power consumptions, optimising TCO while enchaning data security and longevity. Request you to kindly consider the architecture based on SSDs rather than HDDs.	As per Tender Document

619	Application Server	6	Storage Each Server With Minimum Storage of 200 TB,With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency : between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	QD for Random read/ write IOPS is recommended to be calculated at industry standard QD256. Request you to incorporate the same.	As per Tender Document
620	Application Server	6	Storage Each Server With Minimum Storage of 200 TB,With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency : between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	Request you to kindly modify the following as per current SSD standards in the industry and sequential parameters are missing for the drives to be of optimal level: Random R/W IOPS (at 4KB, **QD256**): **1000+/400+** Sequential R/W speed for 64 KB blocks: 7000+/5900+, 120+ MB/s	As per Tender Document
621	Application Server	6	Dedicated Hardware Raid controller= RAID 0,1,5,6,10, 50, 60, SATA/SAS-3 connectivity, 4+ GB cache, battery or flash backed protection for all HDDs. All the HDDs in the server should be configurable under a single virtual drive with RAID 5,6,50,60. Storage management including raid configuration. Required support for SED (Self Encrypting Drive) and ISE (Instant Sanitise Erase) should be available in RAID controller	As per the datacenter optimal recommendation, sofware based RAID should be preffered for NVMe drives over SATA/SAS controllers, as it optimises TCO and boots performances.	As per Tender Document
622	Application Server	7	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe Sequential read 6,200 MB/s, Sequential write 2,600 MB/s (Sequential performance 128KB block size with queue depth 32) - Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS (Random Performance 4K block size with queue depth 256) **Latency, read/write 120/20 µs (4KB transfer size with queue depth 1)**	Proprietry specs for latency, this is not industry standard. Request you to kindly remove these of specify industry standard latency specifications	Kindly refer Revised Technical specification
623	Application Server	7	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe **Sequential read 6,200 MB/s, Sequential write 2,600 MB/s** (Sequential performance **128KB block size with queue depth 32**) - **Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS** (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1)	Queue Depth 32 is not industry standard and all the potential players across the industry develop products based on industry standard of QD 128. Request you to kindly change the same as below: Sequential read 6,800 MB/s, Sequential write 5,300 MB/s (Sequential performance 128KB block size with queue depth 128) Random read (4K) Up to 1,100K IOPS, Random write (4K) Up to 390K IOPS	Kindly refer Revised Technical specification
624	Application Server	7	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe Sequential read **6,200 MB/s, Sequential write 2,600 MB/s** (Sequential performance 128KB block size with queue depth 32) - Random read **(4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS** (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1)	Cache Drives are critical and should have industry standard optimal parameters for the sequenctial and ramdom read writes, hence, request you to kindly modify the following to current industry standards: Sequential read 6,800 MB/s, Sequential write 5,300 MB/s Random read (4K) Up to 1,100K IOPS, Random write (4K) Up to 390K IOPS	Kindly refer Revised Technical specification
625	Application Server	7	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe Sequential read 6,200 MB/s, Sequential write 2,600 MB/s (Sequential performance 128KB block size with queue depth 32) - Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1)	By using NVMe drives instead of HDDs for storage, the need of separate cache drives will be eliminated, as NVMe's exceptional performance already delivers faster data access and will significantly increase the TCO.	Kindly refer Revised Technical specification
626	Application Server	7	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe Sequential read 6,200 MB/s, Sequential write 2,600 MB/s (Sequential performance 128KB block size with queue depth 32) - Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1)	Endurance parameter for the cache drive is missing, DWPD 1 or 3 should be defined for parity in the proposal	Kindly refer Revised Technical specification

627	Web Server	9	Boot Storage: 2 no:s x Enterprise SAS SSD/M.2 NVME SSD, Each SSD spec: 400GB+ Capacity, Write Intensive, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size	The RFP specifies the use of SAS SSDs, which are increasingly becoming obsolete as market adoption shifts towards newer technologies. While NVMe is the Next-gen SSD solution, SAS SSD are based on older technology and their market share is steadily declining. For optimal server performance; faster boot times, OS loading - adopting NVMe not only aligns with current technological trends but also ensures long term scalability, better throughput and overall performance. This will enable the Upcoming datacenter to be more future ready and efficient solution not only for the current applications but also for the future applications. So Request you to kindly restrict the RFP to NVMe SSDs instead of both SAS and NVMe.	Kindly refer Revised Technical specification
628	Web Server	9	Boot Storage: 2 no:s x Enterprise SAS SSD/M.2 NVME SSD, Each SSD spec: 400GB+ Capacity, Write Intensive, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size	Since these drives are intended for boot purpose, they need to handle both read and write intensive opertions efficiently. To ensure optimal performance and reliability, we recommend increasing the ramdom read IOPS to be **atleast 1000K and Random writes IOPS to be atleast 250K and industry standard 3 DWPD**. This enhancement will significantly improve the responsiveness and overall throughput of boot operations, enabling faster system startup time and more reliable performance under heavy workloads. This in turn will not only i**mprove the performance but also in tern reduce the TCO.**	Kindly refer Revised Technical specification
629	Web Server	9	Storage 2 nos x 18+ TB Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours) SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	Recommend using 30TB TLC NVMe SSDs instead of high-capacity HDDs reduces server footprint and power consumptions, optimising TCO while enchaning data security and longevity. Request you to kindly consider the architecture based on SSDs rather than HDDs.	As per Tender Document
630	Web Server	9	Storage Each Server With Minimum Storage of 200 TB,With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency : between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	QD for Random read/ write IOPS is recommended to be calculated at industry standard QD256. Request you to incorporate the same.	As per Tender Document
631	Web Server	9	Storage Each Server With Minimum Storage of 200 TB,With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency : between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	Request you to kindly modify the following as per current SSD standards in the industry and sequential parameters are missing for the drives to be of optimal level: Random R/W IOPS (at 4KB, **QD256**): **1000+/400+** Sequential R/W speed for 64 KB blocks: 7000+/5900+, 120+ MB/s	As per Tender Document
632	Web Server	9	Dedicated Hardware Raid controller= RAID 0,1,5,6,10, 50, 60, SATA/SAS-3 connectivity, 4+ GB cache, battery or flash backed protection for all HDDs. All the HDDs in the server should be configurable under a single virtual drive with RAID 5,6,50,60. Storage management including raid configuration. Required support for SED (Self Encrypting Drive) and ISE (Instant Sanitise Erase) should be available in RAID controller	As per the datacenter optimal recommendation, sofware based RAID should be preffered for NVMe drives over SATA/SAS controllers, as it optimises TCO and boots performances.	As per Tender Document

633	Load Balancer Server	11	Boot Storage subsystem with HW RAID 1 having 2 no:s x Enterprise SAS SSD/M.2 NVME SSD, Each SSD spec: 400GB+ Capacity , Write Intensive, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size	The RFP specifies the use of SAS SSDs, which are increasingly becoming obsolete as market adoption shifts towards newer technologies. While NVMe is the Next-gen SSD solution, SAS SSD are based on older technology and their market share is steadily declining. For optimal server performance; faster boot times, OS loading - adopting NVMe not only aligns with current technological trends but also ensures long term scalability, better throughput and overall performance. This will enable the Upcoming datacenter to be more future ready and efficient solution not only for the current applications but also for the future applications. So Request you to kindly restrict the RFP to NVMe SSDs instead of both SAS and NVMe.	Kindly refer Revised Technical specification
634	Load Balancer Server	11	Boot Storage subsystem with HW RAID 1 having 2 no:s x Enterprise SAS SSD/M.2 NVME SSD, Each SSD spec: 400GB+ Capacity , Write Intensive, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size	Since these drives are intended for boot purpose, they need to handle both read and write intensive opertions efficiently. To ensure optimal performance and reliability, we recommend increasing the ramdom read IOPS to be **atleast 1000K and Random writes IOPS to be atleast 250K and industry standard 3 DWPD**. This enhancement will significantly improve the responsiveness and overall throughput of boot operations, enabling faster system startup time and more reliable performance under heavy workloads. This in turn will not only i**mprove the performance but also in tern reduce the TCO.**	Kindly refer Revised Technical specification
635	Load Balancer Server	12	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe Sequential read 6,200 MB/s, Sequential write 2,600 MB/s (Sequential performance 128KB block size with queue depth 32) - Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS (Random Performance 4K block size with queue depth 256) **Latency, read/write 120/20 µs (4KB transfer size with queue depth 1)**	Proprietry specs for latency, this is not industry standard. Request you to kindly remove these of specify industry standard latency specifications	Kindly refer Revised Technical specification
636	Load Balancer Server	12	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe **Sequential read 6,200 MB/s, Sequential write 2,600 MB/s** (Sequential performance **128KB block size with queue depth 32**) - **Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS** (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1)	Queue Depth 32 is not industry standard and all the potential players across the industry develop products based on industry standard of QD 128. Request you to kindly change the same as below: Sequential read 6,800 MB/s, Sequential write 5,300 MB/s (Sequential performance 128KB block size with queue depth 128) Random read (4K) Up to 1,100K IOPS, Random write (4K) Up to 390K IOPS	Kindly refer Revised Technical specification
637	Load Balancer Server	12	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe Sequential read **6,200 MB/s, Sequential write 2,600 MB/s** (Sequential performance 128KB block size with queue depth 32) - Random read **(4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS** (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1)	Cache Drives are critical and should have industry standard optimal parameters for the sequenctial and ramdom read writes, hence, request you to kindly modify the following to current industry standards: Sequential read 6,800 MB/s, Sequential write 5,300 MB/s Random read (4K) Up to 1,100K IOPS, Random write (4K) Up to 390K IOPS	Kindly refer Revised Technical specification
638	Load Balancer Server	12	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe Sequential read 6,200 MB/s, Sequential write 2,600 MB/s (Sequential performance 128KB block size with queue depth 32) - Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1)	By using NVMe drives instead of HDDs for storage, the need of separate cache drives will be eliminated, as NVMe's exceptional performance already delivers faster data access and will significantly increase the TCO.	Kindly refer Revised Technical specification

639	Load Balancer Server	12	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe Sequential read 6,200 MB/s, Sequential write 2,600 MB/s (Sequential performance 128KB block size with queue depth 32) - Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1)	Endurance parameter for the cache drive is missing, DWPD 1 or 3 should be defined for parity in the proposal	Kindly refer Revised Technical specification
640	Utility Server	13	2 no:s x Enterprise SAS/M.2 SSD, Each SSD spec: 960GB or more Capacity , Write Intensive, Read (1 GB/s or more) Write (500 MB/s or more), MTBF = 2 million hours or more, 2000 TBW or more, 2 DWPD or more	The RFP specifies the use of SAS SSDs, which are increasingly becoming obsolete as market adoption shifts towards newer technologies. While NVMe is the Next-gen SSD solution, SAS SSD are based on older technology and their market share is steadily declining. For optimal server performance; faster boot times, OS loading - adopting NVMe not only aligns with current technological trends but also ensures long term scalability, better throughput and overall performance. This will enable the Upcoming datacenter to be more future ready and efficient solution not only for the current applications but also for the future applications. So Request you to kindly restrict the RFP to NVMe SSDs instead of both SAS and NVMe.	Kindly refer Revised Technical specification
641	Utility Server	13	2 no:s x Enterprise SAS/M.2 SSD, Each SSD spec: 960GB or more Capacity , Write Intensive, Read (1 GB/s or more) Write (500 MB/s or more), MTBF = 2 million hours or more, 2000 TBW or more, 2 DWPD or more	Since these drives are intended for boot purpose, they need to handle both read and write intensive opertions efficiently. To ensure optimal performance and reliability, we recommend increasing the ramdom read IOPS to be **atleast 1000K and Random writes IOPS to be atleast 250K and industry standard 3 DWPD**. This enhancement will significantly improve the responsiveness and overall throughput of boot operations, enabling faster system startup time and more reliable performance under heavy workloads. This in turn will not only i**mprove the performance but also in tern reduce the TCO.**	refer modifed Kindly refer Revised Technical specification
642	Utility Server	13	6 or more no:s x 8 TB or more Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12 Gb/s, 7200 RPM, 256 MB Cache. 3.5", MTBF = 8 Lakhs hours) System must have atleast 12 x LFF front accessible Hot-Swap Drive Bays with backplane supporting SAS/SATA/NVMe drives	Recommend using NVMe SSDs instead of high-capacity HDDs reduces server footprint and power consumptions, optimising TCO while enchaning data security and longevity. Request you to kindly consider the architecture based on SSDs rather than HDDs.	As per Tender Document
643	Utility Server	13	6 or more no:s x 8 TB or more Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12 Gb/s, 7200 RPM, 256 MB Cache. 3.5", MTBF = 8 Lakhs hours) System must have atleast 12 x LFF front accessible Hot-Swap Drive Bays with backplane supporting SAS/SATA/NVMe drives	QD for Random read/ write IOPS is recommended to be calculated at industry standard QD256. Request you to incorporate the same.	As per Tender Document
644	Utility Server	13	6 or more no:s x 8 TB or more Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12 Gb/s, 7200 RPM, 256 MB Cache. 3.5", MTBF = 8 Lakhs hours) System must have atleast 12 x LFF front accessible Hot-Swap Drive Bays with backplane supporting SAS/SATA/NVMe drives	Request you to kindly add the following SSD standards parameters , Random & sequential parameters are missing for the drives to be of optimal level: Random R/W IOPS (at 4KB, **QD256**): **1000+/400+** Sequential R/W speed for 64 KB blocks: 7000+/5900+, 120+ MB/s	As per Tender Document
645	Utility Server	rt A Page	Virtualization Stack: Enterprise virtualization software license for the system for asked cores to be supplied with the system. System offered must be certified with offered virtualization software, certificate must be submitted with technical bid	**Request:** Request to add detailed technical specifications **Justification**: In reference to the guidelines of MeitY for deploying ICT solutions leveraging the latest technologies, virtualization plays a crucial role to ensure scalable and secure infrastructure that enables enhanced application availability and performance. However, the current RFP only covers basic specifications. We kindly request that you provide comprehensive specifications for virtualization stack, similar to those outlined for other products in the RFP. We have attached the detailed generic virtualization specifications for inclusion in the RFP. Request to please incorporate the same	As per Tender Document

646	l balancer with	gestive Cl	Suggestive Clause	**Justification:** the proposed solution should offers flexibility and adaptability, enabling custom traffic management decisions based on real-time events. By supporting a scripting language, it allows for the creation of tailored rules to optimize application performance, handle dynamic scenarios, and meet specific operational requirements effectively. **Suggestive Clause:** The proposed solution should support scripting language for events based rules creation to make traffic management decision using scripting language.	As per Tender Document
647		Suggestive Cl	Suggestive Clause	**Justification:** The proposed solution should support limiting user sessions (cookies) per application or virtual server. This feature ensures that when the number of active sessions reaches the configured limit, new users are blocked from accessing the application. This helps maintain the availability and performance of web/app servers, allowing already logged-in users to complete their transactions without degradation in service. **Suggestive Clause:** The proposed solution should support limitation of users sessions (cookies) per application/vserver. Through this feature, SLB shall insure that new user (beyond the configured threshold limit) get blocked, so as to insure availability of resources on WEB / APP servers already logged in users to complete their transactions.	As per Tender Document
648		Suggestive Cl	Suggestive Clause	**Justification:** Including an anti-bot SDK for mobile applications ensures comprehensive protection for both mobile apps and Web APIs, safeguarding against automated attacks like credential stuffing and data scraping. By using an SDK from the same OEM as the WAF, seamless integration and consistent threat intelligence across platforms are achieved, enhancing security efficacy while simplifying deployment and management. **Suggestive Clause:** The solution should support anti-bot SDK for mobile application for protecting mobile apps and Web APIs. The anti-bot mobile SDK should be available for Android and iOS and should be from same OEM as WAF	As per Tender Document

649	Suggestive Cl		Suggestive Clause	**Justification:** Anti-DDoS solution with advanced score-based traffic shaping leverages machine learning, built-in signatures, and user-defined rules to provide dynamic, adaptive protection. Machine learning enables real-time detection and mitigation of both known and emerging threats, while score-based traffic shaping prioritizes legitimate traffic and limits malicious traffic, ensuring minimal disruption. The combination of these elements enhances threat intelligence, resource efficiency, and customization, making the solution effective against increasingly sophisticated DDoS attacks and adaptable to future challenges. **Suggestive Clause:** The proposed solution should have advanced score based traffic shaping where score is computed from machine-learning, built-in signatures and user defined rules	As per Tender Document
650	Suggestive Cl		Suggestive Clause	**Justification:** Link load balancing solution with a DNS firewall feature enhances network security by blocking access to known malicious domains. This helps prevent threats such as phishing, malware downloads, and command-and-control communications, protecting users and infrastructure while maintaining optimal network performance. Integrating a DNS firewall ensures proactive threat prevention and improves overall network resilience. **Addditional Clause:** The proposed solution should have DNS firewall feature to block malicious domains	As per Tender Document
651	Suggestive Cl		Suggestive Clause	**Justification:** The proposed solution supports caching (static and dynamic) to store frequently accessed content closer to users, reducing server load and improving response times. It also enables gzip and deflate compression to shrink data sizes, saving bandwidth and speeding up content delivery. Together, these features optimize application performance and user experience. **Suggestive Clause:** The proposed solution should support caching (static & dynamic) and compression (gzip & deflate) for improving application performance and saving bandwidth	As per Tender Document
652	Non Smart Rac	162	Each rack should have 2 PDUs The 2 PDUs in each rack should have different chassis color for identification of UPS source. Electrical rating – Input – 230V, 32A, 1 Phase, 3-meter-long input cable with Splash proof IEC60309 input plug. For all 3Ph PDU it must have the color-coded alternating outlets based on the circuit color to identify the phase and help phase balancing when used as a three phase PDU. High temperature grade, operating temperature up to 60°C.	On point 21.1 of the 42U Rack it is mentioned the PDU is 3Ph and in the starting of document it is mentioned 1Ph, kindly clarify. And for 2 nos. Of PDU with 24 nos. Socket each, we need 800W to fit the PDU in side if they insist on 600W we have to mount multiple PDUs on 19" rail itself.	A Rack should be supplied with single three phase 32 Amp PDU, 42U 800x1200mm (WxD)

653	EMS	NA	clause addition	In order to select proven EMS/NMS (Enterprise Monitoring System/Network Monitoring System) solution with deployment experience in projects with similar magnitude, we recommend the authority to consider following clause in the NMS specification: **"The proposed NMS solution should have been successfully implemented in at least two State Data Centers or should be monitoring a minimum of 10,000 nodes across three deployments within State/Central Government or PSU projects in India. Documentary proof, such as Purchase Order (PO) copies and project sign-off/completion certificates, must be submitted at the time of proposal submission."**	As per Tender Document
654	EMS	NA	clause addition	In order to select solution with in-built database for ensuring better control and flexibility along with lower TCO, we recommend the authority to incorporate the below clause: **"The monitoring module of proposed solution must not use any third party database (including RDBMS and open source) to store data in order to provide full flexibility and control on collected data."**	As per Tender Document
655	EMS	NA	clause addition	In order to provide complete visibility of IT infrastructure including servers with micro level monitoring (on need basis) through which granular level details can be captured along with flexibility of monitoring through agent and agentless approach. Hence, we request the authority to add the following clause in the EMS specification: **"The proposed NMS solution must provide agentless as well as agent based monitoring for server infrastructure. The agents should be able to set polling interval as low as 1 second with low overhead on target server infrastructure."**	As per Tender Document
656	EMS	NA	clause addition	ISO and CIS standards are a set of security guidelines and best practices developed by the nonprofit organizations such as ISO and CIS. These standards provide detailed configuration recommendations and benchmarks for securing your enterprise network. The purpose of these benchmarks is to provide industry-recognized guidelines for secure system configuration. These benchmarks help the authority to enhance their security posture, mitigate risks, and ensure compliance with industry standards and regulatory requirements. Hence we request you to add the following cluase in the RFP **"The OEM of the proposed solution should possess Quality certifications ISO 9001, Information security certificate ISO 27001, Application security certificate ISO 27034 and CIS benchmark certificate. Documentary proof must be provided at the time of submission."**	As per Tender Document
657	EMS	389	OEM of EMS Solution should be SOC2, CMMI Level 3, ISO 27001&ISO 27034 certified	Kindly Remove SOC2 Certificate requirement.because this not a relevant certificate for this Product. as only service organizations that stores, processes, or transmits any kind of customer data, are likely need to be SOC 2 compliant (i.e. AWS, Gmail, icloud, dropbox etc.	May refer to respective revised clause
658	EMS	389	OEM should have performed the installation / commissioning at 5 projects with minimum 2500 nodes in each project.	Kindly relax this clause and shall be inline with current requirement (2 projects with 2500 nodes).	Kindly refer Revised Technical specification

659	EMS	367	13. The proposed solution should include hardware(s) and software(s) (including web application stack, database, any servers etc. required for accomplishing the scope of work and requirements) with operating system(s). Bidders must keep in mind the future and scalability of requirements before deciding for a hardware configuration.	Kindly confirm whether bidder need to consider separate server for EMS or same has already been considered in the server provided in the BoQ	Yes, separate server for EMS is supposed to be brought , its not considered in the BoQ . Refer to Clause 'o' at Annexure-1 (Technical Specifications) - "It may be noted by bidder that the required additional resources (any hardware &/or software) to run the solution(s)/equipment(s) should be factored in by bidder and available on Day-1 upon the equipment/solution delivery to support the complete functionality/features sought in the bid. It is understood that proposed hardware would be data centre suitable, rack mountable with redundant power supplies."
660	. (Technical Sp	191	**14.Virtualization Stack:**Enterprise virtualization software license for the system for asked cores to be supplied with the system. System offered must be certified with offered virtualization software, certificate must be submitted with technical bid	As per RFP except utility server no virtualization is required to consider by bidder for other servers.	As per Tender Document
661	Storage Server	181	4.Boot Storage subsystem:Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS SSD/M.2 NVME SSD Each SSD spec: 960GB+ Capacity, Write Intensive, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size	Kindly remove the performance parameters since these are OS drives only; and change the specifications as below: **Each SSD spec: 960GB SSD SAS, Mixed Use**	Kindly refer Revised Technical specification
662	Storage Server	182	5.Storage:With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	Kindly revise the clause as below: With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS **(at 4KB, QD16 or QD32)**: 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	as per tender document
663	Storage Server	182	8 - Hardware RAID Controller:All the HDDs in the server should be configurable under a single virtual drive with RAID 5,6,50,60. Storage management including raid configuration. Required support for SED (Self Encrypting Drive) and ISE (Instant Sanitise Erase) should be available in RAID controller.	We understand that only the drives asked for the capacity as asked in Storage i.e 1440TB shall confirm to SED and ISE. Kindly confirm. **Justification:** SED and ISE is a feature of the proposed HDD and will be supported by the RAID Controller only if the HDD is SED and ISE enabled.Kindly confirm if understanding is correct.	as per tender document
664	Application Server	184	4 - Boot Storage subsystem:Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS/M.2 SSD Each SSD spec: 960GB+ Capacity , **Write Intensive**, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size	Kindly modify the performance parameters since these are OS drives only; and change the specifications as below: **Each SSD spec: 960GB SSD SAS, Mixed Use**	Kindly refer Revised Technical specification

665	Application Server	184	5 - Storage:With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency : between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	Kindly change the specifications as below: With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS **(at 4KB, QD16 or QD32)**: 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	Kindly refer Revised Technical specification
666	Application Server	185	8 - Hardware RAID Controller:All the HDDs in the server should be configurable under a single virtual drive with RAID 5, 6, 50, 60 Storage management including raid configuration. Required support for SED (Self Encrypting Drive) and ISE (Instant Sanitise Erase) should be available in RAID controller.	We understand that only the drives asked for the capacity as asked in Storage i.e 1440TB shall confirm to SED and ISE. Kindly confirm. **Justification:** SED and ISE is a feature of the proposed HDD and will be supported by the RAID Controller only if the HDD is SED and ISE enabled.Kindly confirm if understanding is correct.	yes undertanding is correct
667	Web Server	186	2 - Processor:Processor: 2 Quantity (Dual socket) x Intel Xeon Gold/Platinum scalable series 5th Gen 8 core processor (3.1+ GHz base frequency, Cache Size 20+ MB) OR Processor: 2 Quantity (Dual socket) x AMD Epyc 9004 or latest Series, 8 core processor (3.1+ GHz base frequency, Cache Size 64+ MB)	Kindly Modify the specifications as below: - Processor: 2 Quantity (Dual socket) x Intel Xeon Gold/Platinum scalable series 5th Gen 8 core processor (3.1+ GHz base frequency, Cache Size 20+ MB) OR Processor: 2 Quantity (Dual socket) x AMD Epyc 9004 or latest Series, 8 core processor (3.0+ GHz base frequency, Cache Size 64+ MB)	Kindly refer Revised Technical specification
668	Web Server	187	4 - Boot Storage subsystem:Each SSD spec: 400GB+ Capacity, Write Intensive, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size	Kindly modify the performance parameters since these are OS drives only; and change the specifications as below: **Each SSD spec: 800GB SSD SAS ISE, Mixed Use**	Kindly refer Revised Technical specification
669	Web Server	187	5 - Storage:2 nos x 18+ TB Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours) SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	Kindly change the specifications as below: **Storage: 2 nos x 18+ TB Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours) SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms**	Kindly refer Revised Technical specification
670	Web Server	187	8 - Hardware RAID Controller:All the HDDs in the server should be configurable under a single virtual drive with RAID 5, 6, 50, 60 Storage management including raid configuration. Required support for SED (Self Encrypting Drive) and ISE (Instant Sanitise Erase) should be available in RAID controller.	We understand that only the drives asked for the capacity as asked in Storage i.e 2* 18TB shall confirm to SED and ISE. Kindly confirm. Pls note that SED and ISE is a feature of the proposed HDD and will be supported by the RAID Controller only if the HDD is SED and ISE enabled. Hope the understanding is correct.	understanding is correct

671	Utility Server	191	4 - Boot Storage subsystem:Each SSD spec: 960GB or more Capacity , Write Intensive, Read (1 GB/s or more) Write (500 MB/s or more), MTBF = 2 million hours or more, 2000 TBW or more, 2 DWPD or more	Kindly remove the performance parameters since these are OS drives only; and change the specifications as below: **Each SSD spec: 960GB SSD SAS, Mixed Use**	Kindly refer Revised Technical specification
672	Utility Server	191	5 - Storage:6 or more no:s x 8 TB or more Enterprise Drives, (Each HDD spec: CMR	Kindly Modify the drive capacity to 18TB for standardization. Kindly change the specifications as below: **Storage: 6 or more 8 TB Enterprise drives OR 3 nos of 18+ TB Enterprise Drives, (With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16 or QD32): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s**	as per tender document
673	Utility Server	191	7 - PCIe:All PCIe slots must support Gen 5 speed and supporting 10.5" Length based	Kindly modify the specifications as below:- **All PCIe slots must support Gen 4/5 speed and supporting X8/X16 and FH/ LP or 10.5" Length based Controllers.**	Kindly refer Revised Technical specification
674	Utility Server	191	16 - General Compliances:UEFI Specification v2.8 or above , SMBIOS Specification v3	This clause is conflicting with the clause under section "Common Management & Security Features for all Servers Pt. 4". Kindly remove the same. The aksed specifications under Pt. 4 asks for "UEFI specifications v2.7 and SMBIOS Specifications v3.3.0 or above" which we comply.	Kindly refer Revised Technical specification
675	Utility Server	192	17 - General Features:Storage (HDD) Drives: Sanitize Instant Erase, Self-Encrypting (SED). Required support should be available in RAID controller	Pls note that SED and ISE is a feature of the proposed HDD and will be supported by the RAID Controller only if the HDD is SED and ISE enabled. Kindly confirm if the understanding is correct.	understanding is correct
676	Utility Server	196	8 System Memory:3TB memory using DDR5 (4800 MHz or higher) operating at min. 4400MHz Server should be populated in balanced memory configuration.	Kindly Modify the specifications as below: Kindly note that as per best practices of OEM, 2TB is recommended for such AI workload specific systems. Hence kindly change it to 2TB memory using DDR5 (4800 MHz or higher) operating at min. 4400MHz Server should be populated in balanced memory configuration.	as per tender document

677	Monitoring and Management Tool for Servers	200	12 - Monitoring & Management Tool for Servers:iv. System tagging giving admin flexibility to provide metadata tags to each system to enable users to filter and sort systems based on user assigned attributes	Kindly modifythe specifications as below:- iv. System tagging giving admin flexibility to provide metadata tags to each system to enable users to filter and sort systems based on user assigned attributes **OR the management console should be enabled with Elastic search feature capable of accessing all information within the console**	Kindly refer Revised Technical specification
678	l balancer with	323	The Appliance must support minimum two 40/100Gig SFP Slots and 8 * 10G SFP+ slots populated with 10Gig SR and same should be upgradeable to 25Gig by changing transceivers only	The required throughput can be efficiently handled with fewer ports, ensuring optimal performance and cost-effectiveness. It is recommended to amend the clause as follows: "**The Appliance must support minimum two 40/100Gig SFP Slots and 8 * 10G SFP+ slots populated with 10Gig SR**."	Kindly refer Revised Technical specification
679	l balancer with	323	The solution must be appliance based, 1U rack mountable and it should be having internal redundant Power Supply from day one.	Request to modify the requirement to allow flexibility for the appliance to be **1U or 2U rack-mountable**, as this will enable bidders to propose solutions that best meet performance and scalability needs. This flexibility will not compromise functionality or power redundancy. It is suggested to amend the clause as "**The solution must be appliance based, 1U/2U rack mountable and it should be having internal redundant Power Supply from day one**"	Kindly refer Revised Technical specification
680	EMS	377	131. The platform must consolidate monitoring events from across layers such as Network, Server, Database, 3rd party tools (monitoring solutions to monitor key DC elements like wires / cables etc.)	Passive components cannot be monitored using NMS. Kindly exclude them from the scope of NMS/EMS.	No Change; Monitoring here is via integration with 3rd Party tools such as AIM
681	KVM Console	163	11. Built-in KVM switch should have min. two VGA local console ports.	Kindly revise the clause as " Built-in KVM switch should have min. two console ports" as it will be more generic Specification so more OEM can participate.	As per Tender Document
682	KVM Console	163	13. LCD KVM console should support min. resolutions up to 1366 x 768 @ 60Hz;	Kindly revise the clause as " LCD KVM console should support min. resolutions up to 1280 x 1024 @ 75Hz;" as it will be more generic Specification so more OEM can participate.	As per Tender Document
683	KVM Console	163	14. Operating temperature and Humidity of LCD console tray should be 0°C to 50°C	Kindly revise the clause as" Operating temperature and Humidity of LCD console tray should be 0°C to 40°C" since standard operating temp is 0°C to 40°C only.	As per Tender Document
684	KVM Console	163	18. LCD console tray should be global certified by most of the agencies like UL, CE, BSMI, cUL, IC, UKCA, NOM, FCC Class A	Kindly request to revise the clause as " LCD console tray should be global certified by most of the agencies like UL / CE / BSMI / cUL / IC / UKCA / NOM / FCC / RoHS" for more OEM participation. Certificate clause will not allow more OEM to participate.	Kindly refer Revised Technical specification
685	Non Smart Racl	162	21.1 Each rack should have 2 PDUs The 2 PDUs in each rack should have different chassis color for identification of UPS source. Electrical rating – Input – 230V, 32A, 1 Phase, 3-meter-long input cable with Splash proof IEC60309 input plug. For all 3Ph PDU it must have the color-coded alternating outlets based on the circuit color to identify the phase and help phase balancing when used as a three phase PDU. High temperature grade, operating temperature up to 60°C.	As per RFP clause no. 21.1 bidder need to provide **1 phase PDU or 3 Phase PDU**. Kindly confirm. If bidder need to provide 1 Phase PDU please revise the clause as " Electrical rating – Input – 230V, 32A, **1 Phase**, 3-meter-long input cable with Splash proof IEC60309 input plug". (or) If bidder need to provide 3 Phase PDU please revise the clause as per 3 Phase PDU requirement.	Kindly refer Revised Technical specification

686	Non Smart Rack	162	Rack should be supplied with single phase 32 Amp iPDU, 42U 600x1200mm (WxD)	Kindly request to remove the size of the rack. so revise the clause as " Rack should be supplied with single phase 32 Amp PDU, 42U 800x1200mm" since we need to install 2 PDUs with 24 sockets each on the sides of the racks, the 800mm width is necessary to fit the PDUs inside. If the width is insisted to be 600mm, multiple PDUs will have to be mounted on the 19" rail itself.	Kindly refer Revised Technical specification
687	Non Smart Rack	162	19. 2 numbers of PDU (as per annexure) Metered PDU with minimum 24 sockets (C13/C19) each, Both Racks & PDU must be from same OEM For seamless integration, configuration and service support. 21.1 Each rack should have 2 PDUs The 2 PDUs in each rack should have different chassis color for identification of UPS source.	Do we required iPDU or normal PDU?. Kindly confirm. Since both the RFP mentioned point 19 & 21.1 are contradicting. Kindly clarify.	Kindly refer Revised Technical specification
688	Intelligent AIM system Monitor	251	The AIM System Monitor shall be able to display live end-to-end tracing information on its screen during patching activities. The screen may be a fixed unit or portable unit fixed in the racks using suitable mount/brackets. Both network rack should have one dedicated (AIM) Intelligent system monitor. Bidder shall configure one Intelligent system monitor two Server racks.	Kindly revise the clause as "The AIM System Monitor shall be able to display live end-to-end tracing information on its screen during patching activities. The screen may be a fixed unit in the racks or portable mobile unit for the technicians. Network rack should have (AIM) Intelligent system controller/analyzer which can manage multiple Network racks/Server racks". Since this clause is limiting the flexibility of the monitor to manage more than 2 racks. One single unit of monitor, if possible, should be allowed to connect to as many server racks as possible and not limited to two server racks. Hence we request related change in the clause.	Kindly refer Revised Technical specification
689	Intelligent AIM system Monitor	251	AIM monitor display system should have the capacity to monitor three RACKs	Kindly revise the clause as "AIM monitor with or without a display system should have the capacity to monitor **multiple** RACKs". Since The capacity to monitor multiple racks is based on the hardware communication between the monitor and intelligent patch panels. So the display on monitor or any handheld device have no configutarion requirement. Hence we request this clause to be changed.	Kindly refer Revised Technical specification
690	Intelligent AIM system Monitor	252	The system should support unlimited port in DC & DR AIM solution software and its hardware should be from same OEM.	Kindly revise the clause as " The system should support **required port count**, as per the design in DC & DR AIM solution software and its hardware should be from same OEM" Since solutions around AIM are based on the actual count of intelligent panel ports installed as per requirement and the design of the site. Also the software is mainly based user accessibily i.e. user licenses. The term "unlimited port" is ambigous as count cannot be defined. We request the license be oriented correctly to actual intelliget panel port count.	Kindly refer Revised Technical specification
691	Intelligent AIM system Monitor	252	4. The AIM System Software component shall support IPv4 and IPv6 communications.	Kindly request to revise the clause as " The AIM System Software component shall support IPv4 (or) IPv6 communications." Since this software is for physical infrastructure management only and have very less IP equipment involved.	As per Tender Document
692	Intelligent AIM system Monitor	252	The AIM System Software component shall provide end user with ability to define manual, automatic, or disabled mode for conducting discovery of networked devices. The automatic device discovery feature shall allow end user to determine a polling schedule, as well as the ability to automatically trigger the discovery process based on SNMP link-up traps from managed network switches.	Kindly request to revise the clause as" The AIM System Software component shall provide end user with ability to discover end devices" for more OEM participation.	As per Tender Document
693	Intelligent AIM system Monitor	253	The AIM System Software component shall have the capability to auto discover IP address, MAC ID, WWN and Host Name information for networked devices and then to auto populate this information into its database.	Kindly request to remove this clause since it is specific to one OEM. This software is for physical infrastructure management only and the discovery of IP address, MAC ID, WWN and Host Name information for networked devices is available with NMS software for the Network Switches. So please remove this point.	As per Tender Document
694	Intelligent AIM system Monitor	253	The AIM System Software component shall have the capability to auto discover networked devices with multiple MAC addresses (i.e., servers with multiple NICs, virtual machines, wireless APs, IP phone/computer pairs, etc.) and then to auto populate that information in its database.	Kindly request to revise the clause as " The AIM System Software component shall have the capability to auto end devices and to auto populate that information in its database." since this software is for physical infrastructure management only and not for the discovery of MAC addresses for networked devices is available with NMS software for the Network Switches	As per Tender Document

695	Intelligent AIM system Monitor	253	The AIM System Software component shall have the capability to auto discover VLAN ID information on managed network switches and then to auto populate that information in its database.	Kindly request to remove this clause since it is specific to one OEM. This software is for physical infrastructure management only and not for discovery of VLAN ID information on managed network switches. So please remove this point.	As per Tender Document
696	Intelligent AIM system Monitor	253	The AIM System Software component shall provide the ability to define type of networked devices based on MAC or IP address range that could also be applied retroactively to already discovered devices. Once defined, each device upon its discovery shall be automatically labelled and represented with an appropriate icon in the database to correspond to the device type definition.	Kindly request to remove this clause since it is specific to one OEM.This software is for physical infrastructure management only and not to define type of networked devices based on MAC or IP address range. So please remove this point.	As per Tender Document
697	Intelligent AIM system Monitor	253	The AIM System Software component shall have the capability to detect configuration changes to managed SAN and LAN switches.	Kindly request to remove this clause since it is specific to one OEM. This software is for physical infrastructure management only and not to dto detect configuration changes to managed SAN and LAN switches. So please remove this point.	As per Tender Document
698	Intelligent cabling	236	11. Safety Standard UL 1666, UL 1685 /ETL	Kindly revise the clause as " Safety Standard UL 1666, UL 1685 /ETL/3P/ BIS or equivalent Standards" Since As UL certification is primarily for fire safety, we request that equivalent fire safety test certificates from other recognized bodies be allowed, as referenced in the RFP (Page No. 242, Clause No. I, Sr. No. 14 for MPO Trunk Cable - UL 1666, UL 1685 // BIS or equivalent Standards). We suggest including 3P/BIS or other equivalent standards as acceptable alternatives.	Kindly refer Revised Technical specification
699	Intelligent cabling	238	14. Safety Standard UL 1666, UL 1685/ETL		Kindly refer Revised Technical specification
700	Intelligent cabling	248	Third party certificate for Genunity ETL four connector channel certificate for long distance and short distance test report.	Kindly request to delete this clause Since the four connector channel certificate is based on the connector testing, not for panel.	Kindly refer Revised Technical specification
701	General	General	General	We understand that Patch cord is required for DC, DR and remote locations. Kindly request to add separate line item in the Bill of Material. And also mention the Patch Cords Type in BoM i.e Specify the type of patch cord required (e.g., Cat6, Cat6a, Fiber Optic, etc.) and kindly specify the number of patch cords required for each location (DC, DR, and remote locations)	To be assessed by Bidder
702	Intelligent cabling	240	12. ANSI/ICEA S-83-596, Telcordia GR-409	Kindly request to revise the clause as "ANSI/ICEA S-83-596, Telcordia GR-409 / IEC 61753-1" for more OEM participation.	ANSI/ICEA S-83-596, Telcordia GR-409 / IEC 61753-1 or equivalent. same is changed at all location in cabling
703	Intelligent cabling	240	13. NEC OFNR-LS (ETL) and c(ETL) or equivalent	Kindly request to revise the clause as " NEC OFNR-LS (ETL) / c(ETL) / UL 60950-1, Information Technology Equipment - Safety Part 1 or equivalent " for more OEM participation	NEC OFNR-LS (ETL) / c(ETL) / UL 60950-1. same is changed at all location in cabling
704	Intelligent cabling	241	5. Patch cord compatibility: Intelligent patch panel shall provide a button and an LED indicator at every panel port/single button on panels to enable easy tracing and identification of patch connections in the telecom room.	Kindly request to revise the clause the clause as " Intelligent patch panel shall provide an LED indicator at every panel port on panels to enable easy tracing and identification of patch connections in the telecom room" for more OEM participation.	As per Tender Document
705	Intelligent cabling	242	6. Jacket color: Aqua Color	Kindly request to revise the clause as " 6. Jacket color: Aqua Color / Heather Violet color". For more OEM participation.	Jacket color: Aqua Color / As per OEM. Further under Intelligent cabling, Colors made as per OEM at all places
706	Intelligent cabling	243	Standards: ANSI/ICEA S-83-596, Telcordia GR-409,	Kindly request to revise the clause as " ANSI/ICEA S-83-596, Telcordia GR-409/IEC 61754-7; Telcordia GR-1435-CORE" for more OEM participation.	Standards: ANSI/ICEA S-83-596, Telcordia GR-409//IEC 61754-7 or equivalent. Same is changed at all location in Intelligent Cabling
707	Intelligent cabling	246	Color: Aqua color for cable and Beige color for connector	Kindly request to revise the clause as" Color: Aqua color / Heather Violet color for cable and Beige color / Heather Violet color for connector" for more OEM participation.	Made as per OEM

708	Intelligent cabling	246	Cable Qualification Standards: ANSI/ICEA S-83-596, Telcordia GR-409	Kindly request co revise the clause as" Cable Qualification Standards: ANSI/ICEA S-83-596, Telcordia GR-409/IEC 61753-1" for more OEM participation.	Standards: ANSI/ICEA S-83-596, Telcordia GR-409//IEC 61754-7 or equivalent. Same is changed at all location in Intelligent Cabling
709	Intelligent cabling	246	Flame Test Listing: NEC OFNR-LS (ETL) and c(ETL) or equivalent	Kindly request to revise the clause as " NEC OFNR-LS (ETL) / c(ETL) / UL 60950-1, Information Technology Equipment - Safety Part 1 or equivalent " for more OEM participation	Flame Test Listing: NEC OFNR-LS (ETL) /c(ETL)/ UL 60950-1 or equivalent
710	Intelligent cabling	248	Third party certificate for Genunity: ETL four connector channel certificate for long distance and short distance test report.	Kindly request to revise the clause as " ELT / 3P Certificate need to be provided" for more OEM participation.	Third party certificate for Genunity ETL/3P or equivalent four connector channel certificate and test report .
711	y Duty Workst	348	4. RAM: 64GB+, DDR5, 4500MHz	Is 64GB+ talks about the expandibility of RAM?	means higher
712	y Duty Workst	348	4. RAM: 64GB+, DDR5, 4500MHz	Kindly request to revise the clause as " 4. RAM: 64GB+, DDR5, 4500MHz or more" Since the average processing speed of DDR5 type memory in desktops starts from 4000MHz onwards. We request a change of 4000MHz or more on similar lines.	as per tender document
713	y Duty Workst	349	9. Ports: 2 HDMI, 1 VGA, 2 Audio-in / out, 1 USB 2.0, 3 USB 3.0, 1 USB C	Kindly request to revise the clause as "9. Ports: 2 HDMI/2 DP, 1 VGA, 2 Audio-in / out, 1 USB 2.0, 3 USB 3.0, 1 USB C". We request to change 2HDMI to 2HDMI/ 2DP. Since Display ports are primary video ports used in commercial models.	as per tender document
714	e Workstation	350	7. USB Ports: USB 3, USB 2.0, USB Type-C	Kindly request to revise the clause as " 7. USB Ports: 2xUSB 3, USB 2.0" As USB 3 is the current industry update. USB 3 can improve the data transfer speeds	Refer modife Bidder may also give 2X USB 3
715	e Workstation	349	5. Monitor: 14'' inch UHD or above with Capacitive Touch screen	Kindly request to revise the clause as " Monitor: 14'' inch UHD/FHD or above with Capacitive Touch screen	as per tender document
716	EMS	367	The overall solution should be provided in local High Availability mode. There should be seamless automatic successful switchover/handover (in failure cases) between the two instances. The each instance of applications / modules should execute at different physical servers. The servers should be of industry standard and data center compatible. Each instance should be able to manage & monitor complete infrastructure at DC, DR & Remote Locations.	We understand that the proposed solution will include one instance at the DC with HA and one instance at the DR with HA,. Additionally, the DC and DR instances will operate in an active-standby mode, Kindly confirm if our understanding is correct.	Instances at DC shall be able to monitor and manage DC / DR &/or Remote Sites. Instances at DR shall be able to monitor and manage DR / DC &/or Remote Sites. Remote Sites shouldnt go unmonitored . When the DC instances are down / don't have MPLS connectivity at DC ; DR instances should be able to manage & monitor Remote Sites; Data generated/updated during this period at DR should be able to synced up to DC. & Vice Versa is applicable when DR connectivity is down. The clause "Each instance should be able to manage & monitor complete infrastructure at DC, DR & Remote Locations." may be read as "Each instance should be able to manage & monitor complete infrastructure at DC / DR &/or Remote Locations."
717	EMS	368	EMS solution proposed should have capability to fetch / receive alarms from other Network Monitoring tools / Systems monitoring tools / other domain monitoring tools like AIM , PATS supplied as a part of this bid and including equipment from other locations / bid as defined earlier in this document and /or as per scope of work	We understand that the required integration with proposed solution includes AIM and PATS systems. Kindly confirm if this understanding is correct. If additional integrations are required, please provide detailed information about that systems, including functionalities and the quantity for each integration.	For detailed information about the integrations pls refer to the Tech Specs & Scope of work Section w.r.t EMS
718	EMS	372	Should provide option to provide standard compliance checks w.r.t Configuration, OS version, software process/services running state across all target devices, etc.	We understand that the requirement for standard compliance checks related to configuration, OS version, and software processes/services running state is specific to network switches and routers. Kindly confirm if our understanding is correct.	This will be for other IT Infra as well which provide the relevant data over SNMP, which may further be used for comparing for compliance checks .
719	EMS	368	Solution be bundled with Data base /Data store encryption for Documents encryption and decryption using AES 256 bit cipher.	We understand that the clause refers to documents related to knowledge management , which are intended to be stored in the database in an encrypted format using AES 256-bit cipher. Kindly confirm if our understanding is correct.	The clause may be read as "Solution be bundled with Data base Encryption & (optional feature) Documents encryption and decryption using AES 256 bit cipher."
720	EMS	373	Should be scalable to allow the addition/integration of new instances of devices to be added in future	Kindly provide information on the new instances of devices expected to be added or integrated in the future, along with the approximate quantities for each category.	Refer to maximum change clause allowed in the bid, for identifying the percentage of devices allowed to be increased.

721	EMS	378	5. Database Monitoring parameters such as a Database Availability b Database Process and Logs c Locks and Buffers d Tablespace/Database e Sessions/Connections f Database Memory h SQL Statistics i Database Jobs etc.	kindly provide details and quantity regarding the specific databases/application that need to be monitored, including their types and versions. to ensure accurate planning and implementation	sql, postgres , elastic , mongo etc.
722	EMS	366	The proposed EMS solution and all modules (e.g. Configuration Management, network monitoring, server monitoring, asset management, IT Helpdesk, Change Management etc.) must be from a single OEM to fulfill the sought requirements & functionality. Bidder holds the responsibility to ensure of testing the functionality of these components/modules before proposing a solution in the bid.	Since there is an IPAM requirement also which is clubbed with the EMS Specifications in the RFP, Requesting to remove IPAM from the EMS Specifications and add as an separate section in the RFP. Justification : IPAM solution is different and has no relevance to EMS solution, also EMS and IPAM vendors are different in the market	The clause may be read as : The proposed EMS solution and all modules (e.g. Configuration Management, network monitoring, server monitoring, asset management, IT Helpdesk, Change Management etc.) must be from a single OEM to fulfill the sought requirements & functionality. **The final EMS solution with IPAM & Switch Port Management may be an integration of OEMs to fulfill the sought requirements. In case the IPAM solution is from other OEM, the EMS OEM holds the responsibility along with bidder to accomplish the end to end integrated requirements of IPAM in EMS.** Bidder holds the responsibility to ensure testing of complete functionality of these components / modules before proposing a solution in the bid.
723	EMS	386	The solution must be agentless can be an pre-integrated module of EMS or it could be a separate module . It may be noted that the functionality and specifications sought via IPAM and Switch Port Management Module may be fulfilled as an integrated module of EMS.In either cases , it must allow the secured access via the browsers using SSL certificates(128 bit &/or 256 bit encryption)	Since there is an IPAM requirement also which is clubbed with the EMS Specifications in the RFP, Requesting to remove IPAM from the EMS Specifications and add as an separate section in the RFP. Justification : IPAM solution is different and has no relevance to EMS solution, also EMS and IPAM vendors are different in the market	May refer to respective revised clause
724	EMS	367	14. a. Also, the sizing of the computing in the proposed hardware should be sufficient enough to cater to futuristic projection of IT/Non-IT equipment mentioned in this bid.	For designing the compute requirements for EMS solution keeping futuristic projection in consideration, requesting you to kindly confirm the futuristic projection as 25% of manage devices sought in BoM from day 1, over the teneure of project?	Yes , Bidders must keep other clauses in context, while deciding the compute requirements.such as 14.(a),15(b), 16 (c)
725	EMS	389	286. OEM of EMS Solution should be SOC2, CMMI Level 3, ISO 27001&ISO 27034 certified	"SOC2 certification is not typically a standard requirement for EMS solutions, as it is more relevant for service organizations handling sensitive data. To ensure the certification aligns with the qualifications needed for EMS applications, we, request to ammend this clause as below: "OEM of EMS Solution should be SOC2/CMMI Level 3, ISO 27001&ISO 27034 certified."	May refer to respective revised clause
726	General	General	General	Requesting to provide the following volumetric for Infrastructure volumetric count? Please confirm the infrastructure volumetric count: 1. No. of network devices to be monitored (SNMP/ICMP)? 2. Number of IP based Cameras? 3. Number of IP Phones? 4. Total nos. of DB OS instances to be monitored? 5. No. of Application OS Instance means an OS instance (physical or virtual machine) that runs an application component to be monitored? 6. Total nos. of Helpdesk (HD, Change, KM, SLM etc.) agents logging into the helpdesk system? 7.Helpdesk Analyst Type - Concurrent or Named? 8. Total no. of Client OS instances(desktops/laptops) for asset management & tracking? 9. Total node counts for Integration with EMS solution?	It is bidder's responsibility that sizing will be done as per BOQ/as per project requirement
727	General	93	SI needs to coordinate with Contractor of existing infra to migrate & integrate 80 remote sites from existing to new DC&DR i.e. to migrate their IPSec tunnels to new DC &DR. Configuring/Integrating the Management and Monitoring software at new DC and new DR with all remote sites.	1.Please confirm whether are we required to integrate the existing EMS/NMS with the new EMS/NMS or migrate the existing EMS/NMS to new EMS/NMS 2. Kindly provide the make and model details of the exisiting EMS /NMS 3. Also Confirm whether the existing EMS/NMS supports API Level integration or Device Level Integration	1. Integration of existing EMS may be done with new EMS 2. Asset list is attached in Annexure 3. Yes

728	PAM	267	PAM user licenses	Please provide number of User Licenses required.	3000 target systems scalable to 10k without any change in hardware. 200 concurrent sessions
729	Storage Server	3	Total 2TB or higher RAM, DDR5 5000+ MHz ECC REG DIMM	For such a huge memory capacity it is recommended to adopt a monolithic architecture for DRAM in datacentre, as it offers **lower power consumption**, enhanced performance and simpler design that **minimizes signal integrity issues**. This will not only optimise the TCO but also the department can leverage more robust architecture. Request you to kindly consider the same.	As per Tender Document
730	Storage Server	3	Total 2TB or higher RAM, DDR5 5000+ MHz ECC REG DIMM	The specifications provided only outline the total DRAM requirement. To ensure consistency across the proposal, we kindly request that you include the capacity details for each individual RAM module to be considered in the proposal.	As per Tender Document
731	Storage Server	3	Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS SSD/M.2 NVME SSD Each SSD spec: 960GB+ Capacity, Write Intensive, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size	The RFP specifies the use of SAS SSDs, which are increasingly becoming obsolete as market adoption shifts towards newer technologies. While NVMe is the Next-gen SSD solution, SAS SSD are based on older technology and their market share is steadily declining. For optimal server performance; faster boot times, OS loading - adopting NVMe not only aligns with current technological trends but also ensures long term scalability, better throughput and overall performance. This will enable the Upcoming datacentre to be more future ready and efficient solution not only for the current applications but also for the future applications. So Request you to kindly restrict the RFP to NVMe SSDs instead of both SAS and NVMe.	Kindly refer Revised Technical specification
732	Storage Server	3	Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS SSD/M.2 NVME SSD Each SSD spec: 960GB+ Capacity, **Write Intensive**, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have **150K+/100K+** Random Read/Write IOPS at 4K block size	Since these drives are intended for boot purpose, they need to handle both read and write intensive operations efficiently. To ensure optimal performance and reliability, we recommend increasing the random read IOPS to be **at least 1000K and Random writes IOPS to be at least 250K and industry standard 3 DWPD**. This enhancement will significantly improve the responsiveness and overall throughput of boot operations, enabling faster system startup time and more reliable performance under heavy workloads. This in turn will not only i**mprove the performance but also in tern reduce the TCO.**	Kindly refer Revised Technical specification
733	Storage Server	4	Minimum Storage of 1440 TB With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	Recommend using 30TB TLC NVMe SSDs instead of high-capacity HDDs reduces server footprint and power consumptions, optimising TCO while enchaining data security and longevity. Request you to kindly consider the architecture based on SSDs rather than HDDs.	As per Tender Document

734	Storage Server	4	Minimum Storage of 1440 TB With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	QD (Queue Depth) for Random read/ write IOPS is recommended to be calculated at industry standard QD256.	As per Tender Document
735	Storage Server	4	Minimum Storage of 1440 TB With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	Request you to kindly modify the following as per current SSD standards in the industry: Random R/W IOPS (at 4KB, **QD256**): 1000+/400+ Sequential R/W speed for 64 KB blocks: 7000+/5900+, 120+ MB/s	As per Tender Document
736	Storage Server	4	Minimum Storage of 1440 TB With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s Note: 1. Single DAS expansion can be used. However, the effective I/O throughput of all the disks combined should not be impacted due to any DAS expansion connector limitations. 2. DAS and Server should be compatible and support of DAS to be provided by Server OEM only. Server OEM shall give undertaking for the support of DAS on their letterhead.	DAS based architectures with high-capacity HDDs result in slow performances and are not suitable for high performance environments, potentially increasing TCO and adding a point of failure in the architecture. For the industry standard recommendations request you to kindly refer to the following: Uptime Institute's Tier Standards Storage Networking Industry Association (SNIA) best practices And it would be recommended to use server-storage architecture without DAS expansions.	As per Tender Document
737	Storage Server	5	Dedicated Hardware Raid controller= RAID 0,1,5,6,10, 50, 60, SATA/SAS-3 connectivity, 4+ GB cache, battery or flash backed protection for all HDDs. All the HDDs in the server should be configurable under a single virtual drive with RAID 5,6,50,60. Storage management including raid configuration. Required support for SED (Self Encrypting Drive) and ISE (Instant Sanitise Erase) should be available in RAID controller	As per the datacentre optimal recommendation, software based RAID should be preferred for NVMe drives over SATA/SAS controllers, as it optimises TCO and boots performances.	As per Tender Document
738	Storage Server	5	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe Sequential read 6,200 MB/s, Sequential write 2,600 MB/s (Sequential performance 128KB block size with queue depth 32) - Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS (Random Performance 4K block size with queue depth 256) **Latency, read/write 120/20 µs (4KB transfer size with queue depth 1)** Endurance 3 DWPD with additional 2 free slots for populating additional cache drives.	Proprietary specs for latency, this is not industry standard. Request you to kindly remove these of specify industry standard latency specifications	Kindly refer Revised Technical specification

739	Storage Server	5	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe **Sequential read 6,200 MB/s, Sequential write 2,600 MB/s** (Sequential performance **128KB block size with queue depth 32**) - **Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS** (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1) Endurance 3 DWPD with additional 2 free slots for populating additional cache drives.	Queue Depth 32 is not industry standard and all the potential players across the industry develop products based on industry standard of QD 128. Request you to kindly change the same as below: Sequential read 6,800 MB/s, Sequential write 5,300 MB/s (Sequential performance 128KB block size with queue depth 128) Random read (4K) Up to 1,100K IOPS, Random write (4K) Up to 390K IOPS	Kindly refer Revised Technical specification
740	Storage Server	5	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe Sequential read **6,200 MB/s, Sequential write 2,600 MB/s** (Sequential performance 128KB block size with queue depth 32) - Random read **(4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS** (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1) Endurance 3 DWPD with additional 2 free slots for populating additional cache drives.	Cache Drives are critical and should have industry standard optimal parameters for the sequential and random read writes, hence, request you to kindly modify the following to current industry standards: Sequential read 6,800 MB/s, Sequential write 5,300 MB/s Random read (4K) Up to 1,100K IOPS, Random write (4K) Up to 390K IOPS	Kindly refer Revised Technical specification
741	Storage Server	5	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe Sequential read 6,200 MB/s, Sequential write 2,600 MB/s (Sequential performance 128KB block size with queue depth 32) - Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1) Endurance 3 DWPD with additional 2 free slots for populating additional cache drives.	By using NVMe drives instead of HDDs for storage, the need of separate cache drives will be eliminated, as NVMe's exceptional performance already delivers faster data access and will significantly increase the TCO.	Kindly refer Revised Technical specification
742	Application Server	6	Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS/M.2 SSD Each SSD spec: 960GB+ Capacity , Write Intensive, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block s size	The RFP specifies the use of SAS SSDs, which are increasingly becoming obsolete as market adoption shifts towards newer technologies. While NVMe is the Next-gen SSD solution, SAS SSD are based on older technology and their market share is steadily declining. For optimal server performance; faster boot times, OS loading - adopting NVMe not only aligns with current technological trends but also ensures long term scalability, better throughput and overall performance. This will enable the Upcoming datacentre to be more future ready and efficient solution not only for the current applications but also for the future applications. So Request you to kindly restrict the RFP to NVMe SSDs instead of both SAS and NVMe.	Kindly refer Revised Technical specification
743	Application Server	6	Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS/M.2 SSD Each SSD spec: 960GB+ Capacity , Write Intensive, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block s size	Since these drives are intended for boot purpose, they need to handle both read and write intensive operations efficiently. To ensure optimal performance and reliability, we recommend increasing the random read IOPS to be **at least 1000K and Random writes IOPS to be at least 250K and industry standard 3 DWPD**. This enhancement will significantly improve the responsiveness and overall throughput of boot operations, enabling faster system startup time and more reliable performance under heavy workloads. This in turn will not only i**mprove the performance but also in tern reduce the TCO.**	Kindly refer Revised Technical specification

744	Application Server	6	Storage Each Server With Minimum Storage of 200 TB,With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency : between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	Recommend using 30TB TLC NVMe SSDs instead of high-capacity HDDs reduces server footprint and power consumptions, optimising TCO while enchaining data security and longevity. Request you to kindly consider the architecture based on SSDs rather than HDDs.	As per Tender Document
745	Application Server	6	Storage Each Server With Minimum Storage of 200 TB,With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency : between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	QD for Random read/ write IOPS is recommended to be calculated at industry standard QD256. Request you to incorporate the same.	As per Tender Document
746	Application Server	6	Storage Each Server With Minimum Storage of 200 TB,With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency : between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	Request you to kindly modify the following as per current SSD standards in the industry and sequential parameters are missing for the drives to be of optimal level: Random R/W IOPS (at 4KB, **QD256**): **1000+/400+** Sequential R/W speed for 64 KB blocks: 7000+/5900+, 120+ MB/s	As per Tender Document
747	Application Server	6	Dedicated Hardware Raid controller= RAID 0,1,5,6,10, 50, 60, SATA/SAS-3 connectivity, 4+ GB cache, battery or flash backed protection for all HDDs. All the HDDs in the server should be configurable under a single virtual drive with RAID 5,6,50,60. Storage management including raid configuration. Required support for SED (Self Encrypting Drive) and ISE (Instant Sanitise Erase) should be available in RAID controller	As per the datacentre optimal recommendation, software based RAID should be preferred for NVMe drives over SATA/SAS controllers, as it optimises TCO and boots performances.	As per Tender Document
748	Application Server	7	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe Sequential read 6,200 MB/s, Sequential write 2,600 MB/s (Sequential performance 128KB block size with queue depth 32) - Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS (Random Performance 4K block size with queue depth 256) **Latency, read/write 120/20 µs (4KB transfer size with queue depth 1)**	Proprietary specs for latency, this is not industry standard. Request you to kindly remove these of specify industry standard latency specifications	Kindly refer Revised Technical specification

749	Application Server	7	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe **Sequential read 6,200 MB/s, Sequential write 2,600 MB/s** (Sequential performance **128KB block size with queue depth 32**) - **Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS** (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1)	Queue Depth 32 is not industry standard and all the potential players across the industry develop products based on industry standard of QD 128. Request you to kindly change the same as below: Sequential read 6,800 MB/s, Sequential write 5,300 MB/s (Sequential performance 128KB block size with queue depth 128) Random read (4K) Up to 1,100K IOPS, Random write (4K) Up to 390K IOPS	Kindly refer Revised Technical specification
750	Application Server	7	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe Sequential read **6,200 MB/s, Sequential write 2,600 MB/s** (Sequential performance 128KB block size with queue depth 32) - Random read **(4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS** (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1)	Cache Drives are critical and should have industry standard optimal parameters for the sequential and random read writes, hence, request you to kindly modify the following to current industry standards: Sequential read 6,800 MB/s, Sequential write 5,300 MB/s Random read (4K) Up to 1,100K IOPS, Random write (4K) Up to 390K IOPS	Kindly refer Revised Technical specification
751	Application Server	7	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe Sequential read 6,200 MB/s, Sequential write 2,600 MB/s (Sequential performance 128KB block size with queue depth 32) - Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1)	By using NVMe drives instead of HDDs for storage, the need of separate cache drives will be eliminated, as NVMe's exceptional performance already delivers faster data access and will significantly increase the TCO.	Kindly refer Revised Technical specification
752	Application Server	7	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe Sequential read 6,200 MB/s, Sequential write 2,600 MB/s (Sequential performance 128KB block size with queue depth 32) - Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1)	Endurance parameter for the cache drive is missing, DWPD 1 or 3 should be defined for parity in the proposal	Kindly refer Revised Technical specification
753	Web Server	9	Boot Storage: 2 no:s x Enterprise SAS SSD/M.2 NVME SSD, Each SSD spec: 400GB+ Capacity, Write Intensive, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size	The RFP specifies the use of SAS SSDs, which are increasingly becoming obsolete as market adoption shifts towards newer technologies. While NVMe is the Next-gen SSD solution, SAS SSD are based on older technology and their market share is steadily declining. For optimal server performance; faster boot times, OS loading - adopting NVMe not only aligns with current technological trends but also ensures long term scalability, better throughput and overall performance. This will enable the Upcoming datacentre to be more future ready and efficient solution not only for the current applications but also for the future applications. So Request you to kindly restrict the RFP to NVMe SSDs instead of both SAS and NVMe.	Kindly refer Revised Technical specification

754	Web Server	9	Boot Storage: 2 no:s x Enterprise SAS SSD/M.2 NVME SSD, Each SSD spec: 400GB+ Capacity, Write Intensive, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size	Since these drives are intended for boot purpose, they need to handle both read and write intensive operations efficiently. To ensure optimal performance and reliability, we recommend increasing the random read IOPS to be **at least 1000K and Random writes IOPS to be at least 250K and industry standard 3 DWPD**. This enhancement will significantly improve the responsiveness and overall throughput of boot operations, enabling faster system startup time and more reliable performance under heavy workloads. This in turn will not only i**mprove the performance but also in tern reduce the TCO.**	Kindly refer Revised Technical specification
755	Web Server	9	Storage 2 nos x 18+ TB Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours) SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	Recommend using 30TB TLC NVMe SSDs instead of high-capacity HDDs reduces server footprint and power consumptions, optimising TCO while enchaining data security and longevity. Request you to kindly consider the architecture based on SSDs rather than HDDs.	As per Tender Document
756	Web Server	9	Storage Each Server With Minimum Storage of 200 TB,With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency : between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	QD for Random read/ write IOPS is recommended to be calculated at industry standard QD256. Request you to incorporate the same.	As per Tender Document
757	Web Server	9	Storage Each Server With Minimum Storage of 200 TB,With Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Sanitise Erase) Avg latency : between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s	Request you to kindly modify the following as per current SSD standards in the industry and sequential parameters are missing for the drives to be of optimal level: Random R/W IOPS (at 4KB, **QD256**): **1000+/400+** Sequential R/W speed for 64 KB blocks: 7000+/5900+, 120+ MB/s	As per Tender Document
758	Web Server	9	Dedicated Hardware Raid controller= RAID 0,1,5,6,10, 50, 60, SATA/SAS-3 connectivity, 4+ GB cache, battery or flash backed protection for all HDDs. All the HDDs in the server should be configurable under a single virtual drive with RAID 5,6,50,60. Storage management including raid configuration. Required support for SED (Self Encrypting Drive) and ISE (Instant Sanitise Erase) should be available in RAID controller	As per the datacentre optimal recommendation, software based RAID should be preferred for NVMe drives over SATA/SAS controllers, as it optimises TCO and boots performances.	As per Tender Document

759	Load Balancer Server	11	Boot Storage subsystem with HW RAID 1 having 2 no:s x Enterprise SAS SSD/M.2 NVME SSD, Each SSD spec: 400GB+ Capacity , Write Intensive, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size	The RFP specifies the use of SAS SSDs, which are increasingly becoming obsolete as market adoption shifts towards newer technologies. While NVMe is the Next-gen SSD solution, SAS SSD are based on older technology and their market share is steadily declining. For optimal server performance; faster boot times, OS loading - adopting NVMe not only aligns with current technological trends but also ensures long term scalability, better throughput and overall performance. This will enable the Upcoming datacentre to be more future ready and efficient solution not only for the current applications but also for the future applications. So Request you to kindly restrict the RFP to NVMe SSDs instead of both SAS and NVMe.	Kindly refer Revised Technical specification
760	Load Balancer Server	11	Boot Storage subsystem with HW RAID 1 having 2 no:s x Enterprise SAS SSD/M.2 NVME SSD, Each SSD spec: 400GB+ Capacity , Write Intensive, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size	Since these drives are intended for boot purpose, they need to handle both read and write intensive operations efficiently. To ensure optimal performance and reliability, we recommend increasing the random read IOPS to be **at least 1000K and Random writes IOPS to be at least 250K and industry standard 3 DWPD**. This enhancement will significantly improve the responsiveness and overall throughput of boot operations, enabling faster system startup time and more reliable performance under heavy workloads. This in turn will not only i**mprove the performance but also in tern reduce the TCO.**	Kindly refer Revised Technical specification
761	Load Balancer Server	12	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe Sequential read 6,200 MB/s, Sequential write 2,600 MB/s (Sequential performance 128KB block size with queue depth 32) - Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS (Random Performance 4K block size with queue depth 256) **Latency, read/write 120/20 µs (4KB transfer size with queue depth 1)**	Proprietary specs for latency, this is not industry standard. Request you to kindly remove these of specify industry standard latency specifications	Kindly refer Revised Technical specification
762	Load Balancer Server	12	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe **Sequential read 6,200 MB/s, Sequential write 2,600 MB/s** (Sequential performance **128KB block size with queue depth 32**) - **Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS** (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1)	Queue Depth 32 is not industry standard and all the potential players across the industry develop products based on industry standard of QD 128. Request you to kindly change the same as below: Sequential read 6,800 MB/s, Sequential write 5,300 MB/s (Sequential performance 128KB block size with queue depth 128) Random read (4K) Up to 1,100K IOPS, Random write (4K) Up to 390K IOPS	Kindly refer Revised Technical specification
763	Load Balancer Server	12	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe Sequential read **6,200 MB/s, Sequential write 2,600 MB/s** (Sequential performance 128KB block size with queue depth 32) - Random read **(4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS** (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1)	Cache Drives are critical and should have industry standard optimal parameters for the sequential and random read writes, hence, request you to kindly modify the following to current industry standards: Sequential read 6,800 MB/s, Sequential write 5,300 MB/s Random read (4K) Up to 1,100K IOPS, Random write (4K) Up to 390K IOPS	Kindly refer Revised Technical specification

764	Load Balancer Server	12	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe Sequential read 6,200 MB/s, Sequential write 2,600 MB/s (Sequential performance 128KB block size with queue depth 32) - Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1)	By using NVMe drives instead of HDDs for storage, the need of separate cache drives will be eliminated, as NVMe's exceptional performance already delivers faster data access and will significantly increase the TCO.	Kindly refer Revised Technical specification
765	Load Balancer Server	12	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe Sequential read 6,200 MB/s, Sequential write 2,600 MB/s (Sequential performance 128KB block size with queue depth 32) - Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1)	Endurance parameter for the cache drive is missing, DWPD 1 or 3 should be defined for parity in the proposal	Kindly refer Revised Technical specification
766	Utility Server	13	2 no:s x Enterprise SAS/M.2 SSD, Each SSD spec: 960GB or more Capacity , Write Intensive, Read (1 GB/s or more) Write (500 MB/s or more), MTBF = 2 million hours or more, 2000 TBW or more, 2 DWPD or more	The RFP specifies the use of SAS SSDs, which are increasingly becoming obsolete as market adoption shifts towards newer technologies. While NVMe is the Next-gen SSD solution, SAS SSD are based on older technology and their market share is steadily declining. For optimal server performance; faster boot times, OS loading - adopting NVMe not only aligns with current technological trends but also ensures long term scalability, better throughput and overall performance. This will enable the Upcoming datacentre to be more future ready and efficient solution not only for the current applications but also for the future applications. So Request you to kindly restrict the RFP to NVMe SSDs instead of both SAS and NVMe.	Kindly refer Revised Technical specification
767	Utility Server	13	2 no:s x Enterprise SAS/M.2 SSD, Each SSD spec: 960GB or more Capacity , Write Intensive, Read (1 GB/s or more) Write (500 MB/s or more), MTBF = 2 million hours or more, 2000 TBW or more, 2 DWPD or more	Since these drives are intended for boot purpose, they need to handle both read and write intensive operations efficiently. To ensure optimal performance and reliability, we recommend increasing the random read IOPS to be **at least 1000K and Random writes IOPS to be at least 250K and industry standard 3 DWPD**. This enhancement will significantly improve the responsiveness and overall throughput of boot operations, enabling faster system startup time and more reliable performance under heavy workloads. This in turn will not only i**mprove the performance but also in tern reduce the TCO.**	Kindly refer Revised Technical specification
768	Utility Server	13	6 or more no:s x 8 TB or more Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12 Gb/s, 7200 RPM, 256 MB Cache. 3.5°, MTBF = 8 Lakhs hours) System must have atleast 12 x LFF front accessible Hot-Swap Drive Bays with backplane supporting SAS/SATA/NVMe drives	Recommend using NVMe SSDs instead of high-capacity HDDs reduces server footprint and power consumptions, optimising TCO while enchaining data security and longevity. Request you to kindly consider the architecture based on SSDs rather than HDDs.	As per Tender Document

769	Utility Server	13	6 or more no:s x 8 TB or more Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12 Gb/s, 7200 RPM, 256 MB Cache. 3.5", MTBF = 8 Lakhs hours) System must have atleast 12 x LFF front accessible Hot-Swap Drive Bays with backplane supporting SAS/SATA/NVMe drives	QD for Random read/ write IOPS is recommended to be calculated at industry standard QD256. Request you to incorporate the same.	As per Tender Document
770	Utility Server	13	6 or more no:s x 8 TB or more Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12 Gb/s, 7200 RPM, 256 MB Cache. 3.5", MTBF = 8 Lakhs hours) System must have atleast 12 x LFF front accessible Hot-Swap Drive Bays with backplane supporting SAS/SATA/NVMe drives	Request you to kindly add the following SSD standards parameters , Random & sequential parameters are missing for the drives to be of optimal level: Random R/W IOPS (at 4KB, **QD256**): **1000+/400+** Sequential R/W speed for 64 KB blocks: 7000+/5900+, 120+ MB/s	As per Tender Document
771	IPS/IDS	84	IPS must support high availability in Active-active and active-passive mode **with stateful failover and not only limited to transparent mode.**	The contractor requests ERNET India to modify this clause in the interest of larger OEM participation: "IPS must support high availability in Active-active and active-passive mode".	IPS must support high availabilityin Active-active
772	IPS/IDS	85	■ Self-learning/profile-based detection	The contractor requests ERNET India to delete this clause in the interest of larger OEM participation.	Should protect against DOS/DDOS attacks. Should have learning capability to monitor the network traffic and develops a baseline profile. It should have the ability to constantly update this profile to keep an updated view of the network.:- ■ Threshold and heuristic-based detection ■ Host-based connection limiting
773	IPS/IDS	86	IPS must have inbuilt network **behavioural analysis engine** to provide additional context using flows.	The contractor requests ERNET India to modify this clause in the interest of larger OEM participation: IPS must have inbuilt network behavioural analysis/protocol RFC analysis engine to detect anomalies.	Protocol RFC analysis included.
774	PAM	89	36. PAM in HA	We request ERNET India to clarify the Volumetric details like number of users, applications, devices, concurrent sessions etc. to finalise the BOQ and propose accordingly.	3000 target systems scalable to 10k without any change in hardware. 200 concurrent sessions

775	Anti DDOS	108	The traffic Auto learning threshold can be **apply automatically** after auto learning completed.	The contractor requests ERNET India to modify this clause in the interest of larger OEM participation: **The traffic Auto learning threshold should be applied manually post understanding its impact on the production traffic after auto learning completed.**	Kindly refer Revised Technical specification
776	Anti DDOS	108	Must have full Authoritative DNS capability to understand records like A, AAAA, CNAME, DNAME, HINFO, MX, NAPTR, NS, PTR, SOA, SRV, Should be able to do on the fly DNSSec.	The contractor requests ERNET India to delete this clause in the interest of larger OEM participation as these points are not related to Link Load Balancer (LLB)	Kindly refer Revised Technical specification
777	Anti DDOS	108	the product should convert DNS requests to DNSSec on the fly, should support 1) Delegated DNS and 2) Proxy DNS, supports an GUl integrated zone file management tool that simplifies.	The contractor requests ERNET India to delete this clause in the interest of larger OEM participation as these points are not related to Link Load Balancer (LLB)	Kindly refer Revised Technical specification
778	Anti DDOS	108	DNS Zone file management and reduce the risk of misconfiguration	The contractor requests ERNET India to delete this clause in the interest of larger OEM participation as these points are not related to Link Load Balancer (LLB)	Kindly refer Revised Technical specification
779	Anti DDOS	108	It shall provide a secure environment to manage DNS infrastructure while validating and error- checking zone files. It shall be built on the latest version of BIND.	The contractor requests ERNET India to delete this clause in the interest of larger OEM participation as these points are not related to Link Load Balancer (LLB)	Kindly refer Revised Technical specification
780	Anti DDOS	108	Should be able to define amount of memory for use of DNS caching	The contractor requests ERNET India to delete this clause in the interest of larger OEM participation as these points are not related to Link Load Balancer (LLB)	Kindly refer Revised Technical specification
781	Anti DDOS	109	The solution shall be able to support IPv4 & IPv6 routing protocols for traffic mitigation: Static Routing, OSPF Routing, BGPv4 Routing and Policy Based routing.	We request you to remove this point as DDoS are stateless and do not support routing protocols	Kindly refer Revised Technical specification

782	Anti DDOS	110	Solutions Operating System should be tested and certified for EAL 2 / NDPP (Network Device Protection Profile)/NDcPP (Network Device collaborative Protection Profile)/ or above under Common Criteria Program for security related functions	Request you to change the clause as **" Solutions Operating System should be tested and certified for EAL 2 / NDPP (Network Device Protection Profile)/NDcPP (Network Device collaborative Protection Profile)/ or above under Common Criteria Program for security related functions or The OEM should provide 3 Govt/BFSI customer references in India**"	Kindly refer Revised Technical specification
783	Patch Management & Compliance Solution	113	40. Patch Management & Compliance Solution	We request ERNET India to clarify the Volumetric details like number of end devices, OS and users to finalise the BOQ and propose accordingly.	Bidder shall estimate the sizing as per BoQ. However it is around 2000 in numbers.
784	Patch Management & Compliance Solution	116	41. Configuration Audit Tool	We request ERNET India to clarify the Volumetric details like number of assets, users etcare missing in the compliance requirements to finalise the BOQ and propose accordingly.	Licensing required for 2000 nodes. Further it can be setup in 5 no. of instances. Instances can be increased as per requirement.
785	ASM	118	1. Solution Characteristics	Please specify total number of devices, endpoints, servers, virtual machines, and IoT devices in the environment. This number will provide the capacity requirements for monitoring and managing these nodes effectively in designing of the solution	This responsibility lies with the bidder to plan sizing of the ASM as per BOQ of this tender
786	ASM	118	2. Deployment Options and Characteristics	Please provide physical and logical network topology, including VLANs, subnets, and physical/virtual segments. This will help in determining the number of segments directly influences the number of switches or connections required for solution integration.	This responsibility lies with the bidder to plan sizing of the ASM as per BOQ of this tender

787	ASM	118	2. Deployment Options and Characteristics	Please confirm whether all the components required for the solutions are required in HA along with DR or not.	Yes, in HA at DC and DR
788	ASM	119	2. Deployment Options and Characteristics	Please specify the total number of wireless sensors needed for adequate coverage of the Surface area for scanning wireless network visibility.	This responsibility lies with the bidder to plan sizing of the ASM as per BOQ of this tender
789	Enterprise Data Log Analytics	137	Proposed solution must include data collection from 250 number of endpoints while ingesting Logs and Endpoint EDR telemetry which should be retained for 180 days for online querying. The minimum estimated data volume must be approximately 900 GB raw data ingestion per day. Any additional data must be processed without any drop or filtering.	Volumetrics are not generic as most of the OEMs measure the log management solution in terms of EPS. So kindly share the equivalent EPS also.	As per tender document
790	Active Directory	150	15 High Availability Yes	Contractor assumes that the high availability is required between DC and DR and standalone implementation to be carried out at individual sites. Kindly confirm if the understanding is correct.	As per Tender Document

791	NAC (included AAA)	151	1).The solution must provide Authentication, Authorization and Accounting (AAA) services using **TACACS**, Profiling, Posturing, Guest Management from a single platform	The contractor requests ERNET India to modify this clause in the interest of larger OEM participation: The solution must provide Authentication, Authorization and Accounting (AAA) services using **TACACS+**, Profiling, Posturing, Guest Management from a single platform **Justification for change:** **TACACS is a Cisco proprietary protocol. To ensure broader OEM participation, we kindly request the authority to mandate the use of TACACS+, which is an industry-standard protocol."**	Kindly refer Revised Technical specification
792	NAC (included AAA)	151	9)The solution must support agent-based deployment and provide deep compliance check for Meeting regulatory compliance requirements such as**GDPR, HIPAA, PCI DSS, SOX, or GLBA** revolve around knowing “who, what, when and where” for devices and users on your network and controlling access to the data your company needs to keep secure.	The contractor requests ERNET India to modify this clause in the interest of larger OEM participation: The solution must support agent-based deployment revolve around knowing “who, what, when and where” for devices and users on your network and controlling access to the data your company needs to keep secure. **Justification for Change: Compliance checking is not a standard feature of NAC solutions. In this RFP, specific tools have been mentioned for compliance checking, making this clause OEM-specific. To ensure broader OEM participation, we kindly request the removal of the compliance check requirement**	Kindly refer Revised Technical specification
793	ASM	169	42. Attack Surface Management	We request ERNET India to clarify the Volumetric details like number of assets, number of IPs, number of web applications etc to finalise the BOQ and propose accordingly.	This responsibility lies with the bidder to plan sizing of the ASM as per BOQ of this tender
794	Console Management Server	154	1) Dual-core ARM Cortex-A9 MP Core with Core Sight	ARM Processor has EOL limitations because of Flash Memory , whereas Intel x86 allows ZPE Systems Hardware run latest Gen3 Operating systems because of its cpu core. and compute so request to amend the clause as follows: 1) Dual-core ARM Cortex-A9 MP **OR Intel x86_64 multi-core**	Dual-core ARM Cortex-A9 MP OR Intel x86_64 multi-core
795	Non Smart Rack with Redundant PDU	161	Rear 19" mounting angles supplied as split pairs to allow easy adjustments for equipment of different depths.	Please accept to delete this clause for broader level of participation.	As per Tender Document

796	Non Smart Rack with Redundant PDU	161	Side panels with Slam latches and Indents for improved strength and aesthetics	Please accept to revise this clause as "Side Panel shall be lockable and horizontally split for ease of operation and aesthetics".	As per Tender Document
797	Non Smart Rack with Redundant PDU	161	Component Shelf 720mm Depth - 2 Nos	Please accept to revise this clause as "Component Shelf shall be with depth adjustable of minimum 620mm deep"	As per Tender Document
798	Non Smart Rack with Redundant PDU	162	Each rack should have 2 PDUs The 2 PDUs in each rack should have different chassis color for identification of UPS source. Electrical rating – Input – 230V, 32A, 1 Phase, 3-meter-long input cable with Splash proof IEC60309 input plug. For all 3Ph PDU it must have the color-coded alternating outlets based on the circuit color to identify the phase and help phase balancing when used as a three phase PDU. High temperature grade, operating temperature up to 60°C.	Please accept for single black coloured chassis.	Kindly refer Revised Technical specification
799	KVM Console	163	Proposed 18.5" or higher LCD console tray and 16 port IP KVM switch should be built in design and should occupy 1U space together in 19" standard rack. KVM Console should have provision to integrate with existing/deployed centralized monitoring software to monitor all KVMs.	Please accept for separate unit as well for both KVM & LCD. As the KVM & LCD be fixed in a way that both of them will occupy 1 U Space only.	Kindly refer Revised Technical specification
800	KVM Console	163	It should have cable management arm(CMA) and the 16x RJ45 port KVM switch built in at the rear side of the LCD console tray to save the U space in Rack.	Please accept to revise this clause by removing Cable management arm (CMA) from rear.	Kindly refer Revised Technical specification It should have 16x RJ45 port KVM switch built in at the rear side of the LCD console tray to save the U space in Rack.
801	KVM Console	163	Both LCD console tray and the built-in KVM switch should have single/ separate power supply.	Please accept for separate power supply as well for both KVM & LCD	understanding is correct ;

802	KVM Console	163	Vendor should supply 16 number of KVM cables with VGA, USB connectors.	Please accept to revise this clause as "Vendor should supply 16 number of Dongles / KVM cables with VGA, USB connectors."	As per Tender Document
803	KVM Console	163	Built-in KVM switch should have 16 RJ45 port to connect KVM cable/dongle with CAT cable to extension at least up to 30Mt	Please accept to revise this clause as "KVM switch should have 16 RJ45 port to connect KVM cable/dongle with CAT cable to extension at least up to 30Mt"	As per Tender Document
804	KVM Console	163	Built it KVM switch should have encryption 128-bit AES for keyboard, mouse and video signals and virtual media sessions, internal and LDAP external authentication.	Please accept to revise this clause as "KVM switch should have encryption for keyboard, mouse and video signals and virtual media sessions, internal and LDAP external authentication."	As per Tender Document
805	KVM Console	163	Built-in KVM switch should be cascaded with another KVM switch with max 30Mt CAT cable.	Please accept to revise this clause as "KVM switch should be cascaded with another KVM switch with max 30Mt CAT cable."	As per Tender Document
806	KVM Console	163	Built-in KVM switch should have min. two VGA local console ports.	Please accept to revise this clause as "KVM switch should have min. one VGA local console ports."	As per Tender Document
807	KVM Console	163	LCD KVM console should support min. resolutions up to 1366 x 768 @ 60Hz; & KVM switch to support Local VGA up to 1920 x 1080 & Remote support up to 1600 x 1200	Please accept to revise this clause as "Minimum LCD Resolution as 1280 x 1024 & KVM Resolution as 1600 x 1200.	As per Tender Document
808	KVM Console	163	Operating temperature and Humidity of LCD console tray should be 0°C to 50°C and 10% to 80%	Please accept to revise this clause as "Operating temperature and Humidity of LCD console tray should be 0°C to minimum 40°C and 10% to 80%	As per Tender Document

809	KVM Console	163	LCD console tray should be global certified by most of the agencies like UL, CE, BSMI, cUL, IC, UKCA, NOM, FCC Class A	Please accept to revise this clause as "LCD console tray should be global certified by most of the agencies like C-Tick, CE, Industry Canada, KCC, NOM, UL listed, VCCI class A, VDE, TAA compliance"	Kindly refer Revised Technical specification
810	Non Smart Rack	340	52 Non Smart Rack with Redundant PDU 20 Supply and installation/laying of all the required electrical cabling to the racks shall be carried out by the bidder as per standards. All accessories for successful installation of rack should be supplied by Bidder.	Please provide the length of the power source from the Rack	As per Tender Document
811	Degaussor	347, 348	58 Degausser 1. Media Handling: Standard PC, Laptop and Server 3.5", 2.5" & 1.8" Hard Drives. 5.Degaussing Force : 7000 Gauss	The mentioned media handling type will not be achieved with Degaussing force of the 7000 Gauss, It will be achieved with minimum 10000 Gauss so kindly amend the clause as below to qualify other OEMs also: **Degaussing Force : Minimum 10000 Gauss**	May be read as: 5.Degaussing Force : 7000 Gauss or higher
812	General	179	d. Internet and Internal Firewalls at DC should be from different OEMs. e. Internet and Internal Firewalls at DR should be from different OEMs.	Please calrify if same OEM internet firewall can be considered on DC & DR like wise for the internal firewall.We seek clarification regarding the requirement for Internet and Internal Firewalls at the Data Center (DC) and Disaster Recovery (DR) site. Specifically: **1. Can the same OEM be proposed for the Internet Firewall at both the DC and DR sites, provided they meet all technical and functional requirements?** **2. Similarly, can the same OEM be proposed for the Internal Firewall at both the DC and DR sites, provided compliance with all stated specifications?**	Bidder must ensure that internet firewall and internal firewall must be from different OEM's. However, it is up to bidder to have internet firewall of same OEM/different OEM at DC and DR. Similarly, for internal firewall, bidder may have same OEM/different OEM at DC and DR.
813	Application Server	184	Storage: Each Server With Minimum Storage of 200 TB,	Please specify it is TB or TiB, specifically in terms of Storage Capacity	As per Tender Document
814	Application Server	184	Interface (NIC)	NIC specs and boot drive are mentioned, but data disk and HBA specs are not mentoned, Please clarify	As per Tender Document
815	Application Server	185	Power Supply: Redundant, maximum rated power upto 1600 W	It should be max. 2400W, The consumed power requirement will increase as per configuration. Hence requesting the change.	as per Tender Document

816	Application Server	185	Interface (NIC)	NIC specs and boot drive are mentioned, but data disk and HBA specs are not mentoned, Please clarify	As per Tender Document
817	Load Balancer Server	189	Power Supply: Redundant, maximum rated power upto 1600 W	It should be max. 2400W, The consumed power requirement will increase as per configuration. Hence requesting the change.	As per Tender Document
818	Load Balancer Server	189	Interface (NIC)	NIC specs and boot drive are mentioned, but data disk and HBA specs are not mentoned, Please clarify	As per Tender Document
819	Load Balancer Server	189	Boot Storage subsystem	Is there any Global hot spare disk required ? Please clarify	As per Tender Document
820	Load Balancer Server	189	Power supply rated	Please modify it as upto 2400W	As per Tender Document
821	Load Balancer Server	189	Interface (NIC)	NIC specs and boot drive are mentioned, but data disk and HBA specs are not mentoned, Please clarify	As per Tender Document
822	Utility Server	191	Storage	Is there any Global hot spare disk required ? Please clarify	As per Tender Document
823	GPU Server	196	Internal Storage	Is there any Global hot spare disk required ? Please clarify	as per tender document

824	GPU Server	181-197	Storage	Storage capacity requirement is mentioned as part of the specifications for various categories of Server - e.g. Storage Server (Category 01), Application Server (Category 02), etc. Please confirm if the Storage capacities in TB are to be read as TB or TiB, whether they are Raw or Usable capacities (if usable, what RAID level to be considered), hot spare requirements.	As per Tender Document
825	Remote Firewall	179	Remote Firewalls should be from Internal Firewall OEM.	As per RFP for remote firewall in Delhi, let us know about the firewall segment/ placement for the same. Is there a specific OEM? What about VPNs?	As per Tender Document
826	General	179	Internet and Internal Firewalls at DC should be from different OEMs. Internet and Internal Firewalls at DR should be from different OEMs.	where is DC & DR locations? What interfaces and how many are required for internal and internet firewalls? How is the network connectivity/topology structured with respect to DC/DR sites, and remote locations? How many security policies need to be created on the firewalls? Require Current/existing diagram to draw a proposed diagram	DC and DR location is yet to be finalised
827	General	179	f. Internet, Internal and Solution firewall should not be from offered networking OEM in this bid.	Please clarify if Firewalls can be proposed as blade/chassis in server/storage solutions such as Cisco UCS.	As per Tender Document
828	EMS	386	The IPAM Solution must support 15,000 IP Address Management for both IPv4 & IPv6 together. It should be scalable upto 1,50,000 without any hardware change.	Please specify number of L2 and L3 devices which have to be onboarded for IPAM database. Basis that licensing will be calculated	Kindly refer to revised Tech Specs
829	Active Directory	327	SI must provide desired hardware and software to meet solution requirement along with antivirus for 3 years	the New domain controllers being built will they be a New Domain / Forest or will be part of an Existing Domain/ Forest	Yes new domain/forest will be made
830	Active Directory	327	SI must provide desired hardware and software to meet solution requirement along with antivirus for 3 years	are these new users, has the Windows User CAL licenses for these users already procured or need to be included.	SI must provide desired hardware and software to meet solution requirement along with antivirus for **5 years with 200 CAL license**
831	Active Directory	327	User life cycle management.	User management will have to be performed by another tool, Is ERNET looking for an AD user Management tool?	No
832	Active Directory	327	User life cycle management.	User management will have to be performed by another tool, infrastructure is not asked or allocated for AD Management tool, should that be considered as an add-on to AD Servers.	No
833	BoM	277	Inbuilt ticketing system with 5 level workflow approval with ticket level validation, risk and impact assessments as per LOB wise, Service type and user type. This ticketing system to help in creating a work order on an executer, who will then request for the access through the request workflow with this valid ticke	What ticketing system needs to be integrated with the solution?	Clause is self explanatory
834	EMS	277	The solution should be able to integrate with leading SIEM Solutions.	Which OEM SIEM solution needs to be integrated?	May refer to the Tender Document, BoM and Tech Specs & respective SI will be able t

835	BoM	267	The solution should be agentless i.e. does not require to install any agent on target devices	what Endpoint and operating systems are there?	Clause is self explanatory
836	BoM	269	The solution should support changing a password or group of passwords according to a policy (time based or 'on-demand')	Pls provide the total number of users, number of devices, and number of privileged administrators/users for PAM	Kindly refer to revised Tech Specs
837	Load balancer with WAF	324	Must support layer4 and layer 7 load balancing for well-known protocols.	What is the required WAF throughput? How many web applications are there, and what is the estimated HTTP traffic volume? How many policies need to be created on the WAF?"	As per Tender Document
838	NAC (included AAA)	329	The Solution shall use Agent based approach for Desktops, Laptops, etc. and Agentless for other devices	Pls provide the total number of endpoints and network devices. Additionally, pls specify the operating systems utilized by these endpoints.	As per Tender Document
839	Intelligent cabling	54	Intelligent Cabling is required at DC for 100 Racks & at DR for 50 Racks.	Please share the rack layout for both DC (100 Racks) and DR (50 Racks). This will be required for the preparation of the Passive Structured Cabling BoQ.	DC and DR location is yet to be finalised. Further it is anticipated that there will be 8-10 Rack in each Row in DC and DR. In respect of Server and Network rack bifurcation, there will be 90 Server and 10 Network Rack in DC as well as 40 Server and 10 network rack in DR. However If there is any change in predicted layout, bidder shall accomodate the same without any price escalation to ERNET India/ CERT-In.
840	Intelligent cabling	165	2 X 16 LC Duplex connections will be extended to each Server/Storage via fiber shelf to enable intelligent solution.	Please confirm if any connectivity between two adjacent servers racks is required for Network 1	As per Tender Document
841	Intelligent cabling	61	Color: Lime Green color for cable and Gray color for connector	Usually the connector color of an LC connector is Black or Beige. Request you to allow Black color as well. The clause should be ammended to the following: **Color: Lime Green color for cable and Gray/Black color for connector**	As per OEM
842	Intelligent cabling	62	Flame Test Listing: NEC OFNR-LS (ETL) and c(ETL) or equivalent	There have been ammendments in the standards and is no longer OFNR-LS, but it is OFNR-ST1. Request you to change the standard mentioned. The clause should be ammended to the following: **Flame Test Listing: NEC OFNR-ST1 (ETL) and c(ETL) or equivalent**	NEC OFNR-LS (ETL)/NEC OFNR-ST1 (ETL) and c(ETL) or equivalent
843	Intelligent cabling	68	Color: Aqua color for cable and Beige color for connector	Usually the connector color of an LC connector is Black or Beige. Request you to allow Black color as well. The clause should be ammended to the following: **Color: Aqua color for cable and Beige / Black color for connector**	As per OEM
844	Intelligent cabling	73	4) The AIM System Monitor shall be able to display live end-to-end tracing information on its screen during patching activities. The screen may be a fixed unit or portable unit fixed in the racks using suitable mount/brackets. Both network rack should have one dedicated (AIM) Intelligent system monitor. Bidder shall configure one Intelligent system monitor two Server racks. 9) AIM monitor display system should have the capacity to monitor three RACKs	Please clarify whether the AIM system monitor should monitor two (2) server racks or three (3) server racks as clause 4 and 9 specify different quantity.	AIM monitor display system should have the capacity to monitor three RACKs. Further Bidder should provide one Monitor for three server Racks and One Monitor for each Network Rack.
845	Non Smart Rack	340/389	Each rack should have 2 PDUs The 2 PDUs in each rack should have different chassis color for identification of UPS source. Electrical rating – Input – 230V, 32A, 1 Phase, 3-meter-long input cable with Splash proof IEC60309 input plug. For all 3Ph PDU it must have the color-coded alternating outlets based on the circuit color to identify the phase and help phase balancing when used as a three phase PDU. High temperature grade, operating temperature up to 60°C.	Please confirm the no. of 3phase and 1phase iPDU required	Kindly refer Revised Technical specification
846	EMS	339/389	Racks should be with all requisite accessories and parts including 1U/2U air guiding solution to be used in the network racks	Please confirm the no. of Network Racks along with its dimensions	Check the BoM and Specifcation for details.

847	EMS	357/389	PAT Solution's Asset tag Features - Should be able to alert in real time, if an unauthorized movement of asset is made or an asset falls or there is an attempt to remove or forceful removal of tag from asset or has a low battery or in case any physical tampering is made to asset tag pasted on the asset or any physical tampering is made in between physical connectivity between asset tag to its asset tag locator module/strip or any tampering(physical/software level) tampering is made to solution. Specifically in case of wired solution, the asset tag connector should be able to capture accidental / intentional physical damage to the connecting cable (by detecting continuity tracing or other means), thereby clearly differentiating forceful removal of asset tags & cable/cord cutting incidents.	Can we consider forcefull tampering of asset tag & cable cut one and same as part of tampering to asset ?	Clause is self explanatory
848	EMS	358/389	PATS's Asset Tag form factor & mounting - Form factor of asset tags should be tamper proof & small enough to be able to easily & strongly attach to a IT asset but it should also be noticeable to naked eye. Should not be more than 86m x 50mm x10mm with enclosure. Asset Tags / Solution should be operatable within 0 °C to +70 °C & Operating Humidity levels < 95% RH non-condensing . The tags should be tough(applicable for wireless tags), impact resistant and temperature stable	seems like 86m is typo error, please change it to 86mm	Accepted ; 86mm
849	EMS	358/389	PATS's Alarms & Notification from the Asset Solution- Solution should be able to provide real Time alarm & event notification. Should be able to Generate Alert in at least the following conditions: Addition & removal of Asset , movement of Asset from a RACK, Cage area, Store Room, Floor & DC/DR , Falling of an asset or there is an attempt to remove asset or a forceful removal of tag from asset or a physical / software level tampering is done to asset tag / asset tag solution's supplied accessories or if an asset tag has a low battery & needs battery replacement(wherever applicable) . Accordingly to the locations defined (such as RACK, Cage area, Store Room, Floor , DC,DR etc.) bidder may ascertain & accordingly include the number of Communication Gateways / locator modules required) RFID Asset Management solution should support tracking of assets on both front & rear side of the racks.	Will rear mounted devices/assets overlap with front mounted devices at same start RU level ?	Generally, in our case, the Racking,Stacking won't be done with overlapping unless an
850	EMS	361/389	The system should allow to generate the reports containing inventory details as mentioned above and including the other details such as current assigned IP, device type, device name, location, RACK etc. Reports should include the available space, used space per rack.	May we know which format of report is required as output file type.	The report needs to be in PDF format; Otherwise Reports need to be available in pdf format,csv,excel The html format is optional
851	EMS	362/389	The solution must be an integrated solution with IT helpdesk, Change Management & EMS, so as e.g. movement of asset can be authorized change request, whose time taken for a change may be tracked via the Helpdesk manager.	what is the preferred method of integration between PAT EMS, Helpdesk/Service Management & Change Management etc. Is intgeration method RESTAPI OK?, before the actual deployment at site, we preferred/ recommend a pre workshop to be held to decide and freeze the level of integration, this will benefit everyone.	Non Properiatary such as REST API based methodolody of integration between PAT & EMS is required. The modules such as Helpdesk/Service Management & Change Management are integral part of EMS , hence their functionality should work full fledged as sought in this bid, OEM(s)/Bidder may take a call w.r.t their integration, giving preference to non-properitary (such as REST API) interation methodology. The L1 bidder is advised to proactively discuss the workshop schedule & plan the same with ERNET India & CERT-In team.
852	EMS	363/389	The bidder needs to create such processes and perform similar integrations	what is the preferred method of integration between PAT EMS, Helpdesk/Service Management & Change Management etc. Is intgeration method RESTAPI OK?	Non Properiatary such as REST API based methodolody of integration between PAT & EMS is required. The modules such as Helpdesk/Service Management & Change Management are integral part of EMS , hence their functionality should work full fledged as sought in this bid, OEM(s)/Bidder may take a call w.r.t their integration, giving preference to non-properitary (such as REST API) interation methodology. The L1 bidder is advised to proactively discuss the workshop schedule & plan the same with ERNET India & CERT-In team.
853	EMS	363/389	Updating of Patches, Bug Fixes within support period, upgradation of version during the support period is the joint responsibility of the OEM & SI. They must ensure to update the patches or provision the upgrades via the non-internet modes i.e. by following local update/upgrade mechanisms using HDDs/USBs .	Since offline method is suggested for patch management, maybe we request what is the preferred frequency of updates of patches of Operating system & updating patches of PAT application.	Immediate & As soon as its available; Max time will be 30 days.

854	Internal Firewall	255	Layer3-Layer4, NAT, Application Visibility and Control (AVC), Next Generation Intrusion Prevention System (IPS)	As per Best Practices and Defense in Depth approach, Internal firewall will serve as a protective barrier between internal and external networks. It works by examining and filtering data using specific security modules. Malware and Anti-Virus protection is one of the most important tools to protect internal networks from Different Types of Malware. It is requested to please include malware protection and Anti-Virus protection also along with Layer3-Layer4, NAT, Application Visibility and Control (AVC), Next Generation Intrusion Prevention System (IPS) for enhanced protection. **Layer3-Layer4, NAT, Application Visibility and Control (AVC), Next Generation Intrusion Prevention System (IPS), Anti-Virus and Malware Protection from same OEM on premise without any dependency on cloud.**	As per Tender Document
855	Internal Firewall	255	Application Visibility License, IPS License	"As per Best Practices and Defense in Depth approach, Internal firewall will serve as a protective barrier between internal and external networks. It works by examining and filtering data using specific security modules. Malware and Anti-Virus protection is one of the most important tools to protect internal networks from Different Types of Malware. It is requested to please include malware protection also along with Application Visibility License, IPS License and amend the clause as below : **Application Visibility License, IPS License, Anti-Virus and Anti malware protection.**	As per Tender Document
856	Internal Firewall	255	5."Throughput (Real World/Prod Performance) (All Features enabled)(Gbps)"Throughput (Real World/Prod Performance) (All Features enabled)(Gbps) : 270 Gbps. 6.IPsec ThroughputMinimum 240Gbps 7.SSL Inspection Throughput200 Gbps or Higher 8."Concurrent Session/Concurrent Connection"75 Million Layer 4 sessions or 30 Million Layer 7 sessions 9."New session/Connection per second"Minimum 600K Layer 4 sessions or Minimum 300K Layer 7 sessions 10."Type of Interface Supported Multi- select"GECopper, 10GSFP+, QSFP+40G,GESFP, QSFP28 100G 11.Port PopulationThe Firewall should have minimum 12 x 10GSFP+, 12 x 40G /100G QFSP 28. All the ports shall be fully Populated with respective Transceivers.	Please clarify if these performance perameters should be available in single unit of propsed solution or HA/Clustering/stacking of solution is permitted.	Performance parameters should be available in single unit
857	**Generic**	NA	Current AD,DNS & IAM solution	Bidder request to share the currently deployed AD,DNS & IAM solution	Asset detail attached in Annexure
858	**Generic**	NA	Current Backup solution implemented	Bidder request to share the currently deployed Backup Solution	Asset detail attached in Annexure
859	**Generic**	NA	Data Migration	We understand that there is no Scope of any existing Data to be migrated to new environment.	Only link will be migrated from existing environment to new environment
860	**Generic**	NA	Data Migration	If Data migration is in scope, pls. share the details size of data and from which application data will be migrated.	Only link will be migrated from existing environment to new environment
861	**Generic**	96	Backup size	Need further clarification regarding the following aspects: Backup Size: What is the expected size of the backups? Are we estimating the data volume that will need to be backed up on a regular basis? Backup Frequency: How often will the backups be performed? Will they be scheduled daily, weekly, or based on some other frequency, and how will this frequency be determined? Backup Policy: What is the policy regarding backups? This includes details about retention periods, how long backups will be stored, and whether there are any specific procedures for backup testing or restoration.	Backup requirement for individual line item is already defined in specifications

862	Fireproof Vaul	346	Fireproof Vault - UL certificate required	Request to kindly change the clause for a healthy competition.	As per Tender Document
863	Intelligent AIM system Monitor	76	The offered AIM Solution should be provided along with backup solution. All the Hardware required for backup should be provided by the bidder. The hardware should be sufficient enough to support the backup of at least 1 months. The time period of backup should be configurable.	Backup: Please confirm if any third party backup solution (e.g. Commvault/NetBackup/Veeam) need to be factored as part of the solution. Also please confirm the amount of data to be backed up to factor the required backup licenses and Backup target Storage.	As per tender document
864	PAM	97	The proposed solution shall have built-in options for backup or integration with existing backup solutions.	Please share details of the existing backup solution.	As per Tender Document
865	EMS	12	Note 2: Bidder may propose an alternate design / solution in combination full-filling the sought requirements, if required. SI may add any other third party components (such as a backup solution etc.) to achieve this requirement.	Please confirm details of data to be backed up as part of the solution (e.g. VM Disks/File System/DB etc..) Also please confirm the amount of data to be backed up.	The requirement clause is pertaining to EMS Specifications, where High Availability (HA) mode is being discussed. The data to be backed up discussed in the clause is pertaining to EMS application . All the data being created & required by EMS application (such as Configuration files, Alarms Db, Performance Db,) for working in HA mode is the actual data. As the clause discusses the application specific data , Bidder may discuss it with repective OEMs
866	Generic q	NA	Generic query regarding backup requirement	Please Confirm if there is any requirement for a dedicated backup infrastructure to be set up as part of the infrastructure ((e.g. Commvault/NetBackup/Veeam). If so please confirm the details of data types to be backed up (e.g. VMs, File systems, Data bases, Data drives of servers etc..) and the amount of data to be backed up. Request to include backup requirements (Backup license and Backup Storage) in the BOQ.	for the amount of data based on the way its stored by application.
867	EMS	384	CMS should be integrated with overall solution or be in-built as a part of EMS.	Please clarify, Can we propose SaaS based EMS tools and ITSM tools?	May pls refer to specifications, only on-premises model is to be proposed.
868	EMS	384	Supplied solution should have a standard search , advance search mechanism on the fields for enhanced productivity.	Please clarify, What would source of data and Volume of Data?	May pls refer to the EMS Specifications , Scope of Work to understand the source(s) of data ; the volume of data may accordingly be understood.
869	Generic		Generic	The DDOS L-7 throughput is 10 Gbps and extendable to 30 Gbps but the L-7 throuput of the Internet Firewall is 60 Gbps. As per best practices DDOS must be placed at the outermost perimeter layer so that throughput should match with the External NGFW. Please clarify it.	Kindly refer Revised Technical specification
870	Intelligent AIM system Monitor	Tender Page 251, Annexure 1 - Page 73	The AIM System Monitor shall be able to display live end-to-end tracing information on its screen during patching activities. The screen may be a fixed unit or portable unit fixed in the racks using suitable mount/brackets. Both network rack should have one dedicated (AIM) Intelligent system monitor. Bidder shall configure one Intelligent system monitor two Server racks.	The purpose of a portable device is flexibity of using it over multiple racks/locations. Fixing it on the rack cancels the benefit of portability. So it is important to avoid mounting a portable device on a rack and hence we request change in the clause. Also the clause is limiting the flexibility of the monitor to manage more that 2 racks. One single unit of monitor, if possible, should be allowed to connect to as many server racks as possible and not limited to two server racks. Hence we request related change in the clause. **Suggested Clause:** The AIM System Monitor shall be able to display live end-to-end tracing information on its screen during patching activities. The screen may be a fixed unit or portable unit. Bidder shall configure one Intelligent system monitor for two or more Server racks to utilise complete capacity of the monitor hardware.	The AIM System Monitor shall be able to display live end-to-end tracing information on its screen during patching activities. The screen may be a fixed unit or portable unit fixed in the racks using suitable mount/brackets.

871	Intelligent AIM system Monitor	Tender Page 251, Annexure 1 - Page 73	AIM monitor display system should have the capacity to monitor three RACKs	The capacity to monitor 3 or more racks is based on the hardware communication between the monitor and intelligent patch panels. So the display on monitor or any handheld device have no configutarion requirement. Hence we request this clause to be changed. **Suggested Clause:** AIM monitor with ot without a display system should have the capacity to monitor three or more RACKs	Kindly refer Revised Technical specification
872	Intelligent AIM system Monitor	Tender Page 252, Annexure 1 - Page 74	The system should support unlimited port in DC & DR AIM solution software and its hardware should be from same OEM.	The solutions around AIM are based on the actual count of intelligent panel ports installed as per requirement and the design of the site. Also the software is mainly based user accessibily i.e. user licenses. The term "unlimited port" is ambigous as this cannot be defined. We request the license be oriented correctly to actual intelliget panel port count. **Suggested Clause:** The system should support required port count, as per the design in DC & DR AIM solution software and its hardware should be from same OEM.	The system should support port in DC & DR as per boQ. AIM solution software and its hardware should be from same OEM. This line is added in General Note of Cabling: Bidder should provide AIM solution licenses as per BoQ defined in the Tender Document. Also AIM Solution software and its hardware should be from same OEM. Further, price for AIM Solution along with cabling/patch panel/Patch chords/cassettes/AIM Monitor etc. required due to any increase in Racks along with equipment will be derived on a prorated basis.
873	Intelligent cabling	Tender Page 236, Annexure 1 - Page 58	Safety Standard UL 1666, UL 1685 /ETL	As UL certification is primarily for fire safety, we request that equivalent fire safety test certificates from other recognized bodies be allowed, as referenced in the RFP (Page No. 242, Clause No. I, Sr. No. 14 for MPO Trunk Cable - UL 1666, UL 1685 // BIS or equivalent Standards). We suggest including BIS or other equivalent standards as acceptable alternatives. **Suggested Clause:** Safety Standard UL/ BIS or equivalent Standards	Safety Standard UL 1666 ,UL 1685 /ETL/BIS or equivalent Standards
874	Intelligent cabling	Tender Page 238, Annexure 1 - Page 60	Safety Standard UL 1666, UL 1685/ETL	As UL certification is primarily for fire safety, we request that equivalent fire safety test certificates from other recognized bodies be allowed, as referenced in the RFP (Page No. 242, Clause No. I, Sr. No. 14 for MPO Trunk Cable - UL 1666, UL 1685 // BIS or equivalent Standards). We suggest including BIS or other equivalent standards as acceptable alternatives. **Suggested Clause:** Safety Standard UL/ BIS or equivalent Standards	Safety Standard UL 1666 , UL 1685 /ETL/BIS or equivalent Standards
875	Intelligent cabling	Tender Page 248, Annexure 1 - Page 70	Third party certificate for Genunity ETL four connector channel certificate for long distance and short distance test report.	The four connector channel certificate is based on the connector testing and not panel and hence request to consider this clause under connector.	Third party certificate for Genunity ETL/3P four connector channel certificate and test report .
876	Intelligent cabling	54	Intelligent Cabling is required at DC for 100 Racks & at DR for 50 Racks.	Please share the rack layout for both DC (100 Racks) and DR (50 Racks). This will be required for the preparation of the Passive Structured Cabling BoQ.	Kindly refer Revised Technical specification
877	Intelligent cabling	165	2 X 16 LC Duplex connections will be extended to each Server/Storage via fiber shelf to enable intelligent solution.	Please confirm if any connectivity between two adjacent servers racks is required for Network 1	As per tender document
878	Intelligent cabling	58	Flame Test Method: IEC 60332-3/ IEC 60332-1 , IEC 60754-2, IEC 61034-2	The fiber trunk cables and patch cords must strictly comply with IEC 60332-3, as IEC 60332-1 is not the appropriate flame test standard for cable bundles. Since all fiber trunk cables and patch cords will be installed along the same pathway, forming a cable bundle, permitting compliance with IEC 60332-1 would heighten the risk of significant fire spread in case of a fire. Therefore, the clause should be revised as follows: Flame Test Method: IEC 60332-3, IEC 60754-2, IEC 61034-2	As per tender document

879	Intelligent cabling	60	Flame Test Method: IEC 60332-3/ IEC 60332-1 , IEC 60754-2, IEC 61034-2	The fiber trunk cables and patch cords must strictly comply with IEC 60332-3, as IEC 60332-1 is not the appropriate flame test standard for cable bundles. Since all fiber trunk cables and patch cords will be installed along the same pathway, forming a cable bundle, permitting compliance with IEC 60332-1 would heighten the risk of significant fire spread in case of a fire. Therefore, the clause should be revised as follows: Flame Test Method: IEC 60332-3, IEC 60754-2, IEC 61034-2	As per tender document
880	Intelligent cabling	61	Connector type: LC/UPC to LC/UPC, Fiber patch cord 1.7mm / 3.5mm. Riser	In a Data Center environment, it is preferable to use small-diameter patch cords to effectively manage the high volume of patch cords within a rack. Therefore, we request that 1.6 mm diameter patch cords also be allowed. The clause should be revised as follows: Connector type: LC/UPC to LC/UPC, Fiber patch cord 1.6mm / 1.7mm / 3.5mm. Riser	1.6 mm allowed. Correct in tech spec at all places
881	Intelligent cabling	61	Color: Lime Green color for cable and Gray color for connector	Typically, the connector color for an LC connector is Black or Beige. We request that Black connectors also be permitted, or that the connector color be made color-independent. The clause should be revised as follows: Color: Lime Green color for cable and connector color as per OEM	Kindly refer Revised Technical specification
882	Intelligent cabling	61	Additional Clause: Insertion Loss and Return Loss value specifications missing	The insertion loss and return loss are the most critical performance specifications for any fiber cable or patch cord. These parameters are currently missing and must be included in the specifications to guarantee the supply of high-performance patch cords. The following clause should be added to the specifications: Insertion Loss, maximum: 0.15 dB Return Loss, minimum: 35 dB	As per tender document
883	Intelligent cabling	62	Flame Test Listing: NEC OFNR-LS (ETL) and c(ETL) or equivalent	Recent amendments to the standards have updated the classification from OFNR-LS to OFNR-ST1. We request that the standard mentioned be updated accordingly. The clause should be revised as follows: Flame Test Listing: NEC OFNR-ST1 (ETL) and c(ETL) or equivalent	Kindly refer Revised Technical specification
884	Intelligent cabling	62	Additional Clause: Should detect standard MPO and LC patch cords from and OEM	The proposed solution panels (fiber or copper) should be able to detect standard and any type of proprietary patch cords that are inserted into the panel. This is highly critical from a security point of view, as any solution not supporting this feature can expose the network to external security threats. This is because if the panel should not detect a standard patch cord, then the user/network manager will not get an alert that a patch cord has been inserted in a port. The following clause should be included in the specifications: Panel should be able to detect standard and proprietary patch cords with an alert of the event sent to the software. The same should be demonstrated by the OEM / Bidder.	As per tender document
885	Intelligent cabling	65	Flame Test Method: IEC 60332-3/ IEC 60332-1 , IEC 60754-2, IEC 61034-2	The fiber trunk cables and patch cords must strictly comply with IEC 60332-3, as IEC 60332-1 is not the appropriate flame test standard for cable bundles. Since all fiber trunk cables and patch cords will be installed along the same pathway, forming a cable bundle, permitting compliance with IEC 60332-1 would heighten the risk of significant fire spread in case of a fire. Therefore, the clause should be revised as follows: Flame Test Method: IEC 60332-3, IEC 60754-2, IEC 61034-2	As per tender document

886	Intelligent cabling	67	Attenuation: 1.00 dB/km @ 1,300 nm | 2.20 dB/km @ 953 nm 3.00 dB/km @ 850 nm	We recommend that the specification should be removed as it provides no additional benefit. The important parameter that impacts the performance is the insertion loss value, which has been asked in the specification. Also OM4 which is a multimode fiber and governed by international standards specifies only 2 wavelengths, 1300 nm and 850 nm. Hence 953 nm is not a defined wavelength for OM4 multimode fiber. The clause should be deleted as insertion loss has already been asked.	2.20 dB/km @ 953 nm - Deleted
887	Intelligent cabling	67	Insertion Loss, maximum: 0.47 dB	The asked insertion loss value of 0.35 dB is very high for a high quality and high performance module. Insertion loss is the most critical performance parameter in a fiber component. To ensure that high speed applications, today or in the future, should be supported, the insertion loss should not be more than 0.35 dB. The clause should be ammended to the following: Insertion Loss, maximum: 0.35 dB	As per tender document
888	Intelligent cabling	68	Connector type: LC/UPC to LC/UPC, Fiber patch cord 1.7mm / 3.5mm. Riser	It is prefered in a Data Center enviornment to have a small diameter patch cord to manage the large volumn of patch cords inside a rack. Therefore request you to allow 1.6 mm diameter as well. The clause should be ammended to the following: Connector type: LC/UPC to LC/UPC, Fiber patch cord 1.6mm / 1.7mm / 3.5mm. Riser	Kindly refer Revised Technical specification
889	Intelligent cabling	68	Color: Aqua color for cable and Beige color for connector	Typically, the connector color for an LC connector is Black or Beige. We request that Black connectors also be permitted, or that the connector color be made color-independent. The clause should be revised as follows: Color: Lime Green color for cable and connector color as per OEM	Kindly refer Revised Technical specification
890	Intelligent cabling	68	Flame Test Listing: NEC OFNR-LS (ETL) and c(ETL) or equivalent	Recent amendments to the standards have updated the classification from OFNR-LS to OFNR-ST1. We request that the standard mentioned be updated accordingly. The clause should be revised as follows: Flame Test Listing: NEC OFNR-ST1 (ETL) and c(ETL) or equivalent	Kindly refer Revised Technical specification
891	Intelligent cabling	68	Insertion Loss, maximum: 0.3 dB	The asked insertion loss value of 0.30 dB is very high for a high quality and high performance fiber patch cord. Insertion loss is the most critical performance parameter in a fiber component. To ensure that high speed applications, today or in the future, should be supported, the insertion loss should not be more than 0.15 dB for fiber patch cords. The clause should be ammended to the following: Insertion Loss, maximum: 0.15 dB	As per tender document
892	Intelligent cabling	68	Return Loss, minimum: 27 dB	The asked return loss value of 27 dB is very low for a high quality patch cord connector. Return loss along with Insertion loss is one of the most critical performance parameters in a fiber component. To ensure that high speed applicatoins, today or in the future, should be supported, the return loss value should not be lower than 35 dB for fiber patch cords. The clause should be ammended to the following: Return Loss, minimum: 35 dB	As per tender document
893	Intelligent cabling	73	4) The AIM System Monitor shall be able to display live end-to-end tracing information on its screen during patching activities. The screen may be a fixed unit or portable unit fixed in the racks using suitable mount/brackets. Both network rack should have one dedicated (AIM) Intelligent system monitor. Bidder shall configure one Intelligent system monitor two Server racks. 9) AIM monitor display system should have the capacity to monitor three RACKs	Please clarify whether the AIM system monitor should monitor two (2) server racks or three (3) server racks as clause 4 and 9 specify different quantity.	Kindly refer Revised Technical specification

894	Intelligent cabling	74	Additional Clause: Each individual copper and fiber port must have a push / membrane button to trace the circuit from end to end. The circuit trace must also appear on the AIM system monitor display.	This is a critical feature that the AIM system must have. The trace button on the panel allows the user to quickly check the end to end circuit details of the port. Once the button is pressed, the user should be able to see the complete end to end circuit details on the AIM system monitor along with other details such as VLAN information etc. This feature must be part of the standard AIM solution offering without which the user will have to only rely solely on the software (which can be located remotely)	As per tender document
895	Leaf Switch	29	Should support 250K IPv4 LPM Routes, 125K IPv6 LPM Routes, 100K IPv4/v6 Multicast Routes.	Should support 400K IPv4 LPM Routes, 400K IPv6 LPM Routes, 100K IPv4/v6 Multicast Routes Justification: Since at router 1M route scale is asked, hence requesting to amend the clause to accommodate higher number of routes for east-west traffic.	As per Tender Document
896	Border Leaf Switch	30	Switch should support all functions required to operate as a Border Leaf Switch providing DC Gateway, Service Chaining and Data centre Interconnect (DCI) using EVPN type-5 routes. Should support **300K** **IPv4 Routes,150K IPv6 Routes, 64K Multicast Route**	Requesting to increase the route scale to 1M IPv4 Routes,1M IPv6 Routes, 64K Multicast Route. Justification: Since at router 1M route scale is asked, hence requesting to amend the clause to accommodate higher number of routes for east-west traffic.	Kindly refer Revised Technical specification
897	Network Manager	52	Visibility of the these parameters is expected but not limited to - CPU, Memory, interface stats (traffic counter, error, discard), MAC table, ARP table, IPv6 ND table, IPv4 route table, IPv6 route table, **Multicast table,** BGP, capacity parameters / TCAM ,running config, traffic flow (sflow/IPFIX/Netflow), buffer utilization per interface, MLAG Stats, Switch environment stats(FAN, Temperature, Power Supply).	Requesting to remove "Multicast Table" Justification : For wider participation	Kindly refer revised Technical Specification
898	Network Manager	53	"Should be capable of showing hop-by-hop flow path and drops on links taken by a flow between 2 end points.	Requesting to remove the clause. Justification : For wider participation	Kindly refer Revised Technical specification
899	Network Manager	53	Central controller should provide detailed traffic flow analytics to search and see what protocols/port are used and how much data is transferred between 2 end-points during a period of time.	Requesting to remove the clause. Justification : For wider participation	Kindly refer Revised Technical specification
900	Network Manager	53	Should provide building customized dashboards using any of the collected telemetry data.	Requesting to remove the clause. Justification : For wider participation	Kindly refer Revised Technical specification
901	erconnect Swit	30,37,39	Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN, **data plane telemetry to trace path and per hop latency for a flow ,** buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations.	Requesting to remove "data plane telemetry to trace path and per hop latency for a flow". Also, requesting to include sflow/netflow with IPFIX Justification : For wider participation	Kindly refer Revised Technical specification
902	ine Switch for I	203	EVPN+VXLAN (No proprietary protocols to be deployed for leaf-spine fabric), ESI LAG or equivalent technology. Should support EVPN Route Types (Type-1, Type-2, Type-3, Type-4, Type-5,), Tenant routed Multicast / OISM, OSPF, ISIS, BGP	EVPN+VXLAN (No proprietary protocols to be deployed for leaf-spine fabric). Should support EVPN Route Types (Type-1, Type-2, Type-3, Type-4,Type-5,), Tenant routed Multicast / OISM, OSPF/ISIS, BGP Justification: Since Spine is a Layer 3 Device with no Layer 2 termination on it, hence there is no requirement for Layer 2 protocols such as ESI or LAG	Kindly refer Revised Technical specification
903	ine Switch for I	203	Port, VLAN & Routed ACL,802.1x,16K or higher ACL Entries/group based-segmentation- entries, GRE (Must Support 1000 or Higher GRE Tunnels or 1000 VXLAN Tunnels)	Port/ VLAN/Routed ACL ,9K or higher ACL Entries/group based-segmentation-entries, GRE/VXLAN Tunnel (Must Support 1000 or Higher GRE Tunnels or 1000 VXLAN Tunnels) Justification: Since Spine is a Layer 3 Device with no Layer 2 termination on it, hence there is no requirement for Layer 2 ACLs.	Kindly refer Revised Technical specification

904	ine Switch for I	203	Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sFlow/Netflow, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN, data plane telemetry, buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations.	Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sFlow/Netflow, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN. Same OS across all the proposed network switches for simplified operations. Justification: Data Plane Telemtry and buffer queue depth monitoring is required at the access/leaf level where the application is terminated. Spine acts as a layer 3 backbone to interconnect leaf switches and with the deep buffer and high BW links, this is not a necessity here	Kindly refer Revised Technical specification
905	ine Switch for I	203	Virtual output Queue VoQ)/Egress QoS/Intelligent Buffer/dynamic buffer, WRED,ECN,LLQ,PTP, 8GB Packet Buffer per line card or equivalent, 802.1Qbb,8 queues/port, WRR	Virtual output Queue VoQ)/Egress QoS/Intelligent Buffer/dynamic buffer, WRED,PFC/ECN,PTP, 8GB Packet Buffer per line card or equivalent,8 queues/port, WRR	Kindly refer Revised Technical specification
906	ine Switch for I	203	Should support 250K IPv4 Routes, 125K IPv6 Routes, 100K IPv4/v6 Multicast Routes.	Should support 250K IPv4 Routes, 125K IPv6 Routes, 32K IPv4,8K IPv6 Multicast Routes.	Kindly refer Revised Technical specification
907	ine Switch for I	204	EVPN+VXLAN (No proprietary protocols to be deployed for leaf-spine fabric), ESI LAG or equivalent technology. Should support EVPN Route Types (Type-1, Type-2, Type-3, Type-4, Type-5,), Tenant routed Multicast / OISM, OSPF, ISIS, BGP	EVPN+VXLAN (No proprietary protocols to be deployed for leaf-spine fabric). Should support EVPN Route Types (Type-1, Type-2, Type-3, Type-4,Type-5,), Tenant routed Multicast / OISM, OSPF/ISIS, BGP Justification: Since Spine is a Layer 3 Device with no Layer 2 termination on it, hence there is no requirement for Layer 2 protocols such as ESI or LAG	Kindly refer Revised Technical specification
908	ine Switch for I	204	Port, VLAN & Routed ACL,802.1x,16K or higher ACL Entries/group based-segmentation-entries, GRE (Must Support 1000 or Higher GRE Tunnels or 1000 VXLAN Tunnels)	Port/ VLAN/Routed ACL ,9K or higher ACL Entries/group based-segmentation-entries, GRE/VXLAN Tunnel (Must Support 1000 or Higher GRE Tunnels or 1000 VXLAN Tunnels) Justification: Since Spine is a Layer 3 Device with no Layer 2 termination on it, hence there is no requirement for Layer 2 ACLs.	Kindly refer Revised Technical specification
909	ine Switch for I	204	Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sFlow/Netflow, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN, data plane telemetry, buffer queue depth monitoring, Same OS across all the proposed network switches for simplified operations.	Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sFlow/Netflow, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN. Same OS across all the proposed network switches for simplified operations. Justification: Data Plane Telemtry and buffer queue depth monitoring is required at the access/leaf level where the application is terminated. Spine acts as a layer 3 backbone to interconnect leaf switches and with the deep buffer and high BW links, this is not a necessity here	Kindly refer Revised Technical specification
910	ine Switch for I	204	Virtual output Queue VoQ)/Egress QoS/Intelligent Buffer/dynamic buffer, WRED,ECN,LLQ,PTP, 8GB Packet Buffer per line card or equivalent, 802.1Qbb,8 queues/port, WRR	Virtual output Queue VoQ)/Egress QoS/Intelligent Buffer/dynamic buffer, WRED,PFC/ECN,PTP, 8GB Packet Buffer per line card or equivalent,8 queues/port, WRR	Kindly refer Revised Technical specification
911	ine Switch for I	205	Should support 250K IPv4 Routes, 125K IPv6 Routes, 100K IPv4/v6 Multicast Routes.	Should support 250K IPv4 Routes, 125K IPv6 Routes, 32K IPv4,8K IPv6 Multicast Routes.	Kindly refer Revised Technical specification
912	Border Leaf Switch	208	Port, VLAN & Routed ACL. Should support minimum 16K ACL entries/terms or minimum 32K prefix/host entries for traffic segmentation.	Port, VLAN & Routed ACL. Should support minimum 14K ACL entries/terms or minimum 32K prefix/host entries for traffic segmentation.	Kindly refer Revised Technical specification
913	Interconnect Switch	215	Switch should support all functions required to operate as an interconnect switch connecting various devices including firewall and routers with an non-blocking fabric	Requesting to add 400K Ipv4/Ipv6 route scale. Justification: Requesting to add scale values	As per Tender Document

914	onnect Switch	216	Switch should support all functions required to operate as an interconnect switch connecting various devices including firewall and routers with an non-blocking fabric	Requesting to add 400K Ipv4/Ipv6 route scale. Justification: Requesting to add scale values	As per Tender Document
915	WAN Switch	218	Switch should support all functions required to operate as a WAN Switch acting as interface between Service Provider Links and WAN Router	Requesting to add 400K Ipv4/Ipv6 route scale. Justification: Requesting to add scale values	As per tender document
916	etwork Manag	230	Should provide ability to view Telemetry data over a timeline. The Data Should be available for at least 60 days.	Should provide ability to view Telemetry data over a timeline. The Data Should be available for at least 30 days.	Kindly refer Revised Technical specification
917	CE Router	221	Type of Switch: Chassis Based/Non-Chassis Based	Please remove Switch and mention Router as the specifications are for Router	Kindly refer Revised Technical specification
918	CE Router	221	The Router should be populated with redundant Routing Card/Engines/control plane /supervisor engine/multi-core x86 CPU	Should have multi-core x86 CPU Justification: Since the redundant routers would be deployed, requesting to remove the requirement of redundant routing engines/sup, this is more of the requirement in chassis based router or in the Core/backbone network.	Kindly refer Revised Technical specification
919	CE Router	221	Aggregated Throughput (Gbps) : 1600 Or higher	Requesting to change the routing throughput to 500gbps: Justification: Unlikely the throughput of any layer-3 Switch, The routing throughput is calculated differently. Requesting to reduce it to 500Gbps	As per tender document
920	CE Router	222	Port population: Should be supplied with 16x 10G SFP+ ports and 6 No. of 100G QSFP28 ports with non- blocking architecture and wire-speed from day 1.	Requesting to modify the clause as below: Port population: Should be supplied with 16x 10G SFP+ ports and 6 No. of 100G QSFP28 ports with non- blocking architecture and wire-speed from day 1. Justification: To meet the throughput requirement	As per tender document
921	CE Router	222	Feature Support: Device, OS, Optics, Manager from same OEM. Should be managed through unified Network Manager.	Requesting to remove this clause Justification: Generally, the Network Manager is required to manage the Network Switch Fabric , hence requesting to remove the clause. Also there is a separate NMS solution is asked to monitor all the network equipments.	Kindly refer Revised Technical specification
922	Internet Route	223	No. of 10G SFP+ ports (Fiber /Copper): 16 or higher	Requesting to modify the clause as below: No. of 10G SFP+ ports (Fiber : 16 or higher Justification: Since the "Coppper/Fiber" ports are something that is required in the switch. In routers , 10G interfaces are generally fiber, basis the type of link that will be connecting to the router . Hence requesting to modify it to remove the ambiguity.	Kindly refer Revised Technical specification
923	Internet Route	223	Port Population: Should be supplied on day 1 with 4 x 1000Base-LX Single Mode SFP transceivers, 4 x 10/100/1000Base-T Interface Ports and 4 x 10G Base SR Transceivers. Should be scalable to support additional 4 X 40/100G QSFP ports; Fully Populated from Day-1	Requesting to modify the clause as below: Router should have minimum 20 x 10G and 6 x 40 / 100G QSFP28 LAN / WAN Interface loaded with 10 x 1 G Multimode Fiber SFP, 10 x 10G Multimode Fiber SFP+ , 4 x 40G QSFP28 and 2 x 100G QSFP56	Kindly refer Revised Technical specification
924	Internet Route	223	Switching Capacity (Gbps): 256 or higher	Throughput: Router should have minimum IP forwarding throughput of 500 gbps Justification: Considering the requirement is of router not a Layer-3 Switch. Hence requesting to ammend the clause and throughput accordingly.	Kindly refer Revised Technical specification

925	Internet Route	224	Feature Support: Device, OS, Optics, Manager from same OEM. Should be managed through unified Network Manager.	Requesting to remove this clause Justification: Generally, the Network Manager is required to manage the Network Switch Fabric , hence requesting to remove the clause. Also there is a separate NMS solution is asked to monitor all the network equipments.	Kindly refer Revised Technical specification
926	Web Proxy	302	SWG appliance must have 4x10 GE SFP slots populated with multimode transceiver & 4 x 1GE RJ45 interfaces on each appliance from day one. All these interfaces should be available simultaneously from day one.	Requesting to change to "SWG appliance must have 4x10 GE SFP slots populated with multimode transceiver on each appliance from day one. All these interfaces should be available simultaneously from day one" Web proxy is not an inline network device and hence it doesn't require port density like a firewall, in current form the clause is restricting our participation. Hence requesting change.	Kindly refer Revised Technical specification
927	Web Proxy	303	The solution should provide geo-location awareness for security incidents.	Requesting to change to " The solution should provide geo-location/threat information for security incidents" Web proxy sits inside the network and different vendor have different level of threat information dashboard, geo-location is mostly on the perimeter firewall, while proxy sits inside the network, thus requesting change	Kindly refer Revised Technical specification
928	Web Proxy	304	SWG should not introduce more than 10 microsecond latency	Requesting to remove as latency depends on multiple parameters such as load, policy, granularity, interface, memory consumption	Kindly refer Revised Technical specification
929	Web Proxy	304	The proposed solution must be able to deliver at least 10 Gbps of throughput on full load after enabling multiple security modules together	Requesting to remove, Web proxy is not an inline network firewall device, it is out of path network device working on user requests, In current form this is vendor specific and restricting our participation.	Kindly refer Revised Technical specification
930	Web Proxy	304	The SWG should have both SSL/TLS and SSH Inspection capabilities	Requesting to change to "The SWG should have both SSL/TLS Inspection capabilities" SSH is not a web port in the network, in current form it is specific to firewall vendor thus requesting change.	Kindly refer Revised Technical specification
931	Web Proxy	305	The propose unit shall be able to support the following configuration of explicit proxy: i Proxy FQDN ii Max HTTP request length iii Max HTTP message length iv Add headers to Forwarded Requests v Proxy Port vi Interfaces that listen to proxy request	Requesting to change as "The propose unit shall be able to support the following configuration of explicit proxy: i Proxy FQDN v Proxy Port vi Interfaces that listen to proxy request" In current form is it specific to vendor thus requesting change for wider participation	Kindly refer Revised Technical specification
932	Web Proxy	306	The proposed solution must be able to deliver at least 1 Gbps of Application inspection throughput	Requesting to remove, Web proxy is not an inline network firewall device, it is out of path network device working on user requests, In current form this is vendor specific and restricting our participation.	As per tender document
933	Web Proxy	306	SWG must have capability to do Cloud application based routing not by means of manually adding IPs and or FQDNs i.e. appliance should have database of O365 readily available to select as destination address in security policy and destination address in static route configuration to give particular ISP path	Requesting to change to "SWG must have capability to do Cloud application based routing not by means of manually adding IPs and or FQDNs i.e. appliance should have database of O365 readily available to select as destination address in security policy" in current form it is specific to OEM thus requesting change	Kindly refer Revised Technical specification
934	Web Proxy	306	Should be able to block, allow or monitor only using AV signatures and file blocking based on per security policy based or based on authenticated user groups with configurable selection of the following services and their equivalent encrypted versions, wherever applicable: HTTP, SMTP, POP3, IMAP, FTP, CIFS, NNTP, SSH, MAPI	Requesting to change to "Should be able to block, allow or monitor only using AV signatures and file blocking based on per security policy based or based on authenticated user groups" MAPI, POP3 etc are not web ports they are email channels making it not relevant for web proxy, thus requesting change as in current form it is vendor specific.	Kindly refer Revised Technical specification
935	Web Proxy	306	SWG should offer both anti-virus scanning options - Proxy mode and Flow (streaming) mode.	Requesting to change to "SWG should offer anti-virus scanning and anti-malware analysis" In current form it is OEM specific thus requesting change	Kindly refer Revised Technical specification
936	Web Proxy	306	The SWG should have capability to protect against Denial of Service (DOS) and DDOS attacks. DOS and DDOS protection should be applied and attacks stopped before security policy look-ups.	Requesting to remove as DOS/DDOS is asked as a dedicated solution DOS/DDOS are perimeter attack and Web Proxy sits inside the network	Kindly refer Revised Technical specification
937	Web Proxy	307	The proposed SWG appliance should be able to provide protection against attacks like Cross Site Scripting, SQL-Injection, Generic Attacks, Trojans, Information disclosure, Credit Card Detection, Bad Robot etc.	Requesting to remove as these are WAF specific features which is already ask in RFP	Kindly refer Revised Technical specification
938	Web Proxy	307	SWG should have capabilities to limit number of parameters in URL, number of cookies in request, number of headers lines in request, total URL and Body parameters in length to block advanced HTTP layer attacks.	Requesting to remove as these are WAF specific features which is already ask in RFP	Kindly refer Revised Technical specification

939	Web Proxy	307	The proposed system shall allow administrator to prevent sensitive data from leaving the network. 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. The DLP capability shall support the following protocol & activities: i HTTP/HTTPS POST, HTTP/HTTPS GET ii FTP PUT, GET iii SMTP, IMAP, POP3, SMTPS, IMAPS, POP3S	Requesting to change to "The proposed system shall allow administrator to prevent sensitive data from leaving the network. 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" except for HTTP/HTTPS mentioned ports are email, firewall specific and not web ports wherein in current form becoming specific to OEM thus requesting change	Kindly refer Revised Technical specification
940	Web Proxy	307	The DLP capability shall be configured by creating individual rules, combining the rules into sensors, and then assigning them to profiles which in turn bind to firewall policies.	Requesting to change to "The DLP capability shall be configured by creating individual rules or combining the rules into sensors, and then assigning them to profiles which in turn bind to policies"	Kindly refer Revised Technical specification
941	Web Proxy	307	Ban: if the user is authenticated, will block all traffic to or from the user using the protocol that triggered the rule and the user will be added to the Banned User list. If the user is not authenticated, all traffic of the protocol that triggered the rule from the user using will be blocked.	Requesting to change to "Ban: if the user is authenticated, will block all traffic to or from the user using the protocol that triggered the rule" in current form it is specific to OEM, thus requesting change	Kindly refer Revised Technical specification
942	SSL VPN	312	The appliance should be dedicated SSL VPN Gateway and not a part of UTM/ firewall/ NGFW/ ADC device It should have should have 1x1GbE port for management and 8x10 SFP+ ports Should be populated with its transceivers	Requesting to change to "The appliance should be dedicated SSL VPN Gateway. It should have should have 1x1GbE port for management and 8x10 SFP+ ports Should be populated with its transceivers" in current form it is OEM specific and thus requesting change for wider participation	Kindly refer Revised Technical specification
943	SSL VPN	312	The appliance should have multicore CPU, 64GB RAM, 1TB or higher HDD and dual power supply.	Requesting to change to "The appliance should have multicore CPU, 64GB RAM, 800GB or higher HDD/SSD with redundant hot swappable field replaceable dual power supply and fan module/tray" In multiple solutions in RFP the storage ask is 250Gb on perimeter solution and 1Tb ask on VPN gateway is OEM specific, the field replaceability along with redundancy on power supply, fan module is very important considering the VPN device is inline perimeter network device wherein during failure scenario individual modules replacement ensures higher TCO as against every time removing the device, reconfiguring it during the RMA	Kindly refer Revised Technical specification
944	SSL VPN	312	The solution Should have dedicated hardware SSL card and should support 35 Gbps of SSL Throughput	Requesting change to "The solution Should have dedicated hardware SSL card and should support 35 Gbps of VPN throughput" SSL throughput is relevant for SSL off loaders since this is a VPN device it should have VPN throughput mentioned.	Kindly refer Revised Technical specification
945	SSL VPN	312	The appliance should support 35 Gbps of compression throughput. This capability shall be compatible with most modern browsers, requiring no additional software.	Requesting to remove as this is OEM specific	Kindly refer Revised Technical specification
946	SSL VPN	312	The solution must provide ranking of at least 4 authentication methods for granular authentication of VPN users	Requesting to remove as this is OEM specific	Kindly refer Revised Technical specification
947	SSL VPN	313	The solution should also provide Step-up authentication. This feature allows a per-request policy to authenticate a user at any time during a VPN session. Per-request policy subroutine allows you to create time-limited sub sessions to allow user access to areas of an application based on a different gating criteria. the following authentication types for step-up authentication should be supported: Multi-factor authentication through Radius authentication Certificate-based authentication Password-based authentication	Requesting to change to "The solution should also provide Step-up authentication. This feature allows a per- request policy to authenticate the following authentication types for step-up authentication should be supported: Multi-factor authentication through Radius authentication Certificate-based authentication Password-based authentication" requesting change for wider participation as currently it is OEM specific.	As per Tender Document
948	SSL VPN	313	The Solution should be able to support robust endpoint posture inspection and deny access for non-compliance endpoints. The Solution must support the following checks: * Able to perform Antivirus/Malware software checks, including checks for Enabled State, Engine & Database version, Last Scan, and Last Update of the antivirus software. * Able to perform domain check to auto connect to VPN when outside the office network. * Able to perform IP address / Geolocation check to restrict access from unwanted locations. "* Able to perform Operating System, Windows Registry, File or Process checks. * Able to check if mobile devices have been jailbroken."	Requesting to change to "The Solution should be able to support robust endpoint posture inspection and deny access for non-compliance endpoints. The Solution must support the following checks: * Able to perform Antivirus/Malware software checks, * Able to perform domain check * Able to perform IP address / Geolocation check to restrict access from unwanted locations. "* Able to perform Operating System" requesting change for wider participation as currently it is OEM specific and in overall RFP NAC/AAA is asked which should be used as central authenticator layer irrespective the user comes from land/vpn or wireless.	As per Tender Document

949	NAC(Included AAA)	330	The solution should provide below Deep Compliance checks on minimum based on OESIS Framework from Day 1 on windows & mac-OS endpoints: 1) Check Specific Anti-malware product version and last signature update date 2) Threats detected by the installed Anti-malware product with option to configure threat exclusion. 3) Disk Encryption status of System & Local volume Encryption tool & its version.	Requesting to change to "The solution should provide below Deep Compliance checks on minimum from Day 1 on windows, Linux & mac-OS endpoints: 1) Check Specific Anti-malware product version and last signature update date 2) Threats detected by the installed Anti-malware/Vulnerability scanner product with option to configure threat exclusion. 3) Disk Encryption status of System & Application tool & its version" in current form it is OEM specific thus requesting change	As per Tender Document
950	NAC(Included AAA)	330	The solution should provide the end user to request for temporary access in case of authentication/authorization failure that can be approved by a admin	Requesting to remove as this is OEM specific	Kindly refer Revised Technical specification
951	NAC(Included AAA)	330	The solution should allow endpoint to detect Man In the Middle (MITM) attack using the agent	Requesting change as this is firewall related capability not a function of NAC	Kindly refer Revised Technical specification
952	NAC(Included AAA)	330	The solution should have http/SNI proxy based remediation options	Requesting change as this is firewall, web proxy related capability not a function of NAC	Kindly refer Revised Technical specification
953	IPS/IDS	261	NIPS solution should be a purpose built dedicated standalone appliance and not an integrated firewall module or UTM appliance.	Requesting change to "NIPS solution should be a dedicated appliance with dedicated processing engine and not a part of DDOS, UTM, Web Proxy, appliance" many vendors use the common off the shelf OS thus it is important wherein dedicated appliance is required it should also have dedicated processing engines and not shared with other modules	As per Tender Document
954	IPS/IDS	261	The appliance must have Real World Throughput of 10 Gbps and scalable up to 30 Gbps for future requirements on the same appliance	Requesting to change to "The appliance must have Real World Throughput of 30 Gbps" requesting change as it is OEM specific.	Kindly refer Revised Technical specification
955	IPS/IDS	262	Should have capability for Host quarantine and rate limiting	Requesting to change to "Should have capability for Host quarantine/IP blacklisting and rate limiting" different vendor have different approach the requesting change doesn't change any functionality but allow for more participation thus requesting change	Kindly refer Revised Technical specification
956	IPS/IDS	264	PS must support Inbound SSL Inspection detection and prevention using dynamic agent based key for ECDHA cypher suits	Requesting to change to "IPS must support Inbound SSL Inspection detection and prevention" in current form this is OEM specific thus requesting change for wider participation as the requested change doesn't change any functionality of the RFP	As per Tender Document
957	IPS/IDS	264	IPS must have multiple signature less engines on the appliance without degrading the performance.	Requesting to change to "IPS must have both signature and signature less engines on the appliance without degrading the performance. It must have 25000+ plus pre-build signatures from day1 excluding the custom signatures" IPS must have both approaches as without signatures every time a known attack or traffic is seen it has to be inspected with DPI leading to performance overhead increased latency thus it is important to have the signature count mentioned to improve the overall efficacy of the solution.	As per Tender Document
958	Internet Firewall	259	60 Gbps or higher with 128 KB HTTP/HTTPs	Requesting to change to "60 Gbps or higher with TCP or HTTP/HTTPs" 128KB is a very large packet and only a specific OEM provides reference numbers on it for a interface with MTU of 1500byte 128KB packet would lead to lot of fragmentation thereby negatively impacting the CPU	As per Tender Document
959	Internet Firewall	259	100 Million Layer 4 sessions or 40 Million Layer 7 sessions	Requesting to change to "100 Million Layer 4 sessions or 30 Million Layer 7 sessions measured with Firewall and Application controlled enabled" current clause in as is form is giving a particular OEM advantage thus for equal participation requesting change	Kindly refer Revised Technical specification
960	Internet Firewall	260	Minimum 3 Million Layer 4 sessions or Minimum 1.2 Million Layer 7 sessions	Request to change to "Minimum 3 Million Layer 4 sessions or Minimum 600K Layer 7 sessions measured Firewall and Application Control enabled" current clause in as is form is giving a particular OEM advantage thus for equal participation requesting change	As per Tender Document

961	Internet Firewall	260	35 Gbps (Packet size: 128 KB HTTP/HTTPs) or Higher	Requesting to change to "35 Gbps (measured with TCP or HTTP/HTTPs) or Higher" 128KB is a very large packet and only a specific OEM provides reference numbers on it for a interface with MTU of 1500byte 128KB packet would lead to lot of fragmentation thereby negatively impacting the CPU	As per Tender Document
962	Internet Firewall	260	Redundant Power Supply	Requesting to change to Redundant hot swappable and field replaceable power supply" as power supply is an environment directly exposed to the environmental conditions and leading to a failure pf PSU with no field replaceability requires every time the appliance to be replaced manually and then configuring the new appliance thereby increasing the overall TCO and higher downtime window	As per Tender Document
963	Internet Firewall	260	Redundant FAN for fully loaded chassis from day 1	Requesting to change to Redundant hot swappable and field replaceable fan fully loaded chassis from day 1" as fan is an environment directly exposed to the environmental conditions and leading to a failure of fan with no field replaceability requires every time the appliance to be replaced manually and then configuring the new appliance thereby increasing the overall TCO and higher downtime window	As per Tender Document
964	Web Proxy	123	The Secure Web Gateway should be Hardware based, Reliable, purpose-built security appliance with hardened operating system.	Purpose built Hardware is only with one OEM, however critical aspects of the security is puspose built OS, Hence request you to please amend the clause as : The Secure Web Gateway should be dedicted Hardware based, Reliable, purpose-built hardened operating system security	The Secure Web Gateway should be Hardware based, Reliable, purpose-built appliance with hardened operating system.
965	Web Proxy	124	SWG appliance must have 4x10 GE SFP slots populated with multimode transceiver & 4 x 1GE RJ45 interfaces on each appliance from day one. All these interfaces should be available simultaneously from day one	As per our understanding of the RFP the back plane of the Network is all 10G, Hence we request you to please amend the clause and remove the requirement the 1G RJ45 as : SWG appliance must have 6x10 GE SFP slots populated with multimode transceiver on each appliance from day 1 and one addational IDRAC/Console port as well . All these interfaces should be available simultaneously from day one	Kindly refer Revised Technical specification
966	Web Proxy	124	The solution should have complete license for web security, URL Filtering, Content Control inspection, Antivirus, SSL, and content inspection should be built in solution for user base from the first day in same appliance. The Solution should intercept user requests for web destinations (HTTP, HTTPs and FTP) for web security, Critical & Sensitive data upload and in-line malware scanning.	Web proxy should have complete control over the data exfiltration and should happen over the same proxy appliance, so that there is no user and performance impact when user is browsing the internet Hence request you to please amend the clause as : The solution should have complete license for web security, URL Filtering, Data Leakage Control, Content Control inspection, Antivirus, SSL, and content inspection should be built in solution for user base from the first day in same appliance without depending on ICAP/ other solutions. The Solution should intercept user requests for web destinations (HTTP, HTTPs and FTP) for web security, Critical & Sensitive data upload and in-line malware scanning.	As per Tender Document
967	Web Proxy	124	The solution should provide proxy, caching, on box known malware inspection, content filtering, SSL inspection, protocol filtering, Web data leakage prevention and inline AV in block mode on the same Appliance, with application visibility and control.	Data Leakage using various methods like images, sturctured Data, unsturctured data using fingerprinting. Only mentioning Data Leakage prevention will not enforce bidder to provide robust solution to ERNET. Hence request you to please amend the clause as : The solution should provide proxy, caching, on box known malware inspection, content filtering, SSL inspection, protocol filtering, Web data leakage prevention within Images, fingerprinted documents and inline AV in block mode on the same Appliance, with application visibility and control	As per Tender Document

968	Web Proxy	124	Proposed solution should be able to inspect malicious information leaks even over SSL by decrypting SSL natively. Solution should also provide the decryption bypass to be done for the privacy categories.	Web proxy solution for ernet which serves as backbone to national infrastructure should have clear understanding of different languages including Hindi along with predefined Indian based templates for identification of data processing through proxy. Hence request you to please amend the clause as : Proposed solution should be able to inspect malicious information leaks even over SSL by decrypting SSL natively. Solution should also provide the decryption bypass to be done for the privacy categories and must .provide the information protection and data exfiltration based on the 1000+ predefined templates including Indian Data and also the flexibility to define the policies based on the data type , with specific categories and geo location with support for 20+ languages including Hindi.	As per Tender Document
969	Web Proxy	124	The Solution should be designed in active-active mode with the appliances, managed through centralized management console on server platform.	We would request you to please explictly mention that on box management will not be permitted as many OEMs mention Centralized management on the box as well, so amend the clause as : The Solution should be designed in active-active mode with the appliances, managed through centralized management console on server platform. On box Management will not be permitted.	As per Tender Document
970	Web Proxy	124	The solution should be capable of dynamically blocking a legitimate website which has become infected in real time when the threat has been removed for security categories and vulnerabilities. The solution should have ability to block anonymizer sites or proxy avoidance tools.	We would suggest mention few of the proxy avoidance and anonymizer sites which are known and very critical to be blocked as those would need to be blocked up front for better security posture across ERNET Network: The solution should be capable of dynamically blocking a legitimate website which has become infected in real time when the threat has been removed for security categories and vulnerabilities. The solution should have ability to block anonymizer sites or proxy avoidance tools. Below mentioned tools should be blocked from first day and should be provided in default protocol database Ghost surf, Google web accelerator, Hoopster, Jap, Real tunnel, Socks online, Toonel, Tor, Yourfreedom.	As per Tender Document
971	Web Proxy	124	The solution shall be able to support various form of user Authentication methods simultaneously, including: Local Database, LDAP, Windows AD, SAML, Terminal Server Agent support for Single Sign On	Terminal server agent, SAML are specific to OEM and also not related to proxy in network. It is using usually based IPs, Users which can be provided using Active Directory integration using Kerberos and NTLN with LDAP based which is industry best practice. Hence request you to please amend the clause as : The solution should have authentication options for users/groups, It should supports authentication of users via Integrated Windows Authentication (Kerberos), NTLM (NTLM v1 and v2 in Session Security), and LDAP.	As per Tender Document
972	Web Proxy	124	The solution should have at least millions of websites in its URL filtering database and' should have pre-defined URL categories and application filters along with YouTube, Facebook and linked-in controls. Solution vendor should ensure that along with predefined categories from day-1, it should have ability to configure custom categories for organization	We would request you to please mention some minimum count of no of websites, categories, protocol, along with latest AI applications to be blocked or controls for better and secure product, otherwise it will provide less and ineffective solution. Hence request you to please amend the clause as: The solution should have at least 40 millions of websites in its URL filtering database and' should have pre-defined URL categories and application filters along with YouTube, Facebook and linked-in controls. Solution vendor should ensure that along with 90+ predefined categories &100+ pre- defined protocols should be available on product from day-1, it should have ability to configure custom categories for organization with support for like AI ML Applications with Generative AI for Multimedia, Conversation and Text & Code Advanced Malware Command & Control category, iframe detection category, Key logger and Spyware category, Mobile malware category, Generative AI – Multimedia, Conversation and Text & Code, P2P software database from day 1 to control/block	As per Tender Document
973	Web Proxy	125	The solution should support ICAP or API integration for third party inputs for web filtering database or threat feeds if required	We understand that ERNET is looking for API integration to create the custom category using IPs, Domain and URLs.	As per Tender Document

974	Web Proxy	125	The solution should apply security policy for multiple protocols in multiple categories. This includes the ability to allow, block, log, and assign quota time for multiple security categories.	For a robust solution it is advisable that the minimum count should be mentioned for no of categories and protocols. Hence request you to please amend the clause as : The solution should apply security policy for 100+ protocols in 90+ categories. This includes the ability to allow, block, log, and assign quota time for multiple security categories.	As per Tender Document
975	Web Proxy	126	When SSL encrypted traffic from users will hit the SWG, then the proposed solution should have the capability to inspect & process that encrypted traffic with a minimum processing speed of 1 Gbps	Not all leading OEM in proxy field mention processing speed or throughput, hence request you to please amend the clause as : When SSL encrypted traffic from users will hit the SWG, then the proposed solution should have the capability to inspect & process that encrypted traffic	As per Tender Document
976	Web Proxy	126	Each user traffic should hit the SWG solution when they are trying to access Internet & from day one the proposed SWG should be capable to handle minimum 40,0000 such session request from end-points on every seconds	Not all leading provide mention such number expect Firewall vendors or Cisco, we would request you mention the user count to support the same. Hence request you to please amend the clause and mention 250 users supports: Each user traffic should hit the SWG solution when they are trying to access Internet & from day one the proposed SWG should be capable to handle 250 users / minimum 40,0000 such session request from end-points on every seconds	As per Tender Document
977	Web Proxy	126	SWG should not introduce more than 10 microsecond latency	Not a Proxy related clause, its more of Firewall releated, hence request you to please delete the same.	Kindly refer Revised Technical specification
978	Web Proxy	126	The physical interface should be capable of link aggregation as per IEEE 802.3ad standard, allowing the grouping of interfaces into a larger bandwidth 'trunk'. It should also allow for high availability (HA) by automatically redirecting traffic from a failed link in a trunk to the remaining links in that trunk.	Not a proxy related clause, its more of Firewall/ link load balancer releated, hence request you to please delete the same.	Clause stands deleted
979	Web Proxy	126	The SWG should support at least 250 concurrent users, and it also should support inbuilt Virtualization functionality with minimum 5 Virtual SWG license so that the same SWG hardware can be configured as 5 logically separated SWG solutions if required.	As the proxy solution dependent on user based policy, and concurrency is usually on Firewall or IP based and we don't understand the requirement of Virtual swg as these would be user based requests. Hence request you to please amend the clause as : The SWG should support total of 250 users	The SWG should support at least 250 concurrent users
980	Web Proxy	126	The proposed solution must be able to deliver at least 10 Gbps of throughput on full load after enabling multiple security modules together.	This clause is not related to Proxy and looks like its favouring a particular OEM, Hence request you to please delete this clause	As per Tender Document
981	Web Proxy	126	The SWG should have both SSL/TLS and SSH Inspection capabilities	SSH is a non proxy related protocol, Hence request you to please amend the clause as: The SWG should have both SSL/TLS and SSH Inspection capabilities	Kindly refer Revised Technical specification
982	Web Proxy	126	The SWG shall provide role and profile based access control and should be able to map the same with Active Directory users. The solution should able to fetch the user data from Active Directory server automatically.	Better clarity request you to please re-phrase as Mapping is not proxy solution does, its more of web proxy integration is done with AD to apply users based policies and controls. Hence request you to please amend the clause as : The SWG shall provide user/role/ profile based access/policy control by integrating with Active Directory.	As per Tender Document
983	Web Proxy	127	The solution should be proposed with at least 10 numbers of 2FA via Tokenf or admin users. In case the functionality is not an in-built feature of the proposed solution, bidder is allowed to quote additional solution to fulfil the requirement	2FA is a separate solution not a part of the proxy, Hence request you to please amend the clause as : The solution should be able to ingrate with Radius server for 2FA for console login.	The solution should be able to ingrate with Radius/AAA/TACACS+ server for 2FA for console login
984	Web Proxy	127	The proposed system should have integrated Web Content Filtering solution without external solution, devices or hardware modules	Proxy solution works with Centralized management and database outside of the proxy appliance. Please confirm if that be okay ? Otherwise is a single OEM solution.	The proposed system should have Web Content Filtering solution
985	Web Proxy	127	The propose unit shall be able to support the following configuration of explicit proxy: i Proxy FQDN ii Max HTTP request length iii Max HTTP message length iv Add headers to Forwarded Requests v Proxy Port vi Interfaces that listen to proxy request	Request and message length are part of inbuilt capability of the solution, asking such clause as restrict in nature and we request you to please amend the clause as : The proposed solution shall be able to support the following configuration of explicit proxy: i Proxy FQDN ii Add headers to Forwarded Requests v Proxy Port/ x-forwarder vi Interfaces that listen to proxy request	Kindly refer Revised Technical specification
986	Web Proxy	127	The SWG shall allow administrators to override Web Filtering database ratings with local settings	Please confirm if you are looking the custom category creation via this. If yes, then requst you to pleae amend the clause as : The SWG shall allow administrators to override Web Filtering database ratings with local settings or should allow to create custom URL categories	As per Tender Document

987	Web Proxy	127	The SWG should be capable to identify and prevent in-progress phishing attacks by controlling sites to which users can submit corporate credentials based on the site's URL category thus blocking users from submitting credentials to untrusted sites while allowing users to continue to submit credentials to corporate and sanctioned sites.	This Clause is not releated to Proxy, however an addational solution is required to achieve this requirement called as Remote browser isolation, which as per clause looks to be favouring an OEM (cisco) providing the same over the cloud. Please confirm if you are okay for cloud based solution.	Clause stands deleted
988	Web Proxy	127	The SWG must have advanced URL filtering categories to block access to Newly Registered Domains, Newly Observed Domains, and Dynamic DNS based websites.	Need clarity on the category: Newly Observed domains are you referring to Newly created domains, please confirm	The SWG must have advanced URL filtering categories to block access to Newly Registered Domains, Newly Observed/created Domains, and Dynamic DNS based websites.
989	Web Proxy	127	The SWG must have capability to filter YouTube videos by using channel ID	For Wider pariticipation, we request you to please amend the clause as : The SWG must have capability to filter YouTube videos and must have dedicated for educational and Viral videos as well	As per Tender Document
990	Web Proxy	127	The SWG must have option to rate web resource based on their DNS rating	This is more for DNS security based solution, by putting such clause you are favouring a single OEM. Hence request you to please remove this clause ask dedicated DNS security solution	Clause stands deleted
991	Web Proxy	128	The proposed solution shall support DNS-based signatures to detect specific DNS lookups for hostnames that have been associated with malware	This is more for DNS security based solution, by putting such clause you are favouring a single OEM. Hence request you to please remove this clause ask dedicated DNS security solution	Clause stands deleted
992	Web Proxy	128	The SWG must block Botnet C&C domains request at DNS level itself.	This is more for DNS security based solution, by putting such clause you are favouring a single OEM. Hence request you to please remove this clause ask dedicated DNS security solution	Clause stands deleted
993	Web Proxy	128	The SWG must have DNS Sinkhole functionality from day one to block and redirect malicious request to custom defined web portal.	This is more for DNS security based solution, by putting such clause you are favouring a single OEM. Hence request you to please remove this clause ask dedicated DNS security solution	Clause stands deleted
994	Web Proxy	128	The proposed solution must be able to deliver at least 1 Gbps of Application inspection throughput	Proxy is based on Transcation per second or no of users, Putting clauses are restrict in nature, Hence please delete.	As per Tender Document
995	Web Proxy	128	Should have the intelligence to identify & control of popular IM & P2P applications like KaZaa, Bit Torrent, Skype, You Tube, Facebook, LinkedIn etc along with VPN like Nord, OpenVPN, and Proton, Express VPN etc	VPN blocking is more of a Firewall work rather than Proxy, Hence request you to please amend the clause as :Should have the intelligence to identify & control of popular IM & P2P applications like Bit Torrent, Skype, You Tube, Facebook, LinkedIn etc	Should have the intelligence to identify & control of popular IM & P2P applications like Bit Torrent, Skype, You Tube, Facebook, LinkedIn etc along with VPN like Nord, OpenVPN, and Proton, Express VPN etc
996	Web Proxy	128	SWG must have capability to do Cloud application based routing not by means of manually adding IPs and or FQDNs i.e. appliance should have database of O365 readily available to select as destination address in security policy and destination address in static route configuration to give particular ISP path	Routing traffic to put to particular ISP is the work firewall not proxy, Hence request you to please amend the clause as : SWG must have capability to provide visibility on Cloud application by shadow IT and for O365 vendor to provide authenitication as well.	Kindly refer Revised Technical specification
997	Web Proxy	128	Should be able to block, allow or monitor only using AV signatures and file blocking based on per security policy based or based on authenticated user groups with configurable selection of the following services and their equivalent encrypted versions, wherever applicable: HTTP, SMTP, POP3, IMAP, FTP, CIFS, NNTP, SSH, MAPI	we would to understand that why any other service except Http and https is needed over proxy. This clause tryingt to include Email security within proxy, which is favouring a particular proxy and Firewall OEM. Hence request you to please delete the clause	Kindly refer Revised Technical specification
998	Web Proxy	128	SWG should offer both anti-virus scanning options - Proxy mode and Flow (streaming) mode.	for Wider pariticipation, request you to please ask for Anti-virus Scanning rather than asking the methods. Mentioning such word make the clause and bid move towards particular OEM like Fortinet	Kindly refer Revised Technical specification
999	Web Proxy	128	SWG should allow to integrate with third party threat feed from url, http, https, Malware hash through API to STIX integration	For Wider pariticipation, request you to please amend the clause as : SWG should allow to integrate with third party threat feed from url, http, https through API by creating custom categories or STIX integration	As per Tender Document
1000	Web Proxy	128	The SWG should have capability to protect against Denial of Service (DOS) and DDOS attacks. DOS and DDOS protection should be applied and attacks stopped before security policy look-ups.	DOS and DDOS protection is protected using a stateless device not via proxy and moreover this looking firewall vendor who provide basic DOS and DDOS protection. Hence request you to please delete the clause	Kindly refer Revised Technical specification
1001	Web Proxy	129	The proposed SWG appliance should be able to provide protection against attacks like Cross Site Scripting, SQL-Injection, Generic Attacks, Trojans, Information disclosure, Credit Card Detection, Bad Robot etc.	These WAF related points again favouring single OEM. Hence request you to please amend the clause as : The proposed SWG appliance should be able to provide protection against attacks like , Generic Attacks, Trojans, Credit Card Data leakage control in images etc.	Kindly refer Revised Technical specification
1002	Web Proxy	129	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)	By terminology signatures refers to Firewall, IPS kind of Devices. Please confirm what outcome you are looking at, if its Proxy then delete this clause	Kindly refer Revised Technical specification
1003	Web Proxy	129	SWG should have capabilities to limit number of parameters in URL, number of cookies in request, number of headers lines in request, total URL and Body parameters in length to block advanced HTTP layer attacks.	For Wider participation request to this clause	Kindly refer Revised Technical specification

1004	Web Proxy	129	The proposed system shall allow administrator to prevent sensitive data from leaving the network. 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. The DLP capability shall support the following protocol & activities: i HTTP/HTTPS POST, HTTP/HTTPS GET ii FTP PUT, GET iii SMTP, IMAP, POP3, SMTPS, IMAPS, POP3S	Proxy is only related to Http and https then why we other services. Please amend the clause : The proposed system shall allow administrator to prevent sensitive data from leaving the network. Administrator shall be able to define sensitive data patterns, and data matching, machine learning, finfgeprinting, slow and low data leakage attempts. These patterns and action should be blocked and/or logged when passing through the unit. The DLP capability shall support the following protocol & activities over Http and https both.	Kindly refer Revised Technical specification
1005	Web Proxy	129	The DLP capability shall be configured by creating individual rules, combining the rules into sensors, and then assigning them to profiles which in turn bind to firewall policies.	Single OEM clause binding and words like senors are also inclined towards a particular OEM. Hence request you to please delete this.	Kindly refer Revised Technical specification
1006	Web Proxy	129	Exempt: prevents any DLP sensors from taking action on matching traffic. This action overrides any other action from any matching sensors.	words like senors are also inclined towards a particular OEM. Hence request you to please delete this.	Clause stands deleted
1007	Web Proxy	129	Ban: if the user is authenticated, will block all traffic to or from the user using the protocol that triggered the rule and the user will be added to the Banned User list. If the user is not authenticated, all traffic of the protocol that triggered the rule from the user using will be blocked.	Need the clause on the term Ban as DLP within proxy block the content not Ban the user. OEM specific. Request you to please delete this clause	Kindly refer Revised Technical specification
1008	Web Proxy	130	The administrator shall be able to configure the following detection settings for Email traffic Attachment sizeii Attachment typeiii Content on Email subject or body Content on Email text attachment Sender and receiver Email address	These are Email security related clauses, Hence you to please delete this.	This Clause Stands Deleted
1009	Web Proxy	130	The SWG must provide Load sharing mode along with redundancy in case multiple virtual SWGs are created on it.	Virtual SWG are not needed unless it's a service provider or SI. Hence request you to please amend the clause as : The SWG must be able to do Load sharing mode to provide redundancy	This Clause Stands Deleted
1010	Web Proxy	130	The HA solutions should support silent firmware upgrade process that ensures minimum downtime	Please clarify the meaning of silent Firmware upgrade.	As per Tender Document
1011	Web Proxy	130	The SWG must have provision of fail-over in case of high memory utilisation on primary appliance.	OEM specific, as this fail over would be done using SLB already asked in the bid.	The SWG must have provision of fail-over mechanism for high availability
1012	Web Proxy	130	Support for Built-in Management for simple & secure management of the security appliances through integrated & Web-based GUI. All the above mentioned feature sets should be configurable through the GUI of the proposed SWG appliance.	This is the contradicting clause as centralised is asked and here you are asking Built in management, Hence request you to please delete this clause	As per tender document
1013	Web Proxy	130	The SWG should display past seven-day hit count in the policy list and policy pages along with a seven-day bar chart which shows statistics on each policy page.	OEM Specific, Request you to please delete this clause	Clause stands deleted
1014	Web Proxy	130	The SWG should provide a security rating service from day one which will help to identify potential vulnerabilities in the configuration & highlight best practices that can be used to improve the security and performance of the network, and will also calculate Security scores.	Is the organisation asking for cloud services ? If not then please delete this clause. Moreover its looks to single Oem points.	Clause stands deleted
1015	Web Proxy	130	Should support both CLI and GUI configuration management.	This is the contradicting clause as centralised is asked and here you are asking for CLI management, Hence request you to please delete this clause	as per tender document
1016	Web Proxy	130	Solution must allow administrator to choose to login in read only or read-write mode	For Wider pariticipation, request you to please amend the clause as : Solution must allow RBAC read-write control with different premission sets	as per tender document
1017	Web Proxy	131	Should have capability to provide APIs and logs for integration with other application for data exchange and should have capability for integration with Bank's Security Operation Centre applications	For Proxy as technologies there is no need for data excahange. Only thing which is requiured for SIEM integration. If that is need then we request you to please ask to SIEM integration instead of this.	Should have capability to provide APIs and log integration facility with other application for data exchange
1018	Web Proxy	131	Solution should provide separate Management server which can push policies for centralized management. Management console should provide automatic policy sync to all the remote boxes when the change is made to central console. Centralized management console can be appliance based or software server hardware based	Are you asking for EMS integration in the first part, ? Usually proxy are not required to be integrated in such fashion . Hence request you please amend the clause as : Dedicated Management console should be provided and policy must applied on all the boxes.(Hardware appliances of proxy) when the change is made to central console. Centralized management console can be appliance based or software server hardware based	clause stands deleted

1019	EMS	366	The proposed EMS solution and all modules (e.g. Configuration Management, network monitoring, server monitoring, asset management, IT Helpdesk, Change Management etc.) must be from a single OEM to fulfill the sought requirements & functionality. Bidder holds the responsibility to ensure of testing the functionality of these components/modules before proposing a solution in the bid.	NA	The clause may be read as : The proposed EMS solution and all modules (e.g. Configuration Management, network monitoring, server monitoring, asset management, IT Helpdesk, Change Management etc.) must be from a single OEM to fulfill the sought requirements & functionality. **The final EMS solution with IPAM & Switch Port Management may be an integration of OEMs to fulfill the sought requirements. In case the IPAM solution is from other OEM, the EMS OEM holds the responsibility along with bidder to accomplish the end to end integrated requirements of IPAM in EMS.** Bidder holds the responsibility to ensure testing of complete functionality of these components / modules before proposing a solution in the bid.
1020	EMS	New Clause in EMS	NA		OEM need to develop & provide a page that maps the link id , configured bandwidth & other detail of a remote site with its corresponding ipsec tunnel at Data center . The OEM needs to ensure that real time utilization of these links can be monitored in EMS & accordingly the alarms(& accordingly tickets) pertaining to above or below the particular threshold of link utilization should be enabled .
1021	EMS	New Clause in EMS	NA		EMS OEM of this bid needs to integrate EMS with the existing EMS & provide the information on the existing EMS's dashboard. Mostly all the existing EMS information will be provided over REST APIs by existing EMS; However if required EMS OEMs(both old and new) may also use other secure & Safe integration mechanisms.
1022	EMS	Ammended Clause	It should be a comprehensive SSL 256 bit secure web based IPv4 and IPv6 compliant solution, consisting of all standard features / modules of Enterprise Management Solution (EMS) such as fault management, performance management, configuration management, event management, an IT helpdesk / service desk to perform SLA management , Configuration Management Database(CMDB) ,incident, problem, document / knowledge management, asset management and has a inbuilt syslog server / capability to integrate a syslog server / or an integrated syslog server, so as to act as a sysLog aggregator,		The clause may be read as : It should be a comprehensive SSL 256 bit secure web based IPv4 and IPv6 compliant solution, consisting of all standard features / modules of Enterprise Management Solution (EMS) such as fault management, performance management, configuration management, event management, an IT helpdesk / service desk to perform SLA management , Configuration Management Database(CMDB) ,incident, problem, document / knowledge management, asset management , IP address Management & Switch Port Management and has a inbuilt syslog server / capability to integrate a syslog server / or an integrated syslog server, so as to act as a sysLog aggregator.

Annexure-B

Major Revised Clauses:

Section-1 (NIT)- Clause No. 2.3

2.3 Earnest Money Deposit (EMD): INR 15,00,00,000/- (Rupees Fifteen Crore Only). EMD shall be shall be submitted in one of the following forms:

- Insurance Surety Bonds/ Account Payee Demand Draft/Fixed Deposit Receipt from a Scheduled Commercial bank (which includes Nationalized Banks)/Bank Guarantee from a Commercial bank or online Payment.

1.	Beneficiary Name & Address	ERNET India, 5th Floor, Block I A Wing, DMRC IT Park, Shastri Park, Delhi-110053
2.	Bank Name	Bank of India
3.	Bank Branch & Address	Electronics Niketan 6 CGO complex New Delhi
4.	Beneficiary Account No	604810100002033
5.	IFSC code	BKID0006048

- Bank Guarantee should be issued by a scheduled commercial bank in India (**which includes Nationalized banks**), in the prescribed form provided **at Form-7** .

- In case, Bidder submit EMD in the form of Bank Guarantee then it should be valid for 6 months with claim period of 3 months.

- Bids should be valid for a minimum period of 180 days from the due date. In exceptional circumstances, the ERNET may request the Bidder(s) for an extension of the period of validity of the bid. The request and the responses thereto shall be made in writing and transmitted through speed post/registered post/courier/fax. The validity of EMD shall also be suitably extended.

- EMD submitted in the form of BG/ Demand Draft/Fixed deposit, original of the same should be deposited in the Box at ERNET India, 5th Floor, Block I A Wing, DMRC IT Park, Shastri Park, Delhi-110053 office before Bid Submission. All Bank Guarantees should be submitted through SFMS procedure. EMD is to be submitted along with the bid by the bidders. Therefore, the last date of submission of EMD will be the same as last date of submission of the bids.

- EMD is to be submitted along with the bid by the bidders. Therefore, the last date of submission of EMD will be the same as last date of submission of the bids.

- Bidder(s) who fall under EMD exemption criteria as defined in GeM GTC are exempted from EMD submission. Bidder(s) need to submit respective document(s) to establish their exemption from this clause.

- **Bids received without Earnest Money Deposit /Bid Security Declaration are liable to be rejected.**

- Bidder who fall under EMD exemption, shall submit Bid Security Declaration form along with their bids as per format prescribed below.

Bid Securing Declaration for bidders who are exempted from EMD

(on Company Letter-head)

Bidder's Name______________________

[Address and Contact Details]

Date……….

To

Registrar
ERNET India, 5th Floor,
Block-I, A Wing, DMRC IT Park,
shastri Park,Delhi-110053
Ref: Tender Document No. Tend No./ xxxx;

Sir/ Madam

We, the undersigned, solemnly declare that:

We understand that according to the conditions of this Tender Document, the bid must be supported by a Bid Securing Declaration in lieu of Bid Security.

We unconditionally accept the conditions of this Bid Securing Declaration. We understand that we shall stand automatically suspended from being eligible for bidding in any tender in Procuring Organisation for 2 years from the date of opening of this bid if we breach our obligation(s) under the tender conditions if we:

1) withdraw/ amend/ impair/ derogate, in any respect, from our bid, within the bid validity; or

2) being notified within the bid validity of the acceptance of our bid by the ERNET India:

refused to or failed to produce the original documents for scrutiny or the required Performance Security within the stipulated time under the conditions of the Tender Document.

We know that this bid-Securing Declaration shall expire if the contract is not awarded to us, upon:

1) receipt by us of your notification

   (a) of cancellation of the entire tender process or rejection of all bids or
   (b) of the name of the successful bidder or

2) forty-five days after the expiration of the bid validity or any extension to it.

Yours faithfully,
(Signature with date)
………………………..
(Name and designation)
Duly authorized to sign bid for and on behalf of [name & address of Bidder and seal of company]

Section III: (GCC) Clause no 9.3 (6)

6. Timeline for Delivery, Installation, testing, commissioning & Acceptance:

Sl. No.	Activity	Timeline (Milestone)	Project Milestones
1	Date of issue of contract. This is being referred as 'T' in the timeline column of this table.	T	
2	Delivery of the Equipment at DC	T+ 12 Weeks	**Start of Milestone-1**
3	Installation, Testing & Commissioning of Complete Equipment at DC Offering of this infrastructure under Milestone-1 for Acceptance Testing (AT) to ERNET India as per Acceptance Testing Plan (ATP).	T+ 28 Weeks	
4	Acceptance by ERNET India for Complete Milestone-1 and issuance of acceptance certificate subject to completion of complete work as per tender.	T+ 32 Weeks	**Completion of Milestone-1**
5	Delivery of the Equipment at DR	T+ 14 Weeks	**Start of Milestone-2**
6	Installation, Testing & Commissioning of Complete Equipment at DR Offering of this infrastructure under Milestone-2 for Acceptance Testing (AT) to ERNET India as per Acceptance Testing Plan (ATP).	T+ 32 Weeks	
7	Acceptance by ERNET India for Complete Milestone-2 and issuance of acceptance certificate subject to completion of complete work as per tender.	T+ 36 Weeks	**Completion of Milestone-2**
8	Site Survey (if required), Delivery, Installation, Testing & Commissioning of Complete equipment at Remote Sites and their integration with DC. Offering of this infrastructure for AT to ERNET India as per ATP.	T+ 36 Weeks	**Start of Milestone-3**
9	Acceptance by ERNET India for Complete Milestone-3 and issuance of acceptance certificate subject to completion of complete work as per tender.	T+ 40 Weeks	**Completion of Milestone-3**
10	O&M of Existing DC, DR and Remote sites	To begin within 3 months from date of instructions issued by ERNET India/CERT-In in this regard	**Milestone-4**
11	Training	To begin within 3 months from date of instructions issued by ERNET India/CERT-In in this regard.	**Milestone-5**

Timeline for Operation & Maintenance (O&M) after acceptance of individual milestones.

Sl. No	Activity	Expected time to begin O&M (Milestone)	Completion of O&M
1	O&M of Milestone 1	Within one month from the date of acceptance of Milestone 1	Two year from the effective date of acceptance of respective milestone(s).
2	O&M of Milestone 2	Within one month from the date of acceptance of Milestone 2	
3	O&M of Milestone 3	Acceptance of Milestone 3	
4	O&M of Milestone 4 [Existing Infrastructure (existing DC, DR and remote sites)]	Shall begin within 3 months from the date of instruction given by ERNET India	
5	Training	To begin within 3 months from instruction issued by ERNET India	

Note :

- On request of end user, to align the timelines of completion of all the milestones, O&M period of new DC and remote sites may be extended till the completion of O & M of new DR/existing DC-DR and payment for the extended O&M at rates quoted for O&M will be made on prorata basis (for the complete quarter or part thereof after completion of the quarter) for the extended period as quoted in PART-C**.**

- ERNET India/CERT-In reserves the right to extend the O&M till the expiry of warranty period (i.e. 3rd, 4th & 5th Year) at the originally contracted cost; calculated for the period of extension. All other terms and conditions will remain same.

Section III: (GCC) Clause no 9.5 (2)

2. **Liquidated Damages (LD):**

   If the Contractor fails to meet the prescribed timelines for respective milestones due to any reason whatsoever then in such a case ERNET India would be entitled to impose the Liquidated Damages for the delay:

   i. **Delay in Delivery of the Equipments (only for DC & DR):** @ 0.25 % of the value of delayed equipments (of the respective milestones); per week or part of the week of delayed period.

   ii. **Delay in Commissioning & offering for acceptance (for DC, DR & Remote Sites):** @ 0.5 % of the sum total value of all the equipments for respective milestone; per week or part of the week of delayed period.

Note: Overall Liquidated Damages shall be restricted to 10% of the total contract value. While calculating LD; GST will be excluded from the value on which LD is calculated; thereafter GST may be charged (if applicable) on the LD value as per S.No. 4 clause 5.3 of Section II of this document. In case, delay beyond 20 weeks, ERNET India may initiate termination for default and take remedial action(s) accordingly as per GCC Clause 12.1.

Section VI: Qualification Criteria: Bidder’s Qualification Criteria: Clause no A (3)

3. Bidder should have experience of successful implementation of similar project(s) in Central/State Government/ Govt. undertakings/ UT’s/Autonomous Bodies/Public listed companies/reputed Private organisation in India as:

Single order of Rs. 400 Crore or more;
OR
Two orders each having minimum of Rs. 200 Crore of estimated cost or more;
OR
Three orders each having minimum of Rs. 150 Crore of estimated cost or more

Similar Projects: -

(i) Setting up (Supply, Installation and Commissioning) of Data Centre (including computing, Storage, security & networking Infrastructure) &/or its Ongoing/Completed Operation & Maintenance or;

(ii) Ongoing/Completed Operation & Maintenance of Data Centres (done for minimum of two years) or Ongoing (done for minimum of two years) /completed AMC of Data Center or;

(iii) Setting up (Supply, Installation and Commissioning) of Network Operation Centres/ Security operation centres/ Smart City Projects/ Large IT networking: &/or its Ongoing/Completed Operation & Maintenance

Section VI: Qualification Criteria: Bidder’s Qualification Criteria: Clause no A (4)

4. Bidder should have experience of successful implementation (i.e supply, installation and commissioning)/ O&M/ AMC of leaf and spine architecture in data center for Central/State Government/ Govt. undertakings / UT’s/ Autonomous Bodies/Public listed companies/reputed Private organisation in India as:

Single order of Rs. 80 Crore or more;

OR

Implemented 40 Rack with leaf and spine architecture or more;

Note: This clause (4) is not applicable for those bidder(s), who are having experience of setting up of data center along with leaf and spine architecture as per clause no.3 above.

Section VI: Qualification Criteria: Bidder’s Qualification Criteria: Clause no A (5)

5. Bidder should have experience of successful implementation of Supply & Installation or operation and maintenance at 25 locations of WAN (Wide area networking*) / SDWAN (Software Defined WAN*) setup in customer office premises in single or multiple orders in Central/State Government/ Govt. undertakings / UT’s /Autonomous Bodies/ Public listed companies in India.

* WAN work experience will be established: if bidder has installed or maintaining Router/L3 switch at Customer premises. Further SDWAN work experience will be establish if bidder has installed or maintaining SDWAN equipment at Customer premises and integrated with Central location.

Note **i.r.o clause 3, 4 & 5 -** Bidder shall provide relevant copies of the customer purchase orders in support of scope of work, deliverables, project value and satisfactory work completion certificate from client. Bidder shall also provide Name, Address, email and contact no. of organization whose Purchase orders are submitted by Bidder. Order Completion date/date(s) should fall between 01/11/2019 to 31/10/2024.

For companies, project executed with NDA as an integral part of it, then a confirmation by duly appointed company secretary confirming compliance with the requirements of these clauses with detailed breakup of work order(s), clearly specifying nature of work, components and services provided, date of work order/purchase order, Completion, value of items which are meeting the relevant project experience criteria and status of implementation will be accepted. NDA copy also to be attached by bidder(s). This clause is applicable for OEM also.

Section VI: Qualification Criteria: Bidder's Qualification Criteria: Clause no A (7)

7. The bidder must have following professional(s)* working on its payroll:

SL.no	Professional Certification	Numbers
1	Prince-2/ PMP	2
2	CISA/CISSP/CISM	1
3	CDCP/CDCS	1
4	CCIE-ENT/JNCIE-ENT/CCNP-ENT/JNCIP-ENT	1
5	CCIE-Sec/JNCIE-Sec/CCNP-Sec/JNCIP-Sec/ Fortinet NSE-(4/7/8)/PCNSE , Checkpoint (CCSA/CCSE)	2
6	CCIE-DC/CCNP-DC/JNCIE-DC/JNCIP-DC	2

*Professionals must be regular employee of bidder as on date of submission of this bid. Fixed term contract/contractual employee will not be accepted. Valid certificate(s) of above professional to be submitted along with the bid with covering letter of Director HR / HR Head of bidder's organisation. Further if one employee has more than one certification(s) (e.g CISA & CDCP), it will be counted in both categories.

<u>Section VII: Scope of Work: Clause no. 9</u>

9. Acceptance Testing & VAPT

(I) Acceptance Testing (AT)

1) The draft Acceptance test plan (ATP) with detailed procedure shall be submitted by Contractor. AT shall be carried out jointly by Contractor and ERNET India/CERT-In after successful delivery, installation, testing and commissioning of project as per milestones. On successful completion of AT, certificate for the same shall be issued by ERNET India to the Contractor. Operation and Maintenance of individual milestone will start from the date of acceptance by ERNET India. Responsibility of Contractor shall include below mentioned artefacts but not limited to:

   a) Timely submission of ATP document & acceptance testing of all features as per specs.
   b) OEM(s) Certification for installed equipment(s) as per the best practices and guidelines with requisite quality as per OEM standards by OEM's manpower.
   c) Rack Layouts, Security Audited Low level and Security Audited High level design and Network security policy document.
   d) Any extra solution/tool/equipment/simulators required for showcasing features/specs during AT shall be arranged by Contractor.
   e) All equipment(s) and software items must be installed at site as per the specifications
   f) Verification for the availability of all the defined services.

2) ERNET India may require the Contractor to carry out any test and/or inspection not specified in the Contract but deemed necessary to verify that the characteristics and performance of the equipment(s) and services comply with the technical specification's codes and standards under the Contract. The Contractor shall be required to carry out such test and/or inspection at its own cost.

3) Final Acceptance for each of the milestone in the project will be given by ERNET India along with CERT-In.

4) Any other document/activity identified during project implementation period.

II. Vulnerability assessment (VA) and Penetration Testing (PT)

Vulnerability assessment (VA) and Penetration Testing (PT) report through Third-party certified agencies (CERT-In empanelled Security auditors) and Fixing of all identified Vulnerabilities and submission of VAPT reports post fixing of open issues, risk assessment & risk mitigation. It may be noted that ERNET India & CERT-In reserve the right to accept VAPT reports with any selected open issues post the proper risk assessment & their risk mitigation by the contractor.

It may be noted by bidder that VAPT to be done for entire setup. VAPT should be comprehensive but not limited to following activities:

1) Network Scanning, Port scanning, system identification and trusted system scanning, Vulnerability scanning, Malware scanning, Spoofing, Application Security Testing, Access Control Mapping, Cookie Security, DMZ Network architecture review, Firewall rule review, OS Security configuration, Database Security Configuration, any other attacks. Application Security Testing for the software provided by the System Integrator.

2) Network is not fully air gapped and hence External network penetration to test the effectiveness of perimeter security controls and Internal network penetration test to test the effectiveness against the insider threats are in the scope of the bidder.

3) The bidder has also to do the VA & PT for the Solutions including Applications that are procured as part of in this tender.

4) VAPT Plan w.r.t new and existing DC, DR & Remote Locations

Sl. No	**VAPT Scope per Delivery Milestone**	**VAPT milestone(MS)**
1	New DC Infra VAPT to be done within 3 months of issuance of provisional commissioning certificate.	VAPT-MS-1
2	New DR Infra VAPT to be done within 3 months of issuance of provisional commissioning certificate.	VAPT-MS -2
3	Remote Sites VAPT to be done within 3 months of issuance of provisional commissioning certificate.	VAPT-MS-3
4	New DC-DR Infra with remote sites within 12 month from the start of O&M	VAPT-MS -4
5	New DC-DR Infra with remote sites within 24 month from the start of O&M	VAPT-MS-5
6	Existing infra with Remote Sites (within 1 months of start of O&M by this bid’s contractor)	VAPT-MS-6
7	Existing infra with Remote Site (within 12 months of start of O&M by this bid’s contractor)	VAPT-MS-7
8	Existing infra with Remote Site (within 24 months of start of O&M by this bid’s contractor)	VAPT-MS-8

Note 1 :
The installation , commissioning , integration , acceptance testing & start of VAPT testing will be termed as Acceptance. A provisional commissioning certificate(s) will be issued post completion of Acceptance Testing to be used for payment provisions per respective delivery milestones.

Note 2:
Post the Acceptance & VAPT completion – Final Commissioning certificate(s) will be issued for release of payment related with VAPT Completion Milestone(s).

Section III: General Conditions of Contract (GCC) Clause no 10 (6) (c)

Modification in Payment Terms clause #10 “Prices and Payments Terms” Subclause “6 . The payment terms are:”

c. In respect of equipment (s) at DC and DR, additional 25% of the total value of items will be made after issuance of respective provisional commissioning certificate per delivery milestone(s). Remaining 5% of the total value of items per respective delivery milestone will be made after issuance of respective Final Commissioning certificate (i.e. post the acceptance & VAPT completion). Rest other clauses of payment will remain same.

Revised Annexure-1 (Technical Specifications)

Important notes while quoting the equipment(s) in Bid, Bidder shall make sure following:

a. In DC and DR, all Networking equipment(s) should be from same OEM. Name of such equipment(s) are Spine & Leaf Switch, OOB Switch, Interconnect Type1 & Type 2 Switch, Border Leaf Switch, WAN Switch, CE Routers (WAN Router), Internet Router etc.
b. Remote Firewalls should be from Internal Firewall OEM.
c. In each networking and security equipment (firewalls), the transceivers must be of same networking and security equipment (firewalls).
d. Internet and Internal Firewalls at DC should be from different OEMs.
e. Internet and Internal Firewalls at DR should be from different OEMs.
f. Internet, Internal and Solution firewall should not be from offered networking OEM in this bid.
g. SSL VPN OEM should be different from Internet Firewall OEM.
h. All the active equipment(s) must support SNMP V3.
i. Other line items which are more than one in quantity should be from same OEM line item wise.
j. Quoting Multiple OEM for single product is not allowed.
k. In DC and DR, for all Networking equipment(s), all the Subscription licenses and Direct OEM support (24x7 TAC and NBD device replacement) to be provided for asked warranty period. The response time for the high severity TAC cases should not be more than 01 hour. No Partner led TAC Support to be quoted.
l. NBD device replacement / its hardware components replacement services (as applicable) for all equipment sought in the bid is required for continuous operations
m. Only the Manpower on OEM payrolls shall perform network planning, designing, implementation, integration and testing/validation for all Networking equipment(s) i.e. only direct OEM payroll manpower would be allowed to work on the project's designing, implementation & testing phase. An undertaking for same shall be provided.
n. The hardware equipment proposed to be supplied in this bid should be compatible, stackable i.e. rack mountable

inside a standard sized 42-U rack.

o. All the solutions proposed to be supplied with this bid mandatorily should work in as an on-premises solution & not as a cloud based solution.

p. It may be noted by bidder that the required additional resources (any hardware &/or software) to run the solution(s)/equipment(s) should be factored in by bidder and available on Day-1 upon the equipment/solution delivery to support the complete functionality/features sought in the bid. It is understood that proposed hardware would be data centre suitable, rack mountable with redundant power supplies.

q. It may be noted by the bidders that item#59 at PART-C (OPEX) i.e. "Databases GeoIP, VPN Services" are IP address geolocation services & is not a manpower service. The specifications may be referred in Revised Tech Specs.

r. '+' in the technical specifications refers to the minimum specs requirements for the particular item/feature/functionality/spec etc.

s. All the equipment(s) quoted by the bidder should be compatible with proposed intelligent cabling solution.

t. Bidder must go through these above points carefully before going to technical specification in detail for designing their solution.

u. In case of any ambiguity /confusion related to technical specifications in the query response sheet, the revised technical specifications (Revised Annexure I – PartA,B,C) will prevail and in case of administrative part of the tender the revised Annexure B will prevail.

Part A

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	**Storage Server (Category 01)**			
1	Physical dimension	Maximum up to 7U Rack Mountable		
2	Processor	Processor: 2 Quantity (Dual socket) x Intel Xeon Gold/Platinum scalable series 5th Ge**n, 32+ cores/64+ Thread**s (**2.7+** GHz base frequency, Cache Size **60+ MB)** or Processor: 2 Quantity (Dual socket) x A**MD Epyc 9004 or** latest Series, **32+ cores/64+** Threads (2.7+ GHz base frequency, Cache Size **128+ MB)**		
3	Memory	Total 2TB or higher RAM**,** DDR5 5000+ MHz ECC REG DIMM		
4	Boot Storage subsystem	Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS SSD**/M.2 SSD/ M.2 NVME SSD/E3.S NVMe SSDs** Each SSD spec: **960GB+** Capacity, Write Intensive/Mixed Use, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD **IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size**		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	**Storage Server (Category 01)**			
5	Storage	*Each Server With Minimum Storage of 1440 TB,* *With Each HDD spec:* *CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Secure Erase)* Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s ***Note:*** ***1. Single DAS expansion can be used. However, the effective I/O throughput of all the disks combined should not be impacted due to any DAS expansion connector limitations.*** ***2. DAS and Server should be compatible and support of DAS to be provided by Server OEM only. Server OEM shall give undertaking for the support of DAS on their letterhead.***		
6	Interface (NIC)	2x 1G Copper, 2x10G Fiber SFP+ (connectivity support for copper/fiber transceivers), 10G ports should be fully populated with required SR Transceivers (of appropriate OEM Make)		
7	Baseboard management	Baseboard management console with dedicated RJ45 interface , (IPMI)		
8	HW Raid controller	Dedicated Hardware Raid controller= RAID 0,1,5,6,10, 50, 60, SATA/SAS-3 connectivity, 4+ GB cache, battery or flash backed protection for all HDDs.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	**Storage Server (Category 01)**			
		All the HDDs in the server should be configurable under a single virtual drive with RAID 5,6,50,60. Storage management including raid configuration. Required support for SED (Self Encrypting Drive) and ISE (Instant Secure Erase) should be available in RAID controller.		
9	***Power Supply***	***Redundant, maximum rated power up to 3000 W***		
10	Accessories	Rails kit for rack mounting, power cables and server tag.		
11	General Features	**Certification**: Windows, Red Hat Linux, SUSE Linux, Ubuntu from the respective Server Operating System OEMs. Certification (Virtualization/Cloud Platform): Microsoft Hyper V, VM Ware, Red Hat Open Shift from the respective Hypervisor OEMs. **Power Supply Efficiency**: Platinum/Titanium or higher. Storage (HDD) Drives: Instant Secure Erase, Self-Encrypting (SED). Required support should be available in RAID controller		
12	Cache Drive (For 50 servers)	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe/E3.S NVMe Sequential read 6,200 MB/s, Sequential write 2,600 MB/s (Sequential performance 128KB block size with queue depth 32) Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1) Endurance 3 DWPD with additional 2 free slots for populating additional cache drives.		
13	Feature Support	All the features mentioned above should be available from day one		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
2	**Application Server (Category 02)**			
1	Physical dimension	Maximum up to 2U Rack Mountable		
2	Processor	2 Quantity (Dual socket) x Intel Xeon Gold/Platinum scalable series 5th Gen, 28+ cores (2.7+ GHz base frequency, Cache Size 60+ MB) OR 2 Quantity (Dual socket) x AMD Epyc 9004 or latest , 28+ cores (2.7+ GHz base frequency, Cache Size 128+ MB)		
3	Memory	Total 1 TB (16x 64GB), DDR5 5000+ Mhz ECC REG DIMM		
4	Boot Storage subsystem	Boot Storage subsystem with HW RAID 1 having 2 nos x Enterprise SAS SSD/M.2 SSD/M.2 NVME SSD/E3.S NVMe SSDs Each SSD spec: 960GB+ Capacity , Write Intensive/Mixed Use, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size		
5	Storage	*Each Server With Minimum Storage of 200 TB,* *With Each HDD spec:* *CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours), SED (Self encrypting drive) with ISE(Instant Secure Erase)* Avg latency : between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
2	**Application Server (Category 02)**			
6	Interface (NIC)	2x 1G Copper, 2x10G Fiber SFP+ (connectivity support for copper/fiber transceivers), 10G ports should be fully populated with required SR Transceivers (of appropriate OEM Make)		
7	Baseboard management	Baseboard management console with dedicated RJ45 interface , (IPMI)		
8	HW Raid controller	Dedicated Hardware Raid controller= RAID 0, 1, 5, 6, 10, 50, 60, SATA/SAS-3 connectivity, 4+ GB cache, battery or flash backed protection for all HDDs. All the HDDs in the server should be configurable under a single virtual drive with RAID 5, 6, 50, 60 Storage management including raid configuration. Required support for SED (Self Encrypting Drive) and ISE (Instant Secure Erase) should be available in RAID controller.		
9	***Power Supply***	***Redundant, maximum rated power upto 1600 W***		
10	Accessories	Rails kit for rack mounting, power cables and server tag .		
11	General Features	**Certification:** Windows, Red Hat Linux, SUSE Linux, Ubuntu from the respective Server Operating System OEMs. Certification (Virtualization/Cloud Platform): Microsoft Hyper V, VM Ware, Red Hat OpenShift from the respective Hypervisor OEMs. **Power Supply Efficiency**: Platinum/Titanium or higher. Storage (HDD) Drives: Instant Secure Erase, Self-Encrypting (SED). Required support should be available in RAID controller		
12	Feature Support	All the features mentioned above should be available from day one		
13	Cache Drive	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x8/Gen4 x4 U.2, NVMe/E3.S NVMe Sequential read 6,200 MB/s, Sequential write 2,600 MB/s (Sequential performance 128KB block size with queue depth 32) Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS (Random Performance 4K block size with queue depth 256)		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
2	**Application Server (Category 02)**			
		Latency, read/write 120/20 µs (4KB transfer size with queue depth 1)		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
3	**Web Server (Category 03)**			
1	Physical dimension	Maximum up to 2U Rack Mountable		
2	Processor	Processor: 2 Quantity (Dual socket) x Intel Xeon Gold/Platinum scalable series 5th Gen 8 core processor (3+ GHz base frequency, Cache Size 20+ MB) OR Processor: 2 Quantity (Dual socket) x AMD Epyc 9004 or latest Series, 8 core processor (3+ GHz base frequency, Cache Size 64+ MB)		
3	Memory	Total 32GB, (2nos x 16GB),DDR5 5000+ MHz ECC REG DIMM		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
3	**Web Server (Category 03)**			
4	Boot Storage subsystem	Boot Storage subsystem with HW RAID 1 having 2 no:s x Enterprise SAS SSD/M.2 NVME SSD /M.2 SSD/**E3.S NVMe SSDs**, Each SSD spec: 400GB+ Capacity, Write Intensive/Mixed Use, Read (1+ GB/s) Write (500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size		
5	Storage	Storage: 2 nos x 18+ TB Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12+ Gb/s, 7200+ RPM, 256+ MB Cache, 3.5", MTBF = 8+ Lakhs hours) *SED (Self encrypting drive) with ISE(Instant Secure Erase)* Avg latency: between 4 to 10 ms, Random R/W IOPS (at 4KB, QD16): 150+/300+ Sequential R/W speed for 64 KB blocks: 120+ MB/s		
6	Interface (NIC)	4x 1G Copper, 2x10G Fiber SFP+ (connectivity support for copper/fiber transceivers), 10G ports should be fully populated with required SR Transceivers (of appropriate OEM Make)		
7	Baseboard management	Baseboard management console with dedicated RJ45 interface , (IPMI)		
8	HW Raid controller	Dedicated Hardware Raid controller = RAID 0, 1, 5, 6, 10, 50, 60, SATA/SAS-3 connectivity, 4+ GB cache, battery or flash backed protection for all HDDs. All the HDDs in the server should be configurable under a single virtual drive with RAID 5, 6, 50, 60 Storage management including raid configuration. Required support for SED (Self Encrypting Drive) and ISE (Instant Secure Erase) should be available in RAID controller.		
9	***Power Supply***	***Redundant, maximum rated power upto 1600 W***		
10	Accessories	Rails kit for rack mounting, power cables and server tag.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
3	**Web Server (Category 03)**			
11	General Features	**Certification: Windows**: Red Hat Linux, SUSE Linux, Ubuntu from the respective Server Operating System OEMs. Certification (Virtualization/Cloud Platform): Microsoft Hyper V, VM Ware, Red Hat Open Shift from the respective Hypervisor OEMs. **Power Supply Efficiency:** Platinum/Titanium or higher. Storage (HDD) Drives: Instant Secure Erase, Self-Encrypting (SED). Required support should be available in RAID controller		
12	Feature Support	All the features mentioned above should be available from day one		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
4	**Load Balancer Server (Category 04)**			
1	Physical dimension	Maximum up to 2U Rack Mountable		

S. No.	**Description**	**Specification**	**Marked/ Highlighted Cross Reference of Specification with reference page no.**	**Compliance (Yes/No)**
4	**Load Balancer Server (Category 04)**			
2	Processor	2 Quantity (Dual socket) x Intel Xeon Gold/Platinum scalable series 5th Gen, 24+ cores (2.7+ GHz base frequency, Cache Size 30+ MB) OR 2 Quantity (Dual socket) x AMD Epyc 9004 or latest , 24+ cores (2.7+ GHz base frequency, Cache Size 128+ MB)		
3	Memory	Total 1 TB (16 x 64 GB), DDR5 5000+ MHz ECC REG DIMM		
4	Boot Storage subsystem	Boot Storage subsystem with HW RAID 1 having 2 no:s x Enterprise SAS SSD/M.2 SSD/M.2 NVME SSD/**E3.S NVMe SSDs**, Each SSD spec: 400GB+ Capacity , Write Intensive/Mixed Use, Read (1+ GB/s) Write(500+ MB/s), MTBF = 2+ million hours, 2000+ TBW, 2+ DWPD IOPS: Each SSD should have 150K+/100K+ Random Read/Write IOPS at 4K block size		
5	***Interface (NIC)***	***4x 1G Copper, 2x10G Fiber SFP+ (connectivity support for copper/fiber transceivers), 10G ports should be fully populated with required SR Transceivers (of appropriate OEM Make), 2 no:s x dual 100G QSFP28 , PCIe 4.0 (NIC: Dual port 100G. Mellanox MCX516A-CDAT ConnectX-5 Ex/ Intel E810 2CQDA2/NVIDIA Mellanox MCX613106A-VDAT ConnectX-6/NVIDIA Mellanox MCX623106AN-CDAT ConnectX-6 Dx EN)***		
6	Baseboard management	Baseboard management console with dedicated RJ45 interface , (IPMI)		
7	Power Supply rated	Redundant, 1600 W		
8	Accessories	Rails kit for rack mounting, power cables and server tag.		
9	General Features for Server	Certification (OS): Windows, Red Hat Linux, SUSE Linux, Ubuntu. Certification (Virtualization/Cloud Platform): VM Ware, Red Hat Open Shift. Power Supply Efficiency: Platinum/Titanium or higher.		
10	Feature Support	All the features mentioned above should be available from day one		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
4	**Load Balancer Server (Category 04)**			
11	Cache Drive	Enterprise NVMe drive for caching: Capacity: 2x 3.2 TB, PCI Express Gen4 x4 U.2, NVMe/E3.S NVMe Sequential read 6,200 MB/s Sequential write 2,600 MB/s (Sequential performance 128KB block size with queue depth 32) Random read (4K) Up to 1,000K IOPS, Random write (4K) Up to 180K IOPS (Random Performance 4K block size with queue depth 256) Latency, read/write 120/20 µs (4KB transfer size with queue depth 1) Endurance 3 DWPD.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
5	**Utility Server (Category 05)**			
1	Physical dimension	2U Rack Mountable		
2	Processor	2 Quantity (Dual socket) x Intel Xeon Gold/Platinum scalable series 5th Gen, 32 or more cores (2.4 GHz or more base frequency. Cache Sze 60 MB or more) OR 2 Quantity (Dual socket) x AMD Epyc 9004 or latest Series, 32 or more cores (2.4 GHz or more base frequency Cache Size 60 MB or more)		
3	Memory	Total 512 GB, DDR5 4400 MHz ECC REG DIMM		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
5	**Utility Server (Category 05)**			
4	Boot Storage	Boot Storage subsystem with HW RAID 1 having 2 no:s x Enterprise SAS/M.2 SSD/M.2 NVMe SSD/E3.S NVMe SSD, Each SSD spec: 960GB or more Capacity , Write Intensive/Mixed Use, Read (1 GB/s or more) Write (500 MB/s or more), MTBF = 2 million hours or more, 2000 TBW or more, 2 DWPD or more		
5	Storage	Storage: 6 or more no:s x 8 TB or more Enterprise Drives, (Each HDD spec: CMR Technology, SAS 12 Gb/s, 7200 RPM, 256 MB Cache. 3.5°, MTBF = 8 Lakhs hours) System must have atleast 12 x LFF front accessible Hot-Swap Drive Bays with backplane supporting SAS/SATA/NVMe drives		
6	Interface (NIC)	2x 1G, 2x10G SFP+ Ethernet (connectivity support for copper/fiber transceivers)		
7	PCIe	All PCIe slots must support Gen 4/5 speed and supporting (X8/X16 and FH/ LP) or supporting 10.5" Length based Controllers.		
8	Baseboard management	Baseboard management console with dedicated RJ45 interface , (IPMI)		
9	HW Raid controller	Hardware Raid controller= RAID 0,1,5,6,10, 50, 60, SATA/SAS-3 connectivity, 4 GB or more cache, battery or flash backed protection, for the 4 or more no:s of HDDs		
10	NVMe drive for caching	3.2 TB Enterprise NVMe drive for caching		
11	Redundant Power supply	1500W W or less		
12	OS	Certified for RedHat, Ubuntu, Windows		
13	Accessories	Rails kit for rack mount		
14	Virtualization Stack	Enterprise virtualization software license for the system for asked cores to be supplied with the system. System offered must be certified with offered virtualization software, certificate must be submitted with technical bid		
15	Description	Specifications		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
5	**Utility Server (Category 05)**			
16	General Compliances	UEFI Specification v2.7 or above , SMBIOS Specification v3.3 or above , ACPI Specification v6.4 or above , PMBUs Specification v1.2 or equivalent technology , Redfish API , Advanced Encryption standard (AES) , SNMP v3 , TLS 1.2 or above , Active Directory v1.0. Manufactured in accordance with the international quality standards ISO 9001:2015 Compliance to Safety of IT Equipment: BIS / IEC 62368 Standards for EMC (Electro Magnetic Compatibility) Standards: EN 55035 Class A RoHS : EN IEC 63000		
17	General features	Power Supply Efficiency: Platinum or Higher Storage (HDD) Drives: Instant Secure Erase, Self-Encrypting (SED). Required support should be available in RAID controller		

Common Management & Security features for all above servers				
1	Management Features	1. Remoter power on/ shutdown of server 2. Remote Management of server over LAN & WAN with SSL encryption through gigabit management port 3. Should have virtual Media support with all required licenses 4. Remote KVM 5. Real-time monitoring and alerting of several parameters like: a. Health monitoring of CPU, GPU, Storage, Memory, RAID, NIC, etc. b. Power and thermal monitoring c. SSD wear monitoring/SSD impending and active failure alerts d. Disk SMART data		

Common Management & Security features for all above servers

		e. Multiple components voltage readings (e.g. CPU, system board, PSU, etc.) 6. Telemetry streaming using: a. RSYSLOG b. Redfish c. SNMP, etc. 7. Logging of health and system events 8. Secure component verification and alerting/ Platform Integrity Check		
		9. Secure management with configuration of HTTPS, LDAP/radius, NTP for time sync, SNMP, API based management support, along with support of Redfish, IPMI etc. 10. HTML 5 based virtual console 11. Remote Firmware, bios and driver update 12. Dedicate Ethernet port and OOB baseboard management controller with support for IPv4, IPv6 and DHCP 13. Inventory Export 14. In-built diagnostic tool for troubleshooting 15. Browser-based and command-line interface for managing and monitoring the server hardware. 16. Out of band web management should support automatic/manual backup system configuration settings (BIOS, IPMI, NIC) for restoration of configuration. 17. Storage management including raid configuration 18. All Hardware and Licenses for management features to be provided by bidder without additional cost.		
2	Security Features	1. Secure Boot (Firmware and Bios Level Security) 2. Shall provide dual immutable silicon root of trust to verify the integrity of BIOS and the BMC Firmware Image while booting 3. Server should provide server intrusion detection (even in power-off state) 4. Malicious Code Free design (to be certified by OEM) 5. Role based access 6. ACL based on IP address and Port		

Common Management & Security features for all above servers

		7. Cryptographic firmware updates/ Signed firmware updates / secure firmware updates by server OEM 8. Secure /Automatic BIOS recovery 9. In case of any security breach system should provide features for prevention of security breaches or lockdown on security breaches. 10. Embedded/Integrated TPM 2.0 11. Server OEM should follow NIST SP 800-193 ("Platform Firmware Resiliency") , NIST SP 800-147B (“BIOS Protection Guidelines for Servers”) 12. Should be able to verify BIOS integrity and authenticity from malicious firmware and support automatic BIOS recovery if BIOS is corrupted		
		13. Out of band web management shall provide dynamic USB enable / disable ability 14.A firmware anti-rollback protection to prevent from replacing newer firmware with an older firmware image		
3	General Note	1. Bidder shall supply required quantity of fiber patch chords (Single mode/ Multimode), patch chord as per site requirements. 2. All accessories for successful installation in rack should be supplied by Bidder. 3. Supplied equipment must be mountable on 19-inch rack. 4. The device should have front to back airflow with efficient cooling mechanism. 5. All the features mentioned above should be available from day one. 6. All the server should fully populated with their SFPs		
4	Industry Standard Compliance for Servers	UEFI Specification, v2.7 or above, SMBIOS Specification, v3.3.0 or above, ACPI Specification, v6.4 or above, PMBus Specification, v1.2 or above, NVMe Express Base Specification, v2.0c or above, USB SuperSpeed v3.0, Redfish API, Advanced Encryption Standard (AES), SNMP v3, TLS 1.2 or above, DMTF Systems Management Architecture for Server Hardware Command Line Protocol (SMASH CLP), Active Directory v1.0 Manufactured with quality standards ISO 9001:2015, Compliance to Safety of IT Equipment : IEC 62368, Standards for EMC (Electro Magnetic Compatibility) : EN 55035 Class A and RoHS: EN IEC 63000		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
6	**GPU Servers**			
1	Processor Make	Intel or AMD latest Gen		
2	Processor Description	Processor: 2 Quantity (Dual socket) x Intel Platinum scalable series 5th Ge**n, 48+ cores/96+ Thread**s (**2.1+** GHz base frequency, Cache Size **260+ MB)** or Processor: 2 Quantity (Dual socket) x A**MD Epyc 9004 or** latest Series, **48+ cores/96+** Threads (2.1+ GHz base frequency, Cache Size **256+ MB)**		
3	Motherboard	Chipset should be certified for the quoted Processor		
4	GPU	AMD MI300x (8 No.s configured with AMD Infinity Fabric Link with minimum 896GB/s bidirectional bandwidth) / NVIDIA HGX H200 Tensor Core GPU (8 Nos. in 141+GB 700W SXM5 configuration with minimum 900GB/s bidirectional communication bandwidth configuration)		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
6	**GPU Servers**			
5	Performance	500TF or Higher Double Precision Tensor FP64 / TF64 Performance, 28 PetaFlops or Higher FP8 performance with sparsity.		
6	Multi Instance GPU	Single GPU can be partitioned into as many as 7 GPU instances		
7	Internal Switches	NVLink / Infinity Fabric™ Links for facilitating direct communication between GPUs connectivity.		
8	System Memory	3TB memory using DDR5 (4800 MHz or higher) operating at min. 4400MHz Server should be populated in balanced memory configuration.		
9	GPU Memory	Minimum 141 GB or more per GPU 1100GB Per node minimum memory		
10	Networking	Four OSFP ports serving eight single- port NVIDIA ConnectX-7 VPI or 8* Single port with required Transceivers & Cables and two dual-port NVIDIA ConnectX-7 VPI or 2* Dual Port 100G with required Transceivers & Cables		
11	Interfaces	3*USB 2.0/3.0 or higher Ports 1*VGA Ports		
12	Bus Slots	10 PCI-Express 5.0 slots x16 PCIe slots.		
13	Internal Storage	4 x 1.92TB NVMe Gen 4 or Higher		
14	Power Supply	Should be populated with 6 x Hot-plug redundant 2800 W AC Power Supply or higher		
15	Fans	Redundant hot-plug system fans		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
6	**GPU Servers**			
16	Form Factor	8U or Lower; Rack Mountable with Air Cooled Chassis or Direct Liquid Cooled Any infra required for the same will need to be factored by the Bidder/OEM		
17	AI, HPC Software Containers and Required DL SDKs	AMD RoCM / Nvidia NGC (Nvidia GPU Cloud) containers should be provided. Some of the basic, SDK/library/containers we will use in the system: CUDA toolkit, CUDA tuned Neural Network (cuDNN) Primitives TensorRT Inference Engine CUDA tuned BLAS (cuBLAS) CUDA tuned Sparse Matrix Operations (cuSPARSE) Multi-GPU Communications (NCCL) Industry SDKs – NVIDIA Merlin, DeepStream, ISAAC, Nemo, Morpheus Or corresponding/required Software Stack from the other GPU OEM. Central app manager for HPC/AI applications, must provide below: Optimized Code Repositories for - CPU Optimizations: - Code libraries and binaries with optimization for: - AVX-512: 512-bit Advanced Vector Extensions. - SSE: Streaming SIMD Extensions. for allowing the manager to handle optimized binaries for specific CPU architectures to maximize performance. - GPU Optimizations: - Dedicated repositories for GPU-optimized applications, supporting: - Hopper (H100) / Mi300x for advanced AI and deep learning optimizations. - Each GPU optimization should be able to select the best-fit kernel and configuration based on the architecture detected at runtime.		
18	Miscellaneous	Software suites to be loaded as part of installation process by bidder. All required cables, connectors and harnesses should be provided.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
7	**Monitoring and Management Tool for Servers**			
1		The solution should be deployed at DC and DR working in HA and supplied with all the associated hardware		
2		Access device-level lifecycle management with a single click—no need to navigate among appliances with license to add up to 4000 servers		
3		User defined policy/ template based automated and simultaneous operations like: - OS deployment - Firmware update - BIOS update - Server cloning - Creation of Virtual disks along with RAID configuration - Network configuration - Web server and SSH and configuration - Secure erase of storage drives		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
7	**Monitoring and Management Tool for Servers**			
4		Redfish, Restful API support for automated management		
5		Real-time monitoring, logging and alerting of several parameters like: a. Health monitoring of CPU, GPU, Storage, Memory, RAID, NIC, etc. b. Power and thermal monitoring c. SSD wear monitoring /SSD impending and active failure alerts d. Disk SMART data e. Multiple components voltage readings (e.g. CPU, system board, PSU, etc.) f. Intrusion		
6		Integrated reporting to see server hardware & firmware inventory (of all hardware and software components), including associated firmware versions along with option to create customized reports		
7		Fault management: Get monitoring, pre-failure alerts, failure alerts, log (system events, lifecycle, troubleshooting, user session, etc.) monitoring & extraction, automatic call logging (configurable), status monitoring of trouble ticket and contract/warranty registration & display for each device		
8		Should have management features like: - Power management and configuration - Virtual Console with management features like boot selection, power on/off, Virtual media, Virtual clipboard, etc. without the need to login to respective server IPMI - Asset Tracking - Server profile import/export - Role based user management with feature for integration with LDAP(AD),AAA - Time-zone/NTP		
9		Blink LED to identify a particular server		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
7	**Monitoring and Management Tool for Servers**			
10		Software and Hardware for this Monitoring and management tool for servers shall be provided by the OEM of severs.		
11		All the features asked should be available from day one		
12		i. Management of multiple servers from single console with single source of truth for multiple sites. ii. Automated infrastructure management for patch upgrades, version upgrades, etc. iii. Simplified management with analytics driven actionable intelligence iv. System tagging giving admin flexibility to provide metadata tags to each system to enable users to filter and sort systems based on user assigned attributes Or the management console should be enabled with Elastic search feature capable of accessing all information within the console v. Hardware Profile based deployment to multiple servers simultaneously vi. Policy template for deployment of single policy to multiple servers simultaneously vii. Platform inventory and health status, server utilization statistics collection (including firmware updates and diagnostic tools) viii. Should provide an alert in case the system is not part of OEM hardware compatibility test ix. Should have customizable dashboard to show overall faults/health/inventory for all managed infrastructure the solution should provide option to create unique dashboards for individual users. the user should be flexibility to select name for dashboards and widgets		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
7	**Monitoring and Management Tool for Servers**			
		(viz. health, utilization etc.), x. Real-time out-of-band hardware performance monitoring & alerting		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
8	**SFP- 1 G (SR) for Servers**			
1	Type of Transceiver	SFP 1GBase-SR Transceivers		
2	SFP Mode	Multi		
3	Compatibility with OEMs Products	All		
4	Fibre Cable Type	MMF		
5	Maximum Data Rate	1Gbps		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
9	**SFP-10G (SR) for Servers**			
1	Type of Transceiver	SFP+10GBase-SRTransceivers		
2	SFP Mode	Multi		
3	Compatibility with OEMs Products	All		
4	Fibre Cable Type	MMF		
5	Maximum Data Rate	10 Gbps		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
10	**Spine Switch for DC**			
1	Type of Core Switch	Chassis Based		
2	Number of Interface Slots	4 or higher		
3	Number of Fabric Slots	No. of Fabric slots: minimum 4. All slots should be fully populated from day 1.		
4	Number of Routing engines/ Supervisor Modules	2 or higher		
5	No. of FAN Tray	2 or higher		
6	Support for 100G QSFP28 Port	Yes		
7	Number of 100G QSFP28 Port	min. 250 or more without breakout. All the slots and ports should be fully populated with QSFP optics on day-1.		
8	Switching Capacity (Gbps)	50000 or higher (No oversubscription between front panel ports and backend fabric cards)		
9	a. Advance Layer-3 Protocol	EVPN+VXLAN (No proprietary protocols to be deployed for leaf-spine fabric), ESI LAG / Layer3 port channels or equivalent technology. Should support EVPN Route Types (Type-1, Type-2, Type-3, Type-4, Type-5,), Tenant routed Multicast / OISM, OSPF/ISIS, BGP		
10	b. Security Feature	Port, VLAN & Routed ACL,9K or higher ACL Entries/group based-segmentation-entries, GRE (Must Support 1000 or Higher GRE Tunnels or 1000 VXLAN Tunnels)		
11	c. Management Protocol	Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sFlow/Netflow, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN/ERSPAN, telemetry, buffer queue depth monitoring/QOS for prioritizing the traffic during congestion with minimum 8 queue per port, Same OS across all the proposed network switches for simplified operations.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
10	**Spine Switch for DC**			
12	d. QoS	Virtual output Queue VoQ)/Egress QoS/Intelligent Buffer/dynamic buffer, WRED,PFC/ECN,PTP, 8GB Packet Buffer per line card or equivalent,8 queues/port, WRR		
13	Other Features	Should support 250K IPv4 Routes, 125K IPv6 Routes, 32K IPv4,8K IPv6 Multicast Routes.		
14	Redundant Power Supply	Internal Redundant Power Supply for fully loaded chassis from day 1		
15	Redundant FAN	Redundant FAN for fully loaded chassis from day 1		
16	Feature Support	Device, OS, Optics, Manager from same OEM. Should be managed through unified Network Manager.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
11	**Spine Switch for DR**			
1	Type of Core Switch	Chassis Based		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
11	**Spine Switch for DR**			
2	Number of Interface Slots	4 or higher		
3	Number of Fabric Slots	No. of Fabric slots: minimum 4. All slots should be fully populated from day 1.		
4	Number of Routing engines/ Supervisor Modules	2 or higher		
5	No. of FAN Tray	2 or higher		
6	Support for 100G QSFP28 Port	Yes		
7	Number of 100G QSFP28 Port	min. 140 or more without breakout. All the slots and ports should be fully populated with QSFP optics on day-1.		
8	Switching Capacity (Gbps)	28000 or higher (No oversubscription between front panel ports and backend fabric cards)		
9	a. Advance Layer-3 Protocol	EVPN+VXLAN (No proprietary protocols to be deployed for leaf-spine fabric), ESI LAG/Layer3 port channels or equivalent technology. Should support EVPN Route Types (Type-1, Type-2, Type-3, Type-4, Type-5), Tenant routed Multicast / OISM, OSPF/ISIS, BGP		
10	b. Security Feature	Port, VLAN & Routed ACL,9K ACL or higher Entries/group based-segmentation-entries, GRE (Must Support 1000 or Higher GRE Tunnels or 1000 VXLAN Tunnels)		
11	c. Management Protocol	Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sFlow/Netflow, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN/ERSPAN, telemetry, buffer queue depth monitoring/QOS for prioritizing the traffic during congestion with minimum 8 queue per port, Same OS across all the proposed network switches for simplified operations.		
12	d. QoS	Virtual output Queue VoQ)/Egress QoS/Intelligent Buffer/dynamic buffer, WRED,PFC/ECN,LLQ,PTP, 8GB Buffer per line card or equivalent, ,8 queues/port, WRR		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
11	**Spine Switch for DR**			
13	Other Features	Should support 250K IPv4 Routes, 125K IPv6 Routes, 32K IPv4, 8K IPv6Multicast Routes.		
14	Redundant Power Supply	Internal Redundant Power Supply for fully loaded chassis from day 1		
15	Redundant FAN	Redundant FAN for fully loaded chassis from day 1l		
16	Feature Support	Device, OS, Optics, Manager from same OEM. Should be managed through unified Network Manager.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
12	**Leaf Switch**			
1	No of SFP/ SFP+ Ports	Minimum 24 Nos		
2	Type of SFP Port	10G		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
12	**Leaf Switch**			
3	Support for 100GQ SFP+ Port (Uplink)	Yes		
4	No .of 100G QSFP+ Port	4 or higher		
5	Switching Capacity (Non-Blocking) (Gbps)	1280 or higher		
6	a. Advance Layer-3 Protocol	EVPN+VXLAN (No proprietary protocols to be deployed for leaf-spine fabric), ESI LAG or equivalent technology. Should support EVPN Route Types (Type-1, Type-2, Type-3, Type-4, Type-5), Tenant routed Multicast / OISM, OSPF, ISIS, BGP		
7	b. Security Feature	Port, VLAN & Routed ACL, 1500 Ingress /1500 Egress ACL Entries/Group-based micro-segmentation, 802.1x.		
8	c. Management Protocol	Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX, PTP, OpenConfig, Filtered packet mirroring over GRE/SPAN/ERSPAN, telemetry , buffer queue depth monitoring/QOS for prioritizing the traffic during congestion with minimum 8 queue per por, Same OS across all the proposed network switches for simplified operations.		
9	d. QoS	WRED, SPQ, SDWRR/WRR, , , 802.1Qbb PFC and ECN, 8queues/port, Remarking of bridged packets		
10	Other Features	Should support 250K IPv4 LPM Routes, 125K IPv6 LPM Routes, 100K IPv4/v6 Multicast Routes.		
11	Redundant Power Supply	Internal Redundant Power Supply for fully loaded chassis from day 1		
12	Redundant FAN	Redundant FAN for complete Chassis from day 1		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
12	**Leaf Switch**			
13	Feature Support	Device, OS, Optics, Manager from same OEM. Should be managed through unified Network Manager.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
13	**Border Leaf Switch**			
1	Type Of Core Switch	Chassis Based/Non-Chassis Based		
2	Support for 100G QSFP+ Port	Yes		
3	No. of Ports	Should have minimum 24Nos of 100G QSFP28 Ports and fully populated from day-1		
4	Switching Capacity (Gbps)	4800 Or higher		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
13	**Border Leaf Switch**			
5	a. Advance Layer-3 Protocol	EVPN+VXLAN (No proprietary protocols to be deployed for leaf-spine fabric), ESI LAG or equivalent technology. Should support EVPN Route Types (Type-1, Type-2, Type-3, Type-4, Type-5), Tenant routed Multicast / OISM, OSPF, ISIS, BGP		
6	b. Security Feature	Port, VLAN & Routed ACL. Should support minimum 14K ACL entries/terms or minimum 32K prefix/host entries for traffic segmentation.		
7	c. Management Protocol	Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX, PTP, OpenConfig, Filtered packet mirroring over GRE/span/ERSPAN, telemetry , buffer queue depth monitoring/QOS for prioritizing the traffic during congestion with minimum 8 queue per port, Same OS across all the proposed network switches for simplified operations.		
8	d. QoS	WRED, SPQ, SDWRR/WRR, Virtual output Queue/dynamic/intelligent buffer, 2 GB Packet Buffer, 802.1Qbb PFC and ECN, 8queues/port, Remarking of bridged packets		
9	Other features	Switch should support all functions required to operate as a Border Leaf Switch providing DC Gateway, Service Chaining and Data centre Interconnect (DCI) using EVPN type-5 routes. Should support 250K IPv4 Routes,150K IPv6 Routes, 64K Multicast Route		
10	Redundant Power Supply	Internal Redundant Power Supply fully loaded day 1		
11	Redundant FAN	Redundant FAN fully loaded from day 1		
12	Feature Support	Device, OS, Optics, Manager from same OEM. Should be managed through unified Network Manager.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
14	**OOB Core Switch for DC**			
1	Type of Core Switch	Chassis Based/Non Chassis Based		
2	No. of interface slots/line cards	3 or higher		
3	No of 10G SFP/SFP+ Ports	Minimum 110 Nos (Without breakout or Stacking). Fully Populated from Day-1		
4	Type of SFP Port	10G		
5	Support for 100GQSFP+ Port (Uplink)	Yes		
6	No .of 100G QSFP+ Port	12 or higher ; Fully Populated from Day-1		
7	Switching Capacity (Non-Blocking) (Gbps)	4600 or higher		
8	a. Advance Layer-3 Protocol	EVPN+VXLAN (No proprietary protocols to be deployed for leaf-spine fabric), ESI LAG or equivalent technology. Should support EVPN Route Types (Type-1, Type-2, Type-3, Type-4, Type-5), Tenant routed Multicast / OISM, OSPF, ISIS, BGP		
9	b. Security Feature	Port, VLAN & Routed ACL, 1500 Ingress /1500 Egress ACL Entries/ Group-based micro-segmentation.		
10	c. Management Protocol	Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/Netflow/sFlow, OpenConfig, Filtered packet mirroring over GRE/SPAN/ERSPAN, Same OS across all the proposed network switches for simplified operations.		
11	d.QoS	WRED,SPQ, SDWRR / WRR, 32MB Buffer, 8queues / port, PFC and ECN		
12	Redundant Power Supply	Internal Redundant Power Supply fully loaded from day 1		
13	Redundant FAN	Redundant FAN fully loaded from day 1		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
14	**OOB Core Switch for DC**			
14	Feature Support	Device, OS, Optics, Manager from same OEM. Should be managed through unified Network Manager.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
15	**OOB Core Switch for DR**			
1	Type of Core Switch	Chassis Based/Non Chassis Based		
2	No. of interface slots/line cards	0 or higher		
3	No of 10G SFP/SFP+ Ports	Minimum 60 Nos (Without breakout or Stacking) ; Fully Populated from Day-1		
4	Type of SFP Port	10G		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
15	**OOB Core Switch for DR**			
5	Support for 100GQSFP+ Port (Uplink)	Yes		
6	No .of 100G QSFP+ Port	8 or higher ; Fully Populated from Day-1		
7	Switching Capacity (Non-Blocking) (Gbps)	2800 or higher		
8	a. Advance Layer-3 Protocol	EVPN-VXLANESI-LAG or equivalent (No proprietary solutions are to be deployed), OSPF, ISIS and BGP		
9	b. Security Feature	Port, VLAN & Routed ACL, 1500 Ingress /1500 Egress ACL Entries/ Group-based micro-segmentation, 802.1x.		
10	c. Management Protocol	Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/Netflow/sFlow, OpenConfig, Filtered packet mirroring over GRE/Span/ERSPAN, Same OS across all the proposed network switches for simplified operations.		
11	d.QoS	WRED,SPQ, SDWRR / WRR, 32MB Buffer, 8queues / port, PFC and ECN		
12	Redundant Power Supply	Internal Redundant Power Supply fully loaded from day 1		
13	Redundant FAN	Redundant FAN fully loaded from day 1		
14	Feature Support	Device, OS, Optics, Manager from same OEM. Should be managed through unified Network Manager.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
16	**OOB Access Switch**			
1	Type of Core Switch	Chassis Based/Non-Chassis Based		
2	Number of 1000Base-T Ports	24 or higher		
3	Number of 10G SFP+ Port(Uplink)	2 or higher Fully Populated from Day-1		
4	Switching Capacity / Forwarding Bandwidth (Non-Blocking) (Gbps)	128 or higher		
5	Number of active VLAN Supported	500		
6	Layer2 Protocols	802.1QVLAN, LAG, LACP, STP, MSTP, RSTP, IEEE802.3x, VLAN, 32K MAC Address.		
7	Basic Layer-3 Protocol from day1	Static Routing		
8	Advance Layer-3Protocol support	8K IPv4 LPM routes, OSPFv2, OSPFv3, ISIS, BGP		
9	Premium Layer-3 Protocol support	VRF Lite/VRF/VRRP, EVPN		
10	Security Feature	RA Guard or equivalent, DHCP Snooping, Dynamic ARP Inspection (or similar security feature which validates ARP packets and prevents attacks like ARP cache poisoning or Similar, Control Plane Policing.		
11	Management Protocol	GUI/Web, CLI, Telnet, TFTP, SMPv1, SNMPv2/V2C, SNMPv3, NTP, RMON, SSHv2, IP Based Management, IPFIX/Netflow/sFlow, OpenConfig, filtered packet mirroring over GRE/SPAN/ERSPAN, Same OS across all the proposed network switches for simplified operations.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
16	**OOB Access Switch**			
12	QoS	802.1p,SP,Queues per port, WRED /WTD, Sflow/Netflow, Shaping, Policing/Rate Limiting, Strict Priority Queueing or Low Latency Queueing, ECN and PFC/802.3x		
13	Redundant Power Supply	Internal Redundant Power Supply fully loaded day 1		
14	Redundant FAN	Redundant FAN fully loaded from day 1 **(Airflow: Front to Back)**		
15	Feature Support	Device, OS, Optics, Manager from same OEM. Should be managed through unified Network Manager.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
17	**Remote Site Switch**			
1	Type of Core Switch	Chassis Based/Non-Chassis Based		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
17	**Remote Site Switch**			
2	Total Port Requirement	16		
3	No of 1G/10G SFP/SFP+ Ports	12 Nos (Without breakout or Stacking); Fully Populated from Day-1		
4	Type of SFP Port	10G		
5	Support for 25G SFP Port	Yes		
6	No of 25G SFP Ports	4 Nos (Without breakout or Stacking); Fully Populated from Day-1		
7	Switching Capacity (Non-Blocking) (Gbps)	440 or higher		
8	a. Advance Layer-3 Protocol	EVPN-VXLANESI-LAG or equivalent VXLAN-EVPN LAG/Multi homing (No proprietary solutions are to be deployed), OSPF, ISIS and BGP		
9	b. Security Feature	Port, VLAN & Routed ACL,1500 Ingress/1500 Egress ACL Entries, 802.1x, MAC 100 K		
10	c. Management Protocol	Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sflow/netflow, OpenConfig, Filtered packet mirroring over GRE/SPAN/ERSPAN		
11	d.QoS	WRED,SPQ, SDWRR / WRR, 32MB Buffer, 8queues / port, ECN and PFC/802.3x		
12	Redundant Power Supply	Internal Redundant Power Supply fully loaded from day 1		
13	Redundant FAN	Redundant FAN fully loaded from day 1		
14	Feature Support	Device, OS, Optics, from same OEM.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
18	**Interconnect Switch - Type 1**			
1	Type of Core Switch	Chassis Based/Non-Chassis Based		
2	Support for 100G QSFP+ Port	Yes		
3	No. of Ports	Should have minimum 8 Nos of 10G and 8 Nos of 100G QSFP28 Ports; Fully Populated from Day-1		
4	Switching Capacity (Gbps)	2560 Or higher		
5	a. Layer 2 Protocols	a. VLAN, LAG, LACP, STP, MSTP, RSTP, IEEE 802.3x		
6	b. Basic & Advance Layer-3 Protocol	b. EVPN-VXLANESI-LAG or equivalent (No proprietary solutions are to be deployed), OSPFv2, OSPFv3, PBR, BGP, BGP4 , IS-IS, PIM-SSM		
7	c. Management Protocol	c. Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, NTP, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sflow/netflow, OpenConfig, Filtered packet mirroring over GRE/SPAN/ERSPAN, telemetry buffer queue depth monitoring/QOS for prioritizing the traffic during congestion with minimum 8 queue per port, Same OS across all the proposed network switches for simplified operations.		
8	d. QoS	d. WRED, SPQ, SDWRR/ WRR, , , 802.1Qbb, 8queues /port, Remarking of bridged packet,-PFC, ECN		
9	Security Feature	VLAN & Routed ACL, Should support 1500 Ingress /1500 Egress or more ACL entries or 32K or more prefix/host entries as endpoint for traffic		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
18	**Interconnect Switch - Type 1**			
		segmentation, 802.1x, RADIUS/TACACS, Port Security / equivalent ,BPDU Guard, IGMP snooping		
10	Other features	Switch should support all functions required to operate as an interconnect switch connecting various devices including firewall and routers with an non-blocking fabric		
11	Redundant Power Supply	Internal Redundant Power Supply fully loaded on day 1		
12	Redundant FAN	Redundant FAN fully loaded from day 1		
13	Feature Support	Device, OS, Optics, Manager from same OEM. Should be managed through unified Network Manager.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
19	**Interconnect Switch - Type 2**			
1	Type of Switch	Chassis Based/Non-Chassis Based		
2	Support for 10 SFP & 100G QSFP+ Port	Yes		
3	No. of Ports	Should have minimum 16 Nos of 10G and 8 Nos 100G QSFP28 Ports; Fully Populated from Day-1		
4	Switching Capacity(Gbps)	1920 Or higher		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
19	**Interconnect Switch - Type 2**			
5	a. Layer 2 Protocols	802.1Q VLAN, LAG, LACP, STP, MSTP, RSTP, VXLAN, IEEE 802.3x,VLAN		
6	b. Basic & Advance Layer-3 Protocol	EVPN-VXLANESI-LAG or equivalent VXLAN-EVPN LAG (No proprietary solutions are to be deployed), Static routing, RIPv1/RIPv2, BGP, OSPFv2, OSPFv3, PBR		
7	c. Management Protocol	Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, NTP, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sflow/netflow, OpenConfig, Filtered packet mirroring over GRE/SPAN/ERSPAN, telemetry, buffer queue depth monitoring//QOS for prioritizing the traffic during congestion with minimum 8 queue per port, Same OS across all the proposed network switches for simplified operations.		
8	d. QoS	WRED, SPQ, SDWRR/ WRR, , , 802.1Qbb ,802.1Qaz, 8queues /port, Remarking of bridged packets, PFC, ECN		
9	Security Feature	VLAN & Routed ACL, Should support 1500 Ingress /1500 Egress or more ACL entries or 32K or more prefix/host entries as endpoint for traffic segmentation, 802.1x, RADIUS/TACACS, Port Security or equivalent, BPDU Guard, IGMP snooping		
10	Other features	Switch should support all functions required to operate as an interconnect switch connecting various devices including firewall and routers with an on-blocking fabric		
11	Redundant Power Supply	Internal Redundant Power Supply fully loaded day 1		
12	Redundant FAN	Redundant FAN fully loaded from day 1		
13	Feature Support	Device, OS, Optics, Manager from same OEM. Should be managed through unified Network Manager.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
20	**WAN Switch**			
1	Type of Switch	Chassis Based/Non-Chassis Based		
2	No. of FAN Tray	2 Or higher		
3	Support for100G QSFP+ Port	Yes		
4	No. of Slots	Should be populated with 4x1GBase-LX, 4x1000 Base-T,4x10G Base- LR and 4 x 10GBase-SR transceivers. Also should have minimum 8 Nos of 100G QSFP28 Ports and populated with 8 x100G Transceivers (LR/SR will be decided as per TSP MUX); Fully Populated from Day-1		
5	Switching Capacity (Gbps)	2568 Or higher		
6	a. Advance Layer-3 Protocol	EVPN-VXLANESI-LAG or equivalent VXLAN-EVPN LAG/ Multi homing (No proprietary solutions are to be deployed)		
7	b. Security Feature	Port, VLAN & Routed ACL, 802.1x. Should support 1500 Ingress /1500 Egress or more ACL entries or 32K or more prefix/host entries as endpoint for traffic segmentation.		
8	c. Management Protocol	Role Based CLI, SNMPv1/v2/v3, Openstack/REST-API, Python, XML, SSH, Realtime Streaming Telemetry, gRPC, Netconf, ZTP, IPFIX/sflow/netflow, OpenConfig, Filtered packet mirroring over GRE/span/ERSPAN, telemetry, buffer queue depth monitoring//QOS for prioritizing the traffic during congestion with minimum 8 queue per port, Same OS across all the proposed network switches for simplified operations.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
20	**WAN Switch**			
9	d. QoS	WRED, SPQ, SDWRR / WRR, , , 8queues /port, PFC, ECN		
10	Other features	Switch should support all functions required to operate as a WAN Switch acting as interface between Service Provider Links and WAN Router		
11	Redundant Power Supply	Internal Redundant Power Supply for fully loaded chassis from day 1		
12	Redundant FAN	Redundant FAN for fully loaded chassis from day 1		
13	Feature Support	Device, OS, Optics, Manager from same OEM. Should be managed through unified Network Manager.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
21	**Layer-3 Access Switch**			
1	Type of Switch	Chassis Based/Non-Chassis Based		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
21	**Layer-3 Access Switch**			
2	Number of 1000Base-T Ports	48 or higher		
3	Number of 10G SFP+ Port (Uplink)	2 or higher; Fully Populated from Day-1		
4	Stacking Bandwidth	Minimum 20Gbps of stacking/MLAG/MCLAG bandwidth with stacking/MLAG/MCLAG ports from day 1 (along with its transceivers, if required)		
5	Switching Capacity / Forwarding Bandwidth (Non-Blocking) (Gbps)	136 or higher		
6	Number of active VLAN Supported	500		
7	Layer2 Protocols	802.1QVLAN, LAG, LACP, STP, MSTP, RSTP, IEEE802.3x, VLAN, 64K MAC Address.		
8	Basic Layer-3 Protocol from day1	Static Routing		
9	Advance Layer-3Protocol support	16K IPv4 LPM routes, OSPFv2, OSPFv3, ISIS, BGP		
10	Premium Layer-3 Protocol support	VRF Lite/VRF/VRRP, EVPN		
11	Security Feature	RA Guard or equivalent, DHCP Snooping, Dynamic ARP Inspection (or similar security feature which validates ARP packets and prevents attacks like ARP cache poisoning or Similar, Control Plane Policing.		
12	Management Protocol	GUI/Web, CLI, Telnet, TFTP, SMPv1, SNMPv2/V2C, SNMPv3, NTP, RMON, SSHv2, IP Based Management, IPFIX/Sflow/Netflow, OpenConfig, filtered packet mirroring over GRE/span/ERSPAN, Same OS across all the proposed network switches for simplified operations.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
21	**Layer-3 Access Switch**			
13	QoS	802.1p, SP, Queues per port, WRED /WTD, Sflow/Netflow, Shaping, Policing/Rate Limiting, Strict Priority Queueing or Low Latency Queueing.		
14	Redundant Power Supply	Internal Redundant Power Supply fully loaded day 1		
15	Redundant FAN	Redundant FAN fully loaded from day 1		
16	Feature Support	Device, OS, Optics, from same OEM.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
22	**CE Router / Internal WAN Router**			
1	Type of Router	Chassis Based/Non-Chassis Based		
2	Type of Router	WAN		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
22	**CE Router / Internal WAN Router**			
3	Routing Engine	The Router should be populated with Routing Card/Engines/control plane /supervisor engine/multi-core x86 CPU		
4	Aggregated Throughput (Gbps)	1600 Or higher		
5	Port population	Should be supplied with 16x 10G SFP+ ports and 6 No. of 100G QSFP28 ports with non-blocking architecture and wire-speed from day 1.; Fully Populated from Day-1		
6	Number of Routes	Should support 1M IPv4, 450K IPv6 Routes		
7	Routing Protocols from day-1	OSPF, BGP MPLS, EVPN-MPLS, Segment Routing, Multicasting-MVPN/ MOFRR, RSVP-TE, LDP, BGP-LU-SR-TE		
8	Network Management Protocols	Role based cli, config rollback, python scripts, rest API, netconf, xml, schema, secure boot/signed image verification, secure copy		
9	Security Protocol	radius,802.1x, tacacs, stateless ACL, dynamic ACL, rule propagation via BGP, control plane dos,		
10	QoS	Support Class-Based Weighted Fair Queuing (CBWFQ) or Weighted round robin queuing, WRED, Hierarchical QoS for Traffic Management, inspections.		
11	IPv6 Ready	IPv6: OSPF v3 and static routers ipv6 Routing IPv6 Multicast IPv6 QoS, IPv6 VPN over MPLS		
12	Redundant Power Supply	Internal Redundant Power Supply fully loaded day 1		
13	Redundant FAN	Redundant FAN fully loaded from day 1		
14	Feature Support	Device, OS, Optics, from same OEM.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
23	**Internet Router**			
1	Type of Router	WAN		
2	No. of 10G SFP+ ports (Fiber)	16 Or higher		
3	Port population	Should be supplied on day 1 with 4 x 1000Base-LX Single Mode SFP transceivers, 4 x /1000Base-T Interface Ports and 4 x 10G Base SR Transceivers. Should be scalable to support additional 4 X 40/100G QSFP ports; Fully Populated from Day-1		
4	Switching Capacity (Gbps)	256 or higher		
5	Number of Routes	Should support 1M IPv4, 450K IPv6 Routes		
6	Routing Protocols	OSPF, BGP, MPLS, EVPN-MPLS, Segment Routing, Multicasting MVPN/MOFRR, RSVP- TE, LDP, BGP-LU, SR-TE		
7	Network Management Protocols	Role based CLI, Config rollback, python scripts, rest API, Netconf, xml schema, secure boot/signed image verification, secure copy		
8	Security Protocol	secure boot/signed image verification, secure copy		
9	QOS	Support Class-Based Weighted Fair Queuing (CBWFQ) or Weighted round robin queuing, WRED, Hierarchical QoS for Traffic Management, inspections.		
10	IPv6 Ready	IPv6:OSPFv3 and static routers IPv6 RoutingIPv6 Multicast IPv6QoS IPv6 VPN over MPLS		
11	Redundant Power Supply	Internal Redundant Power Supply fully loaded day 1		
12	Redundant FAN	Redundant FAN fully loaded from day 1		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
23	**Internet Router**			
13	Feature Support	Device, OS, Optics, from same OEM.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
24	**Remote Firewall – Type 1**			
1	Type of Router	WAN		
2	Port population	Should be supplied on day 1 with 8 x Gigabit Ethernet (10/100/1000 Base T) ports, 2 X 1000Base-SX Single Mode SFP transceivers and 2x 10G Base LR Transceivers. All mentioned SFP should be fully populated from day one (1).		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
24	**Remote Firewall – Type 1**			
3	Features	Layer3-Layer4, NAT, Application Visibility and Control (AVC), Next Generation Intrusion Prevention System (IPS)		
3	RoutingProtocolsfromday-1	RIPv1 and v2, OSPF v2 and v3, ISIS, BGP4		
4	Network Management Protocols	Role based CLI, Web-UI, Config roll back		
5	IPsec Throughput	10 Gbps (Packetsize:512 bytes)		
6	IPsec Encryption	site-to-site, hub and spoke, advpn/static vpn or equivalent, aes-gcm, sha- 384 or hmac-sha-256 IPSEC encryption		
7	IPsec VPN Tunnels(S2S)	1500		
8	IPsec VPN Tunnels(C2S)	15000		
9	SSL VPN Tunnel	500		
10	SSL Inspection Throughput	1 Gbps		
11	Security Protocol	Stateful firewall, distributed dos, ipv6, nat, 802.1x		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
24	**Remote Firewall – Type 1**			
12	QOS:	Shared policy shaping, per-IP shaping, interface-based traffic shaping, maximum and guaranteed bandwidth, maximum concurrent connections per IP, traffic prioritization, Type of Service (TOS), ,Differentiated Services (DiffServ) and Forward Error Correction (FEC) for VPN support		
13	IPv6Ready	Management over IPv6, IPv6 routing protocols, IPv6 tunneling, NAT46, NAT64, IPv6 IPsec VPN,		
14	Redundant Power Supply	Internal Redundant Power Supply fully loaded day 1		
15	Feature Support	All the features mentioned above should be available from day one		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
25	**Remote Firewall – Type 2**			
1	Type of Router	WAN		
2	Port population	Should be supplied on day 1 with 8 x Gigabit Ethernet (10/100/1000 Base T) ports, 2 X 1000Base-SX Single Mode SFP transceivers and 2x 10G Base LR Transceivers. All mentioned SFP should be fully populated from day one (1).		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
25	**Remote Firewall – Type 2**			
3	Features	Layer3-Layer4, NAT, Application Visibility and Control (AVC), Next Generation Intrusion Prevention System (IPS)		
4	RoutingProtocolsfromday-1	RIPv1 and v2, OSPF v2 and v3, ISIS, BGP4		
5	Network Management Protocols	Role based CLI, Web-UI, Config roll back		
6	IPsec Throughput	5 Gbps (Packetsize:512 bytes)		
7	IPsec Encryption	site-to-site, hub and spoke, advpn/static vpn or equivalent, aes-gcm, sha-384 or hmac-sha-256 IPSEC encryption		
8	IPsec VPN Tunnels(S2S)	1000		
9	IPsec VPN Tunnels(C2S)	5000		
10	SSL VPN Tunnel	500		
11	SSL Inspection Throughput	512Mbps		
12	Security Protocol	Stateful firewall, distributed dos, ipv6, nat, 802.1x		
13	QOS:	Shared policy shaping, per-IP shaping, interface-based traffic shaping, maximum and guaranteed bandwidth, maximum concurrent connections per IP, traffic prioritization, Type of Service (TOS), Differentiated Services (DiffServ) and Forward Error Correction (FEC) for VPN support		
14	IPv6Ready	Management over IPv6, IPv6 routing protocols, IPv6 tunneling, NAT46, NAT64, IPv6 IPsec VPN,		
15	Redundant Power Supply	Internal Redundant Power Supply fully loaded day 1		
16	Feature Support	All the features mentioned above should be available from day one		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
26	**SFPTransceiver-10GBase-SR (For Networking Equipment)**			
1	**Type of Transceiver**	SFP+10GBase-SRTransceivers		
2	SFP Mode	Multi		
3	Compatibility with OEMs Products	All		
4	Fibre Cable Type	MMF		
5	Maximum Data Rate	10 Gbps		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
27	**QSFP+28 Transceiver-100 GBase-SR4 (For Networking Equipment)**			
1	**Type of Transceiver**	QSFP 28 - 100GBase-SRTransceivers		
2	SFP Mode	Multi		
3	Compatibility with OEMs Products	All		
4	Fibre Cable Type	MMF		
5	Maximum Data Rate	100 Gbps		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
28	**SFP Transceiver -10GBase-LR (For Networking Equipment)**			
1	**Type of Transceiver**	SFP+10GBase-LR Transceivers		
2	SFP Mode	Single		
3	Compatibility with OEMs Products	All		
4	Fibre Cable Type	SMF		
5	Maximum Data Rate	10 Gbps		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
29	**QSFP+28 Transceiver-100GBase-LR4 (For Networking Equipment)**			
1	**Type of Transceiver**	QSFP 28 -100 GBase-LR4 Transceivers		
2	SFP Mode	Single		
3	Compatibility with OEMs Products	All		
4	Fibre Cable Type	SMF		
5	Maximum Data Rate	100Gbps		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
30	**Network Manager in HA**			
1		Solution to be provided for unified management and monitoring of all the proposed network switches of DC and DR that are part of the RFP.		
2		The leaf-spine fabric must be based on IETF/IEEE Open Standards and interoperable networking protocols with eBGP/ISIS for underlay and EVPN for overlay.		
3		The solution should provide UI-driven wizard based approach to simplify and accelerate deployment of EVPN overlay fabric by automatically generating the resultant CLI configurations and pushing it to the **Data Center** network Switches (i.e Spine, Leaf and Border Leaf Switch).		
4		The Solution should provide management of group-based segmentation/ACL rules centrally from the unified dashboard.		
5		Image upgradation / patch management of the managed network devices should be supported Centrally for Spine and Leaf Fabric		
6		The Network Manager(/Manager) should support user-defined/configuration work flows to carry out multiple network-wide changes automated execution and conditional/system checks.		
7		The manager should provide network wide rollback to revert back changes if required from Central Controller.		
8		The Manager should gather streaming telemetry from all the managed devices for management		
9		Should provide ability to view Telemetry data over a timeline. The Data Should be available for at least 30 days.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
30	Network Manager in HA			
10		Visibility of the these parameters is expected but not limited to - CPU, Memory, interface stats (traffic counter, error, discard), MAC table, ARP table, IPv4 route table, IPv6 route table, BGP, capacity parameters / TCAM/VXLAN/VNID table ,running config, traffic flow (sflow/IPFIX/Netflow), Switch environment stats(FAN, Temperature, Power Supply).		
11		Should provide building customized dashboards/access using any of the collected telemetry data.		
12		Should be capable of showing hop-by-hop flow path and drops on links taken by a flow between 2 end points or should support Netflow/SFLOW		
13		Should be able to show deviation from user defined config/policy .		
14		All proposed network switches part of this RFP should be managed from single dashboard for ease of management.		
15		Should show underlay and overlay Topology view, Endpoint search and connectivity on network topology, Flow Visualization on topology and Health/error summary on topology.		
16		Should support ML for dynamic baselining/proactive alerting/suggestion or Should support telemetry for proactive alerting/suggestion.		
17		Should provide zero touch provisioning for quick deployment and replacement of Switches.		
18		Central controller should provide detailed traffic flow analytics to search and see what protocols/port are used and how much data is transferred between 2 end-points during a period of time or should support Netflow/SFLOW Or Central controller should provide detailed traffic flow analytics to search and to show ping, traceroute, forward and reverse path between 2 end-points.		
19		Controller should support role based access control.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
30	**Network Manager in HA**			
20		Should support in-product documentation to simplify operators experience		
21		All licenses required for the mentioned features as per product specification must be available on day-1 for all the proposed network switches as part of this RFP		
22		The proposed solution must be fully on-premises not requiring any user data to be processed on the cloud.		
23		All the communication between Fabric management appliance and switches should be encrypted.		
24		Bidder shall provide required server Hardware & Software to run the solution in HA for DC & DR Respectively. Failure of all server hardware should not impact packet forwarding on the network devices.		
25		All relevant licenses for the asked features should be supplied on day-1. ERNET India may ask for POC as part of technical evaluation and all features should be show cased off the shelf.		
26		Management solution should be from same OEM as the managed devices. 24x7 TAC support should be available directly from the OEM.		

31 Intelligent cabling solution# including all accessories

Intelligent Cabling is required at DC for 100 Racks & at DR for 50 Racks. The Cabling Structure required is as follows:

Network-1,100G Network:

a) There are Two Spine Switch-Primary and secondary in DC & DR each
b) Each DC spine switch will have 250 X 100G port (Total 2 X 250, 100G port).

c) Each DR spine switch will have 140 X 100G port (Total 2 X 140, 100G port).
d) 48 MPO port to be established between Primary and secondary spine rack for connecting Network/routing devices.
e) 48 each MPO port to be established within (Primary and secondary) spine rack for connecting Network /routing devices.
f) At Server/storage rack end, there will be two nos of 24 port Leaf switches.
g) Each Leaf switch will have 2 X 100G MPO connectivity from Spine switch (Primary & Secondary). Total 4 X 100G connections per rack will connect to spine switches as two leaf switches are available in each Rack.
h) Each Leaf switch will have 24X 10G on fiber, to connect server/storage
i) 2 X 16 LC Duplex connections will be extended to each Server/Storage via fiber shelf to enable intelligent solution.

Network-2,10GNetwork:

a) There are Two Core Switch-Primary and secondary in DC & DR each
b) Core switch will have 110 X10G port in DC & 60x10G ports in DR
c) 24 LC port to be established between Primary and secondary core rack for connecting Routing/Network.
d) 24 LC port to be established within Primary and secondary core rack for connecting Routing/Network.
e) At Server/storage rack end, there will be one 48 copper port edge switch to support 10G from core switch.
f) Each OOB will have 2 X 10G LC connectivity towards core switch (Primary & Secondary). 1x10G for Primary and 1x10G for secondary core Switch.
g) Edge switch will have 48 X 1G on copper to connect server/storage to connect server/storage of the rack.
h) 48 Copper connections will be extended to Server/Storage via copper panel to enable intelligent solution.

i) The Top of Rack (ToR) i.e leaf switch in the S/R will connect to the ***each*** Spine switch (in N/R) via 12F (2 x 12 MPO connectors on each side) MPO trunk cables on OM5. All MPO trunk cables and MPO cable assemblies shall be Method B polarity only. The adapters shall be compliant to TIA/EIA FOCIS 5, which is commonly referred to as “aligned keys” or “key-up to key-up.” Each link between the ToR and Spine shall support 100GBASE-SR4 application for the complete channel. Contractor shall check and guarantee the support of 100GBASE-SR4 application for the longest distance possible between racks inside the data center. All patch cords required to complete the connectivity shall be standard compliant.
j) ***Each OOB will connect to primary and secondary core switch (N/W) via 12F (2 x 12 MPO connector on each side) MPO trunk cables on OM4***. Each link between the edge and core Switch shall support 10GBASE-S application for the complete channel. Contractor shall check and guarantee the support of 10GBASE-S application for the longest distance possible between racks inside the data centre. All patch cords required to complete the connectivity shall be standard compliant.

GENRAL NOTE for all Active equipment(s): Bidder shall supply required quantity of fiber patch chords (Single mode/ Multimode), patch chord as per site requirements. All accessories for successful installation in rack should be supplied by Bidder.

Bidder should provide AIM solution licenses as per BoQ defined in the Tender Document. Also AIM Solution software and its hardware should be from same OEM. Further, price for AIM Solution along with cabling/patch panel/Patch chords/cassettes/AIM Monitor etc. required due to any increase in Racks along with equipment will be derived on a prorated basis.

DC and DR location is yet to be finalised. Further it is anticipated that there will be 8-10 Rack in each Row in DC and DR. In respect of Server and Network rack bifurcation, there will be 90 Server and 10 Network Rack in DC as well as 40 Server and 10 network rack in DR. However If there is any change in predicted layout, bidder shall accomodate the same without any price escalation to ERNET India/ CERT-In.

Product specification for 100G MPO Connectivity- OM5 components

Deploy optical fiber pre-terminated solution consisting of trunk cables with pre-terminated MPO connector, cassettes, patch cords and optical fiber patch panels etc. as a standard configuration. The entire component shall be intelligent enabled solution. The fiber count per MPO trunk cable shall be 12F MPO pinned connectors on either sides) The application shall support up to 10/40/100/400G. The fiber shall be multimode OM5 fiber features extended bandwidth range of 850 to 950nm that enables it to provide optimal support to SWDM applications by enhancing its capability to transmit at least four low-cost wavelengths for longer distance, reducing parallel fiber count by four-folds and high-speed application of 400G. **Complete Passive Components, Intelligent Cabling including AIM Monitor and Intelligent (AIM) System Software should be from Same OEM.**

i. Performance Specification

S. N.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	OM5 LC - MPO 2 connector Fiber Link Performance	The losses should not exceed the following dB values for the various lengths mentioned below:		
2	16 Meters	0.9 dB for 850 nm and 0.87 dB for 1300 nm		
3	36 Meters	0.96 dB for 850 nm and 0.89 dB for 1300 nm		

S. N.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
4	56 Meters	1.02 dB for 850 nm and 0.91 dB for 1300 nm		
5	OM5 MPO - MPO 2 connector Fiber Link Performance			
6	16 Meters	0.7 dB for 850 nm and 0.67 dB for 1300 nm		
7	36 Meters	0.76 dB for 850 nm and 0.69 dB for 1300 nm		
8	56 Meters	0.82 dB for 850 nm and 0.71 dB for 1300 nm		
9		The minimum distance of the following applications shall be supported by the OM5 four (4) connector link performance		
10	25GBASE-SR	130 meters		
11	40GBASE-SR4	210 meters		
12	40GBiDi	210 meters		
13	40G-SWDM4	460 meters		
14	100GBASE-SR4	130 meters		
15	100G-SWDM4	150 meters		
16	16G FC @ 850 nm	200 meters		
17	32G FC @ 850 nm	130 meters		
18	128 FC @ 850 nm	110 meters		
19		Tool reports / test report to be shared for above configuration.		

ii. Fiber Patch cord assembly OM5 MPO to MPO, Male/Female

S. N.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	Type	**To be assessed by Bidder**		
2	Interface and port			
3	Fiber Type			
4	Interface Feature,			
5	Total fiber quantity			
6	Jacket color	As per OEM		
7	Cable Product Type	Fiber indoor cable, Non-armored, Gel free		
8	Outer Sheath/ Environmental Space	Low Smoke Zero Halogen (LSZH), Riser, Indoor Single sheath jacket		
9	Flame Test Method	***IEC 60332-3/ IEC 60332-1 , IEC 60754-2, IEC 61034-2***		
10	Standards:	ANSI/ICEA S-83-596, Telcordia GR-409/ IEC 61753-1 or equivalent		
11	Safety Standard	UL 1666, UL 1685 /ETL / BIS or equivalent Standards		
12	Insertion Loss Change, mating	0.3 dB		
13	Return Loss, minimum	27dB		
14	Insertion Loss Change, temperature	0.3 dB		
15	Insertion Loss, maximum	0.25 dB		
16	Intelligent compatibility	Patch cord shall be compatible for intelligent solution		
17	RoHS	RoHS Compliant		

iii. Fiber Distribution adaptor OM5, MPO Port

S. N.	Details	Standard Compliance	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	Type	**To be assessed by Bidder**		
2	Interface and port			
	Interface Feature, rear			
4	Port Duct cover	No		
5	Standard	MPO distribution adaptor shall meet the most recent revision of TIA/EIA-568-C.3 standard, and its published addenda.		
6	Safety Standard	UL/ BIS or equivalent Standards		
7	Intelligent compatibility	Distribution adaptor shall be modular type and Intelligent enabled		
8	Fiber Type	OM5.		
9	Qualification Standards	IEC 61753-1 | TIA-568.3-D		
10	RoHS	RoHS Compliant		

iv. Fiber Trunk cable assembly OM5 MPO (Male/Female) to MPO (Male/Female)

S. N.	Details	Standard Compliance	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	Type	**To be assessed by Bidder**		
2	Interface and port			
3	Interface Feature,			
4	Total fiber quantity			
5	Panel compatibility			
6	Cable compatibility			
7	Fiber Type	OM5		
8	Jacket color	As per OEM		
9	Cable Product Type	Fiber indoor cable, Non-armored, Gel free		
10	Outer Sheath/ Environmental Space	Low Smoke Zero Halogen (LSZH), Riser, Indoor Double sheath jacket for more protection		
11	Cable strength member	Ripcord and Aramid Yarn shall be included as cable protection		
12	***Flame Test Method***	***IEC 60332-3/ IEC 60332-1 , IEC 60754-2, IEC 61034-2***		
13	Standards:	ANSI/ICEA S-83-596, Telcordia GR-409/ IEC 61753-1 or equivalent,		

S. N.	Details	Standard Compliance	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
14	Safety Standard	UL 1666, UL 1685/ETL/ BIS or equivalent Standards		
15	Insertion Loss Change, mating	0.3 dB		
16	Return Loss, minimum	27dB		
17	Insertion Loss Change, temperature	0.3 dB		
18	Insertion Loss, maximum	0.20 dB		
19	RoHS	RoHS Compliant		

LC type fiber patch cords, OM5

S. N.	Specifications	Requirement	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	Fiber type	Multimode OM5		
2	Construction	Two fiber duplex Cordage Non-armored gel free cable		
3	Cable Sheath	Low Smoke Zero Halogen (LSZH) Riser rated		
4	Connector type	LC/UPC to LC/UPC, Fiber patch cord (1.6/1.7)mm / 3.5mm. Riser		
5	Cable Length	As per the BOQ		
6	Color	Lcable and connector should be of different color		

S. N.	Specifications	Requirement	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
7	Protection	Aramid yarn shall be provided around 250nm coating on fiber cable		
8	Minimum Bend Radius	38 mm (Loaded), 15mm (Unloaded)		
9	Tensile Load, maximum	20N (long term) 67N short term)		
10	Compression	10 N/mm as per IEC 60794-1 E3 test method		
11	Ferrule	Pre-radiused made of Zirconia		
12	Cable Qualification Standards	ANSI/ICEA S-83-596, Telcordia GR-409/ IEC 61753-1 or equivalent		
13	Flame Test Listing	NEC OFNR-ST1 (ETL) / NEC OFNR-LS (ETL) and c(ETL)/ UL 60950-1 or equivalent		
14	Flame Test Method	IEC 60332-3/ IEC 60332-1, IEC 60754-2, IEC 61034-2, IEEE 383, UL1666, UL 1685/ BIS or equivalent Standards		

v. Intelligent fiber panel- MPO type, OM5

S. N.	Details	Standard Compliance	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	Type	Intelligent fiber Patch panel shall be modular, accept cassette type module and distribution adaptor pack for multimode (OM5) type fiber		
2	Standards	Intelligent panel should meet ANSI/TIA 568C.2 specifications and AIM standard such as ISO/IEC 18598 and TIA 606-B and ISO/IEC 14763-2.		

S. N.	Details	Standard Compliance	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
3	LC Port capacity	Intelligent pre-terminated fiber shelves shall be available in 1U sliding/fixed configuration to support up to 48 -duplex LC ports or 2U sliding configuration to support up to 144 -duplex LC ports		
4	MPO Patch connections	Intelligent fiber patch panels shall be available in 1Usliding configurations with up to 24/32 MPO ports, in 2U/4U sliding configuration to support up to 96 MPO ports. Requirement of 1U/2U/4U in each rack shall be assessed by bidder.		
5	***Patch cord compatibility***	***Intelligent patch panel shall provide a button and an LED indicator at every panel port/single button on panels to enable easy tracing and identification of patch connections in the telecom room.***		
6	Sensing Assembly Installation	Intelligent patch panels shall be provided with all necessary system-connecting cable(s).		
7	Connection of existing port	Intelligent fiber patch panels should allow for removal and replacement of sensing Assembly. Any fault in the sensor should not disrupt the operation of panel network port.		
8	***Patch cord/wire manager***	***Panel shall have inbuilt rear cable manager and from patch cord manager including visible label plate. Separate Patch cord manager is also allowed.***		
8	RoHS	RoHS Compliant		

vi. Any other item required to complete the OM5 Intelligent cabling – To be assessed by bidder & its OEM. Quantity and price of the same shall be included in bid

S. N.	Details	Standard Compliance	Compliance (Yes/No)

1	Any other item required to complete the OM5 Intelligent cabling	To be assessed by bidder & its OEM. Quantity and price of the same shall be included in bid	

Product specification for 10G MPO Connectivity- OM4 components

Deploy optical fiber pre-terminated solution consisting of trunk cables with pre-terminated MPO connector, Fiber modular cassette with LC interface, 2F LC -LC patch cords and Intelligent fiber patch panels as a standard configuration. The entire component shall be intelligent enabled solution. The application shall support up to 10/40G. The fiber shall be multimode OM4 fiber. **Complete Passive Components, Intelligent Cabling including AIM Monitor and Intelligent (AIM) System Software should be from Same OEM.**

i. Fiber trunk cable assembly OM4 MPO (male/Female) to MPO (male/Female)

Sl. No.	**Details**	**Standard Compliance**	**Marked/ Highlighted Cross Reference of Specification with reference page no.**	**Compliance (Yes/No)**
1	Type	**To be assessed by Bidder**		
2	Interface and port			
3	Interface Feature,			
4	Total fiber quantity			

Sl. No.	Details	Standard Compliance	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
5	Panel compatibility			
6	Cable compatibility			
7	Fiber Type	OM4		
8	Jacket color	As per OEM		
9	Cable Product Type	Fiber indoor cable, Non-armored, Gel free		
10	Outer Sheath/ Environmental Space	Low Smoke Zero Halogen (LSZH), Riser, Indoor Double sheath jacket for more protection		
11	Cable strength member	Ripcord and Aramid Yarn shall be included as cable protection		
12	***Flame Test Method***	***IEC 60332-3/ IEC 60332-1 , IEC 60754-2, IEC 61034-2***		
13	Standards:	ANSI/ICEA S-83-596, Telcordia GR-409/ IEC 61754-7 or equivalent,		
14	Safety Standard	UL 1666, UL 1685// BIS or equivalent Standards		
15	Insertion Loss Change, mating	0.3 dB		
16	Return Loss, minimum	27dB		
17	Insertion Loss Change, temperature	0.3 dB		
18	Insertion Loss, maximum	0.20 dB		

Sl. No.	Details	Standard Compliance	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
19	RoHS	RoHS Compliant		

ii. Fiber Distribution fiber panel, Modular, OM4 LC

Sl. No.	Details	Standard Compliance	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	Type	**To be assessed by Bidder**		
2	Interface and port			
3	Interface Feature, rear			
	Panel compatibility			
	Cable compatibility			
4	Port Duct cover	Yes		
5	Standard	Fibre distribution fiber panel shall meet the most recent revision of TIA/EIA-568-C.3 standard, and its published addenda.		
6	Safety Standard	UL/ BIS or equivalent Standards		
7	Fiber Type	OM4 Multimode		
8	Intelligent compatibility	Fibre distribution fiber panel shall be modular type and Intelligent enabled		
9	RoHS	RoHS Compliant		

iii. Fiber Modular Cassette OM4 MPO – LC

Sl. No.	Details	Standard Compliance	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	Type	**To be assessed by Bidder**		
2	Interface and port			
3	Interface Feature, rear			
4	Panel compatibility			
5	Cable compatibility			
6				
7	Port Duct cover	Yes, must required		
8	Standard	MPO cassettes shall meet the most recent revision of TIA/EIA-568-C.3 standard, and its published addenda.		
9	Safety Standard	UL/ BIS or equivalent Standards		
11	***Approximate dimension***	***OEM may asses the dimensions as per site requirement.***		
12	Fiber Type	OM4 Multimode		
13	Attenuation	1.00 dB/km @ 1,300 nm 3.00 dB/km @ 850 nm		
14	Insertion Loss Change, temperature	0.3 dB		
15	Insertion Loss, maximum	0.47 dB		

Sl. No.	Details	Standard Compliance	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
16	Intelligent compatibility	Fiber Cassette shall be modular type and Intelligent enabled		
17	RoHS	RoHS Compliant		

iv. LC type fiber patch cords, OM4

Sl. No.	Specifications	Requirement	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	Fiber type	Multimode OM4		
2	Construction	Two fiber duplex Cordage Non-armored gel free cable		
3	Cable Sheath	Low Smoke Zero Halogen (LSZH) Riser rated		
4	Connector type	LC/UPC to LC/UPC, Fiber patch cord (1.6/1.7mm) / 3.5mm. Riser		
5	Cable Length	As per the BOQ		
6	Color	cable and connector should be of different color		
7	Protection	Aramid yan shall be provided around 250nm fiber cable		
8	Minimum Bend Radius	38 mm (Loaded), 15mm (Unloaded)		
9	Tensile Load, maximum	20N (long term) 67N short term)		
10	Compression	10 N/mm as per IEC 60794-1 E3 test method		
11	Ferrule	Pre-radiused made of Zirconia		

Sl. No.	Specifications	Requirement	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
12	Cable Qualification Standards	ANSI/ICEA S-83-596, Telcordia GR-409/ IEC 61754-7 or equivalent		
13	Flame Test Listing	NEC OFNR-ST1 (ETL) / NEC OFNR-LS (ETL) and c(ETL)/ UL 60950-1 or equivalent		
14	Flame Test Method	IEC 60332-3/ IEC 60332-1, IEC 60754-2, IEC 61034-2, IEEE 383, UL1666, UL 1685/ BIS or equivalent Standards		
15	Insertion Loss, maximum	0.3 dB		
16	Return Loss, minimum	27 dB		
17	Regulatory Compliance	RoHS 2011/65/EU compliant		

v. OEM should have completed Two projects of Intelligent Cabling & AIM.

vi. Any other item required to complete the OM4 Intelligent cabling – To be assessed by bidder & its OEM. Quantity and price of the same shall be included in bid

S. N.	Details	Standard Compliance	Compliance (Yes/No)
1	Any other item required to complete the OM4 Intelligent cabling	To be assessed by bidder & its OEM. Quantity and price of the same shall be included in bid	

Product specification for 1G/10G Copper components

Deploy Copper cabling solution consisting of single ended copper patch cord with RJ45 male connector, intelligent Copper patch panel, reduced diameter patch cords for high density connecting servers as a standard configuration. The entire component shall be intelligent enabled solution. The application shall support up to 1/10G.The copper solution shall be Cat-6A U/UTP cabling. **Complete Passive Components, Intelligent Cabling including AIM Monitor and Intelligent (AIM) System Software should be from Same OEM.**

i. CAT 6A Intelligent Patch Panel

Sl. No.	**Details**	**Standard Compliance**	**Marked/ Highlighted Cross Reference of Specification with reference page no.**	**Compliance (Yes/No)**
1	Type	Patch panel Unshielded / Unshielded Twisted Pair (U/UTP), Category 6A		
2	Standards	The panel should meet ANSI/TIA 568C.2 Category 6A Specifications		
3	Panel configuration	The panel shall be available in 24-port and 48-port configurations with universal A/B labelling and 110 connector terminations on rear of panel allowing for quick and easy installation of 22 to 24 AWG cable		
4	Material used	Panel shall be available in straight with made of Powder- coated steel. Color shall be as per OEM		
5	Intelligent system	The panel must be an intelligent system		
6	Additional future for noise cancellation	Termination managers must be provided with the panel. These termination managers provide proper pair positioning, control, and strain relief features to the rear termination area of the panel.		

Sl. No.	Details	Standard Compliance	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
7	Third party certificate for Genunity	Third party certificate for Genunity ETL/3P or equivalent four connector channel certificate and test report .		
8	Rear cable manager	Panel shall have rear cable manger with proper design to hold all 24 cable. This shall provide strain relief for outlet and organization of cables being routed to the back of a patch panel.		
9	RoHS	RoHS Compliant		
10	Patch Panel Ports	To be assessed by bidder to connect 48 port OoB Switch and other respective units (server and Leaf Switch)		

ii. CAT 6A LSZH U/UTP RJ45 regular Patch Cords

Sl. No.	Details	Standard Compliance	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	Type	Unshielded / Unshielded Twisted Pair (U/UTP), Category 6A patch cords		
2	Standards	The Cordage should meet ANSI/TIA 568C.2 Category 6A Specifications		
3	Length	The cordage shall be available in different length based on the site requirement		
4	Conductor	Copper must be solid single strand copper conductor for panel termination		

Sl. No.	Details	Standard Compliance	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
5	Fire Safety standards:	LSZH		
6	Diameter Over Jacket	7.24 mm		
7	Safety Standard	UL 1863/ETL		
8	Additional info	The cable and cordage shall be UTP components that do not include internal or external shields, screened components or drain wires that require additional grounding and bonding		
9	RoHS	RoHS Compliant		

iii. CAT 6A LSZH U/UTP RJ45 reduced dia. Patch Cords

Sl. No.	Details	Standard Compliance	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	Type	Unshielded / Unshielded Twisted Pair (U/UTP), Category 6A patch cords.		
2	Standards	The Cordage should meet ANSI/TIA 568C.2 Category 6A Specifications		
3	Length	The cordage shall be available in different length based on the site requirement		
4	Fire Safety standards:	LSZH		
5	Diameter Over Jacket	4.95 mm | 0.195 in		

Sl. No.	Details	Standard Compliance	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
6	Safety Standard	UL 1863/ BIS or equivalent Standards		
7	Additional info	The cable and cordage shall be UTP components that do not include internal or external shields, screened components or drain wires that require additional grounding and bonding		
8	RoHS	RoHS Compliant		

iv. Any other item required to complete the Copper cabling – To be assessed by bidder & its OEM. Quantity and price of the same shall be included in bid

S. No.	Details	Standard Compliance	Compliance (Yes/No)
1	Any other item required to complete the Coper Intelligent cabling	To be assessed by bidder & its OEM. Quantity and price of the same shall be included in bid	

Intelligent AIM system Monitor

Sl. No.	AIM System Monitor at Rack level	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	The AIM System Monitor shall be compatible with mounting on 19” (width) based hardware per EIA-310.		
2	The AIM System Monitor shall provide capability for a technician to communicate with AIM System Software component.		

Sl. No.	AIM System Monitor at Rack level	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
3	The AIM System Monitor shall communicate with the AIM-enabled patch panels in the racks		
4	The AIM System Monitor shall be able to display live end-to-end tracing information on its screen during patching activities. The screen may be a fixed unit or portable unit fixed in the racks using suitable mount/brackets.		
5	The AIM System Monitor shall be able to display on the screen information indicating if a traced panel port is assigned to a scheduled work order.		
6	The AIM System Monitor shall be able to display electronic work orders for moves, adds and changes (MACs).		
7	The AIM System Monitor shall have a configurable Ethernet LAN connection capability (10BASE-T, 100BASE-TX or 1000BASE-T) to enable communication with AIM System Software component.		
8	Complete Passive Components, Intelligent Cabling including AIM Monitor and Intelligent (AIM) System Software should be from Same OEM.		
9	AIM monitor display system should have the capacity to monitor three RACKs. Further Bidder should provide one Monitor for three server Racks and One Monitor for each Network Rack.		
10	All the features mentioned above should be available from day one		

Intelligent AIM system Software

Sl. No.	Intelligent System (AIM) Software defined by the ISO/IEC 18598 standard	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	The AIM System Software component shall be web based.		
2	The system should support port in DC & DR as per BoQ. AIM solution software and its hardware should be from same OEM.		
3	*The AIM System Software component shall support REST APIs and Simple Network Management Protocol (SNMP) and support SNMP v1, SNMP v2c, and SNMP v3. Bidder/OEM needs to support integration with third party monitoring and management systems.*		
4	The AIM System Software component shall support IPv4 and IPv6 communications.		
5	The AIM System Software component shall support automatic and manual database backups.		
6	The AIM System Software component shall have capability to auto discover the installed AIM hardware component (intelligent panels and control systems) in each rack/cabinet and to auto populate this information in its database.		
7	The AIM System Software component shall have the capability to auto discover networked devices that are connected to the pre-defined managed network switches (LAN and SAN environments) and then to auto populate that information in its database.		
8	The AIM System Software component shall provide end user with ability to define manual, automatic, or disabled mode for conducting discovery of networked devices. The automatic device discovery feature shall allow end user to determine a polling schedule, as well as the ability to automatically trigger the discovery process based on SNMP link-up traps from managed network switches.		

Sl. No.	Intelligent System (AIM) Software defined by the ISO/IEC 18598 standard	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
9	The AIM System Software component shall have the capability to auto discover IP address, MAC ID, WWN and Host Name information for networked devices and then to auto populate this information into its database.		
10	The AIM System Software component shall have the capability to auto discover networked devices with multiple MAC addresses (i.e., servers with multiple NICs, virtual machines, wireless APs, IP phone/computer pairs, etc.) and then to auto populate that information in its database.		
11	The AIM System Software component shall have the capability to auto discover VLAN ID information on managed network switches and then to auto populate that information in its database.		
12	The AIM System Software component shall provide the ability to define type of networked devices based on MAC or IP address range that could also be applied retroactively to already discovered devices. Once defined, each device upon its discovery shall be automatically labelled and represented with an appropriate icon in the database to correspond to the device type definition.		
13	The AIM System Software component shall have the capability to detect configuration changes to managed SAN and LAN switches.		
14	The AIM System Software component shall have the capability to detect when a networked device has moved or changed its physical location.		
15	The AIM System Software component shall provide capabilities for defining a set of specific system conditions that need to be tracked.		
16	The AIM System Software component shall provide a dedicated service-provisioning feature for servers, including server templates, and graphics to allow for efficient planning and deployment of servers in the data center.		

Sl. No.	Intelligent System (AIM) Software defined by the ISO/IEC 18598 standard	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
17	The AIM System Software component shall provide a server decommissioning feature that ensures removal of all circuits connected to the server to eliminate “dormant” connections.		
18	The AIM System Software component shall have the capability to document various topologies (zone, pod, cell, etc.) for Data Center applications.		
19	The AIM System Software component shall have the capability to audit the switch ports.		
20	The AIM System Software component shall have the capability to send an email message to specified personnel, to automatically execute a designated program or to send a SNMP trap to a destination server each time a pre-defined system event is received.		
21	Complete Passive Components, Intelligent Cabling including AIM Monitor and Intelligent (AIM) System Software should be from Same OEM.		
22	The offered AIM Solution should be provided along with backup solution. All the Hardware required for backup should be provided by the bidder. The hardware should be sufficient enough to support the backup of at least 1 months. The time period of backup should be configurable		
23	All the features mentioned above should be available from day one		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
32	**Internal Firewall**			
1	Type	NGFW Or higher		
2	Features	Layer3-Layer4, NAT, Application Visibility and Control (AVC), Next Generation Intrusion Prevention System (IPS)		
3	Traffic handled	TCP, UDP, HTTP/HTTPs		
4	Packet Size	1024 Bytes or 64KB HTTP/application-mix/Enterprise Mix		
5	Throughput (Real World/Prod Performance) (All Features enabled)(Gbps)	Throughput (Real World/Prod Performance) (All Features enabled)(Gbps) : 270 Gbps.		
6	IPsec Throughput	Minimum 240Gbps at layer 4 and Minimum185 Gbps at layer 7		
7	SSL Inspection Throughput	150 Gbps or Higher		
8	Concurrent Session/Concurrent Connection	75 Million Layer 4 sessions or 30 Million Layer 7 sessions		
9	New session/Connection per second	Minimum 600K Layer 4 sessions or Minimum 300K Layer 7 sessions		
10	Type of Interface Supported Multi-select	GECopper, 10GSFP+, QSFP+40G,GESFP, QSFP28 100G		
11	Port Population	The Firewall should have minimum 12 x 10GSFP+, 12 x 40G /100G QFSP 28. All the ports shall be fully Populated with respective Transceivers		
12	Details of the Firewall Policies for the Firewall	Application Visibility License, IPS License		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
32	**Internal Firewall**			
	provided with the License			
13	Tunnels	IPSEC VPN (Site to site), Hub and Spoke		
14	Internet Key Exchange	IKEv1, IKEv2		
15	Security mechanism	State-full signatures, protocol anomaly detection		
16	Number of IPsec VPN Peers Supported (Site to Site)	20000 Or higher. Licenses to be included from day one		
17	Number of IPsec VPN Peers Supported (Client to Site)	20000 Or higher. Licenses to be included from day one		
18	SSL VPN tunnels	20,000 Or higher. Licenses to be included from day one		
19	Power Supply	Internal Redundant Power Supply for fully loaded chassis from day 1		
20	NG IPS Signature supported	15000 or higher		
21	Virtual Domain	minimum 10 and scalable to 200		
22	Onboard storage	3 TB SSD or higher		
23	Feature Support	All the features asked should be available from day one and should be from same OEM. Any open source and third party solution is not accepted		
	Additional Specs -			
24	Security mechanism	Proposed solution shall have required subscription like Threat Intelligence for proper functioning		
25	Certification	Common Criteria/Indian Common Criteria Certification Scheme(IC3S)		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
32	**Internal Firewall**			
26	POC	POC of the solution proposed may be done where the bidder/OEM will have to showcase all the technical features mentioned in the RFP practically. If bidder/OEM fails to showcase any technical feature mentioned in the RFP, then their bid will be rejected.		
27	Feature Support	All the features asked should be available from day one and should be from same OEM. Any open source and third party solution is not accepted		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
33	**Solution Firewall**			
1	Type	NGFW Or higher		
2	Features	Layer3-Layer4, NAT, Application Visibility and Control(AVC), Next Generation Intrusion Prevention System (IPS)		
3	Traffic handled	HTTP/HTTPs		
4	Packet Size	128KB HTTP/HTTPs		
5	Throughput (Real World/Prod Performance) (All Features enabled)(Gbps) considering 100% HTTP Traffic mix	40 Gbps with 128 KB HTTP/HTTPs		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
33	**Solution Firewall**			
6	IPsec Throughput considering 100% HTTP Traffic mix	Minimum 40 Gbps on 128 KB HTTP/HTTPs		
7	Concurrent Session/Concurrent Connection	Minimum 50 Million Layer 4 sessions or minimum 9 Million Layer 7 sessions		
8	New session/Connection per second	Minimum 1.5 Million Layer 4 sessions or minimum 380K Layer 7 sessions		
9	Type of Interface Supported Multi-select	GECopper, 10GSFP+, QSFP+40G, GESFF, QSFP28100G		
10	Port Population	The Firewall should have minimum 12 X 10GSFP+, 4X40G /100G QFSP 28. All the ports shall be fully Populated with respective Transceivers		
11	Details of the Firewall Policies for the Firewall provided with the License	Application Visibility License, IPS License		
12	Tunnels	IPSEC VPN (Site to site), Hub and Spoke		
13	Internet Key Exchange	IKEv1, IKEv2		
14	Security mechanism	State-full signatures, protocol anomaly detection		
15	Number of Ipsec/SSL VPN Peers (concurrent client to site)	25000 Or higher. Licenses to be included from day one		
16	Supported (Site to Site) IPSEC Peers	10000 Or higher Licenses to be included from day one		
17	Power supply	Internal Redundant Power Supply for fully loaded chassis from day 1		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
33	**Solution Firewall**			
18	NG IPS Signature supported excluding custom IPS signatures	15000 or higher		
19	Certification	Common Criteria/Indian Common Criteria Certification Scheme(IC3S) or equivalent		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
34	**Internet Firewall (NGFW)**			
1	Type	NGFW Or higher		
2	Features	Layer 3-Layer 4, NAT, Next Generation Intrusion Prevention System (IPS)		
3	Traffic handled	HTTP/HTTPs		
4	Throughput (Real World/Prod Performance) (All Features enabled)(Gbps) considering 100% HTTP Traffic mix	60 Gbps or higher with 128 KB HTTP/HTTPs		
5	Concurrent Session/Concurrent Connection	100 Million Layer 4 sessions or 30 Million Layer 7 sessions		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
34	**Internet Firewall (NGFW)**			
6	New session/Connection per second	Minimum 3 Million Layer 4 sessions or Minimum 1.2 Million Layer 7 sessions		
7	IPsec Throughput (Gbps) considering 100% HTTP Traffic mix	35 Gbps (Packet size: 128 KB HTTP/HTTPs) or Higher		
8	Port population	Should be supplied on day1 with 8x10GBase-SR Transceivers and 4 x100G Base-SR4 Transceivers		
9	Power Supplies	Dual Or higher		
10	Details of the Firewall Policies for the Firewall provided with the License	Application Visibility License, IPS License		
11	Tunnels	IPSEC VPN (Site to site), Hub and Spoke		
12	Internet Key Exchange	IKEv1, IKEv2		
13	Security mechanism	State full signatures, protocol anomaly detection		
14	NG IPS Signature supported excluding custom IPS signatures	15000 or Higher		
15	Number of IPsec VPN Peers Supported (Site to Site)	8000 Or higher. Licenses to be included from day one		
16	Certification	Common Criteria/Indian Common Criteria Certification Scheme(IC3S) or equivalent		
17	Redundant Power Supply	Internal Redundant Power Supply for fully loaded chassis from day 1		
18	Redundant FAN	Redundant FAN for fully loaded chassis from day 1		
19	Feature Support	All the features asked should be available from day one and should be from same OEM. Any open source and third party solution is not accepted		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
35	**IPS/IDS**			
1	**Platform Requirement**			
1.1		NIPS solution should be a purpose built dedicated standalone appliance and not an integrated firewall module or UTM appliance.		
1.2		Monitoring Interface should be able to operate at layer 2.		
1.3		The appliance must have Real World Throughput of 10 Gbps and scalable up to 20Gbps for future requirements on the same appliance		
1.4		The solution should support on the box SSL inspection.		
1.5		Solution must support SSL throughput of 5 Gbps from day 1.		
1.6		The appliance should have below port density:- 1. Fixed 8 - 1G copper ports with/without fail open. 2. 4 - 10G SFP+ ports with/without internal fail open. 3. Fixed 2 - 10G SFP+ ports. 4 All the ports shall be fully populated with its transceivers only		
1.7		The appliance should have separate dedicated interface for management console. None of the monitoring ports should be used for this purpose.		
1.8		The proposed appliance must support 10,000,000 Concurrent Connections.		
1.9		The proposed appliance must support 200,000 new Connections per Second.		
1.10		The appliance must have redundant power supply		
2	**Detection Technology**			
2.1		NIPS should support different mode of deployment. a)IDS b) TAP mode c) Inline		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
35	**IPS/IDS**			
2.2		Solution must accurately detect intrusion attempts and discerns between the various types and risk levels including Zero-Day attacks, unauthorized access attempts, pre-attack probes, suspicious activity, DoS, DDoS, vulnerability exploitation, brute force, hybrids. The NIPS solution should be able to perform deep inspection of network traffic by using a combination of advanced technologies, including full protocol analysis, threat reputation and behaviour analysis to detect and protect against Zero-day attacks, malware call-backs (C&Cs), Denial of service (DoS) and other advanced threats.		
2.3		IPS Solution should have built-in SSL decryption Engine for SSL Traffic decryption to support prevention of encrypted attacks - which includes attacks over secured http channel without need to have additional appliances.		
2.4		The IPS Solution should support Anti-malware protection/propagation through various engines as part of solution offerings.		
2.5		The IPS Solution should have real time emulation techniques for embedded malware protection/propagation.		
2.6		IPS appliance should provide advanced DoS detection with self-learning/ heuristics/threshold based detection for more accurate and fewer false positives.		
2.7		The IPS must support IPv4 and Ipv6 from day-one and detect attacks inside IPv6 encapsulated packets		
2.8		IPS should provide protection from evasion based attacks		
2.9		The solution should have Anti-spoofing capabilities		
2.10		Should have capability for Host quarantine/IP blacklisting and rate limiting		
2.11		IPS must support high availabilityin Active-active.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
35	**IPS/IDS**			
2.12		IPS must support protocol tunnelling for following:- ■ IPv6 ■ V4-in-V4, V4-in-V6, V6-in-V4, and V6-in-V6 tunnels ■ MPLS ■ GRE		
2.13		NIPS should support provide advanced botnet protection using following detection methods:- ■ DNS sink holing ■ Heuristic bot detection ■ Heuristic bot detection ■ Command and control database		
2.14		Should protect against DOS/DDOS attacks. Should have learning capability to monitor the network traffic and develops a baseline profile. It should have the ability to constantly update this profile to keep an updated view of the network.:- ■ Threshold and heuristic-based detection ■ Host-based connection limiting ■		
2.15		Solution should be able to control traffic based on geographical locations -- For e.g. a policy can be created to block traffic coming or going to a particular country. Provision should be there to allow specific IPs for any blocked country		
2.16		Solution should have the capability to create Black List rules and White List rules which should allow to block or allow traffic to or from specified networks, based on protocols, applications, and other criteria.		
3	**Advanced Prevention and Response**			
3.1		IPS Solution must have capability to PRIORITIZE risk of threats to you with Campaigns detected and IP addresses that could be exposed		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
35	IPS/IDS			
3.2		Solution should provide threat intelligence feeds to provide pre-emptive protection against emerging threats along with geo/country blocking.		
3.3		IPS must support Inbound SSL Inspection detection and prevention using dynamic agent based key for ECDHA cypher suits		
3.4		IPS must have multiple signature less engines on the appliance without degrading the performance.		
3.5		Solution must have dedicated emulation engine to provide protection from advanced attacks. The IPS solution should identify malwares without the need for signatures.		
3.6		IPS must support on demand throughput scalability by just upgrading software license-Scalable on demand throughput based scalability without changing the hardware		
3.7		IPS must support Advanced Analytics, Heuristics and Machine Learning		
3.8		IPS must provide communication fabric based integration with multiple other existing solution. IPS must have the capability to share threat intelligence with other solutions enabling security intelligence and adaptive security.		
3.9		IPS must have inbuilt network behavioural analysis/protocol RFC analysis engine to provide additional context using flows.		
3.10		NIPS should support High Availability.		
3.11		NIPS should support Active-Active high availability. It should not require any third party or additional software for the same		
3.12		NIPS should be able to perform entire packet capture of the traffic and sent to the manager for analysis		
4	Management			
4.1		Solution should manage the NIPS appliances from a central management console		
4.2		Management platform supports policy configuration, command, control, and event management functions for the NIPS appliances		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
35	**IPS/IDS**			
4.3		Management console should support Radius and LDAP authentication in addition to the local user authentication		
4.4		Management console should have the ability to allow access to specific hosts by enabling GUI Access and defining the list of authorized hosts/networks		
4.5		NIPS Management console should support high availability which should have Automated failover and fail-back		
4.6		NIPS solution should provide Intelligent security management: ■ Intelligent alert prioritization ■ Robust dashboards for investigation of attacks/Robust malware investigation dashboards ■ Preconfigured investigation workflows ■ web-based management		
4.7		NIPS Management console should be capable of producing extensive graphics metric for analysis. Further, users should be able to drill down into these graphical reports to view pertinent details.		
5	**OEM Support**			
5.1		Bidders must address Problems in equipment which cause downtime/degradation of services and resolution of which require development of patches, bug fixes etc. shall be treated, by Security products OEM, on priority basis.		
5.2		Bidder must provide Schedules and performs Quarterly on-site visits; completes Protection Analysis and offers best practices recommendations.		
5.3		Bidder must provide Proactive notification of malware threat advisories and product updates		
6	**Feature Support**			
6.1		All the features asked should be available from day one and from same OEM. Any open source and third party solution is not accepted		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
35	**IPS/IDS**			
		OEM should have supplied and installed at a minimum of 5 installations with minimum throughput of 2 Gbps in each project		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
36	**PAM in HA**			
1	**Single - Sign On and Authentication Models**			
1.1		**The solution should be able to create seamless single sign-on for various technologies such as Operating Systems, Databases, Network and Security Devices.**		
1.2		The solution should have a Generic Target System Connectors to enable one to uses this connector for non-standard devices etc		
1.3		The solution should be agentless i.e. does not require to install any agent on target devices		
1.4		The solution should support transparent connection to the target device, without seeing the password or typing it in as part of the connection		
1.5		The solution should support direct connections to windows, ssh, databases and other managed devices without having to use a jump server.		
1.6		The solution should have an inbuilt dual factor authentication for soft token, mobile OTP etc. Also it should have an inbuilt authentication for Bio-Metrics without having to acquire another biometric authentication server.		
1.7		The solution should be able to integrate with enterprise authentication methods e.g. multiple 3rd party authentication methods including LDAP, RADIUS and a built-in authentication mechanism		
1.8		The solution should also provide local authentication and all the security features as per best standards.		
1.9		The solution should provide flexibility **user/device wise** for local authentication or enterprise authentication		
1.10		The solution should support an application integration framework for web based as well as .exe based applications. There should be strong out of the box support including ease of integration with any thrid party connectors.		
1.11		The solution should provide a method for creating new connectors with minimal intervention required from OEM.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
36	**PAM in HA**			
1.12		The solution should provide multi-tenancy feature whereby the entire operations can be carried out within a tenant or line of business.		
1.13		The solution should provide multi-domain feature whereby the entire operations can operate in an distributed environment		
1.14		The solution should provide features of SAML, Oauth and OIDC authentication as an identity consumer or identity provider.		
1.15		The solution should be able to handle multi-location architecture or distributed architecture with seamless integration at the User Level. For example: Multiple datacentre may have multiple secondary installations but the primary installation will also simultaneously work for all users and all locations		
2	**Shared Account Password Management**			
2.1		The solution shall perform password change options which is parameter driven		
2.2		The solution should set password options every x days, months, years and compliance options via the use of a policy		
2.3		The solution should be able to manage SSH Keys		
2.4		For Linux/Unix servers, the solution should have an option to generate the SSH key pair directly from the tool.		
2.5		Ability to create exception policies for selected systems, applications and devices		
2.6		The solution should enable an administrator to define different password formation rules for target accounts on different target systems and supports the full character set that can be used for passwords on each target system.		
2.7		The solution enables an administrator to change a target-account password to a random value based on a manual trigger or automatic schedule.		
2.8		Allow single baseline policy across all systems, applications and devcices (eg one single update to enforce baseline policy		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
36	**PAM in HA**			
2.9		The solution should support changing a password or group of passwords according to a policy (time based or 'on-demand')		
2.10		Ability to generate 'One-time' passwords as an optional workflow		
2.11		Ability to send notifications via email or other delivery methods triggered by any type of activity		
2.12		Ability to send notification via email to the user requesting the password that checkout is complete		
2.13		All locally stored target-account passwords should encrypted using AES or similar encryption with at least 256 bit keys.		
2.14		The solution should automatically reconcile passwords that are detected 'out of sync' or lost without using external restore utilities		
2.15		The solution should have the ability to reconcile passwords manually, upon demand		
2.16		The solution should automatically verify , notify and report all passwords which are not in sync with PIM		
2.17		The solution should have the ability to automatically "check-out" after a specific time and "check-in" within a specified time.		
2.18		The solution should set unique random value anytime a password is changed. The password generated should be strong and should not generate a similar value for a long iteration.		
2.19		The tool allows secure printing of passwords in Pin Mailers. Lifecycle of printing and labelling of envelopes should be part of the module.		
2.20		Secured Vault platform - main password storage repository should be highly secured (built-in firewall, hardened machine, limited and controlled remote access etc.)		
2.21		The proposed solution should restrict the solution administrators from accessing or viewing passwords or approve password requests		
2.22		The solution should have the capability to seamlessly change the passwords for the large number of desktops. It should be able to handle floating IPs		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
36	**PAM in HA**			
2.23		The solution should have provision for secure offline access of managed credentials in case of vault failure (break glass scenario)		
2.24		Offline access of managed credentials in case of vault failure should generate audit logs that are synced with the Vault once it's back online.		
2.25		3000 target systems with scalability to 10k target systems without any change in hardware is required . atleast 200 concurrent sessions are required to be supported.		
3	**Access Control**			
3.1		The solution should be able to restrict usage of critical commands over a SSH based console based on any combination of target account, group or target system and end-user.		
3.2		The solution should restrict privileged activities on a windows server (e.g. host to host jumps, cmd/telnet access, application access, tab restrictions) from session initiated with PIM		
3.3		The solution should be able to restrict usage of critical commands on command line through SSH clients on any combination of target account, group or target system and end-user.		
3.4		The solution should be able to restrict usage of critical commands on tables for database access through SSH, SQL+(client/), front-end database utilities on any combination of target account, group or target system and end-user.		
3.5		The solution should provide for inbuilt database management utility to enable granular control on database access for Sql, my Sql, DB2, Oracle etc.		
3.6		The solution enables an administrator to restrict a group of commands using a library and define custom commands for any combination of target account, group or target system and end user.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
36	**PAM in HA**			
3.7		The solution should provide secure mechanism for blacklisting/whitelisting of commands for any combination of target account, group or target system and end user.		
3.8		The solution can restrict user-specific entitlements of administrators individually or by group or role.		
3.9		The solution should have workflow control built-in for critical administrative functions over SSH including databases (example user creation, password change etc) and should be able to request for approval on the fly for those commands which are critical.		
3.10		The solution can restrict target-account-specific entitlements of end users individually or by group or role.		
3.11		The solution can restrict end-user entitlements to target accounts through a workflow by days and times of day including critical command that can be fired.		
3.12		The solution should provide for a script manager to help in access controlling scripts and allow to run the scripts on multiple devices at the same time.		
3.13		System should be able to define critical commands for alerting & monitoring purpose and also ensure user confirmation (YES or NO) for critical commands over SSH.		
3.14		It should be possible to grant access to a managed asset using a specific method of access. For e.g. access to a SQL database ONLY through SQL Management Studio.		
3.15		Solution should allow access to users while using Linux/Unix based terminal systems		
4	**Privileged Session Management and Log Management**			
4.1		The solution should be able to support a session recording on any session initiated via PIM solution including servers, network devices, databases and virtualized environments.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
36	**PAM in HA**			
4.2		The solution should be able to **log commands** for all commands fired over SSH Session and for database access through ssh, sql+		
4.3		The solution should be able to log/search text commands for all sessions of database even through the third party utilities		
4.4		The solution should be able to log/search text commands for all sessions on RDP		
4.5		The solutions should support selective option for enabling session based recording on any combination of target account, group or target system and end-user.		
4.6		All logs created by the solution should be tamper proof and should have legal hold		
4.7		The solution logs all administrator and end-user activity, including successful and failed access attempts and associated session data (date, time, IP address. Machine address, BIOS No and so on). The tool can generate — on-demand or according to an administrator-defined schedule — reports showing user activity filtered by an administrator, end user or user group.		
4.8		The tool can restrict access to different reports by administrator, group or role.		
4.9		The tool generates reports in at least the following formats: Word, CSV and PDF		
4.10		System should be able to define critical commands for alerting & monitoring purpose through SMS or Email alerts		
4.11		The solution should provide separate logs for commands and session recordings. Session recordings should be available in image/ video based formats		
4.12		The session recording should be SMART to help jump to the right session through the text logs		
4.13		Secure and tamper-proof storage for audit records, policies, entitlements, privileged credentials, recordings etc.		
4.14		The proposed solution shall cater for live monitoring of sessions and manual termination of sessions when necessary		
4.15		The proposed solution shall allow a blacklist of SQL commands that will be excluded from audit records during the session recording. All other commands will be included.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
36	**PAM in HA**			
4.16		The proposed solution shall enable users to connect securely to remote machines through the tool from their own workstations using all types of accounts, including accounts that are not managed by the privileged account management solution.		
4.17		The proposed solution shall allow configuration at platform level to allow selective recording of specific device.		
4.18		The proposed solution shall allow specific commands to be executed for RDP connections (e.g. Start the connection by launching a dedicated program on the target machine without exposing the desktop or any other executables).		
4.19		The proposed solution shall support correlated and unified auditing for shared and privileged account management and activity.		
4.20		The proposed system shall support full colour and resolution video recording.		
4.21		The proposed system shall support video session compression with no impact on video quality.		
4.22		The solution should provide a secure method to facilitate access to managed asset in case of PAM failure for identified users (local vault)		
4.23		These managed assets accessed in offline mode should generate access logs that are synced with the PAM solution once it's back online.		
4.24		The solution should provide an option to supervise privileged user activity with real time session shadowing capability.		
5	**PIM Security**			
5.1		The solutions should use minimum FIPS 140-2 validated cryptography for all data encryption.		
5.2		The Solution should be TLS 1.2 and SHA-2 compliant for PCI-DSS compliance		
5.3		All communication between system components, including components residing on the same server should be encrypted.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
36	**PAM in HA**			
5.4		All communication between the client PC and the target server should be completely encrypted using secured gateway. (Example: a telnet session is encrypted from the client PC through the secured gateway)		
5.5		The Administrator user cannot see the data (passwords) that are controlled by the solution.		
5.6		Secured platform - main password storage repository/Vault should be highly secured (hardened machine, limited and controlled remote access etc.).		
5.7		The solution should secure master data, records, entitlement, policy data and other credentials in tamper proof storage container.		
5.8		The solution should store Password and SSH keys safekeeping in the certified vault (minimum AES 256-bit encryption)		
5.9		The solution should not require direct third party access to PAM Database		
5.10		The solution should support common protocols to connect to PAM servers to ensure the best interoperability with environments.		
6	**PIM Administration**			
6.1		The solution should have central administration web based console for unified administration.		
6.2		The tool uses Active Directory/LDAP as an identity store for administrators and end users.		
6.3		The tool enables an administrator to define groups (or similar container objects) of administrators and end users.		
6.4		The tool enables an administrator to add an administrator or end user to more than one group or to add a group to more than one super group.		
6.5		The tool enables an administrator to define a hierarchy of roles without limit.		
6.6		Administrative configurations (e.g. configuration of user matrix) shall be accessible via a separate client where client access is controlled by IP address.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
36	**PAM in HA**			
6.7		Important configuration changes in the solutions (example changes to masters) should be based on at least 5 level workflow approval process and logged accordingly		
6.8		The tool should have a provision to enable maker-checker configuration for critical administrative actions. For e.g. new user creation, on-demand password change etc.		
6.9		Segregation of Duties - The Administrator user cannot view the data (passwords) that are controlled by other teams/working groups (UNIX, Oracle etc.).		
6.10		The solution should provide for self-service portal for users and devices for ease of on boarding both users and devices.		
6.11		All administrative task should be done LOB wise i.e. Line of Business Wise		
6.12		All administrative tasks/actions should be logged along with change in configuration value i.e. value before change made and after the change made.		
7	**System Architecture**			
7.1		The solution architecture should be highly scalable both vertically as well as horizontally.		
7.2		The proposed solution shall provide multi-tier architecture where the database and application level is separated.		
7.3		The solution should work at the network layer instead through a jump server. This will have achieve large number of sessions.		
7.4		The proposed solution shall provide scalability where it is not limited by the hardware. Also the solution shall provide modular design for capacity planning and scalability metrics.		
7.5		The proposed solution shall have the ability to support multiple mirrored systems at offsite Disaster Recovery Facilities across different data centre locations.		
7.6		The proposed solution shall have built-in options for backup or integration with existing backup solutions		
7.7		The proposed solution shall handle loss of connectivity to the centralized password management solution automatically.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
36	**PAM in HA**			
7.8		The proposed solution shall not require any network topology changes in order to ensure all privileged sessions are controlled by the solution.		
7.9		The proposed solution shall support distributed network architecture where different segments need to be supported from a central location.		
7.10		The proposed solution shall support both client based (in the case where browser is not available) as well as browser based administration		
7.11		The proposed solution should be 100% agentless that includes password storage, password management and session recording features.		
7.12		The solution must support parallel execution of password resets for multiple concurrent requests.		
7.13		The solution should provide fully failover from a single active instance to a backup/standby instance with a fully replicated repository		
7.14		The solution should support multiple active instances with load balancing and fully automatic failover to another active instance		
7.15		The solution if required should be available to install on a virtual sever		
7.16		The system should be highly available (24x7x365) and redundant from a hardware failure, application failure, data failure, and or catastrophic failure. Please elaborate		
7.17		The solution should have an ability to have direct connection to target device as well as using secured gateway channel.		
7.18		Solution should not require CAL license to integrate PAM		
7.19		Solution should support hybrid architecture		
8	**Out of box Integration**			

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
36	PAM in HA			
8.1		Ability to integrate with enterprise authentication methods e.g. multiple 3rd party authentication methods including AD, LDAP, Windows SSO, PKI, RADIUS and a built-in authentication mechanism.		
8.2		Ability to integrate with Bio-Metric Solutions		
8.3		Ability to integrate with Hard and Soft token solutions		
8.4		Ability to integrate with ticketing systems.		
8.5		Ability to integrate with Automation softwares for enhancing productivity in the data center		
8.6		The proposed solution supports integration with the Hardware Security Module (HSM) devices to store the encryption keys.		
9	Ticketing System integration			
9.1		The solution can force the requestor of password / session to provide a reason, including a service desk incident ticket number, for the request.		
9.2		The solution can communicate with a workflow engine to verify an incident ticket number cited in the end user's request.		
9.3		The solution provides the capability to enable end users to retrieve (or reset) a target-system password only after approval by a designated approver (to allow dual control). Approval criteria can be based on any combination of target account, group or target system and end-user identity, group or role, as well as contextual information such as day of the week or time of day.		
9.4		Ability to enforce ticketing integration as well as approval workflow for specific ticket types (e.g. change/incident ticket)		
9.5		Inbuilt ticketing system with 5 level workflow approval with ticket level validation, risk and impact assessments as per LOB wise, Service type and user type. This ticketing system to help in creating a work order on an executer, who will then request for the access through the request workflow with this valid ticket		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
36	**PAM in HA**			
10	**SIEM Integration**			
10.1		The solution should be able to integrate with leading SIEM Solutions.		
10.2		The solution should be able to integrated with applications like VA Systems, performance monitoring applications to eliminate hard coded passwords		
11	**Application Password Management (Hard-Coded Password Management)**			
11.1		The solution should have an ability to eliminate, manage and protect privileged credentials in applications, scripts, configuration files etc.		
11.2		The solution should be able to authenticate and trust the application requesting the privileged password based on various authentication methods		
11.3		Application Servers Support - The product should support removing static hard coded passwords from Data Sources in Application Servers. Please elaborate.		
12	**Auto Discovery of Privileged Accounts**			
12.1		The solution should be able to perform auto discovery of privileged accounts on target systems and perform two-way reconciliation.		
12.2		The solution should provide feature for user governance on the target devices i.e AutoDetect users and schedule a governance workflow and user certification process with adequate review process.		
12.3		Map privileged and personal accounts on various target systems		
12.4		Ability to quickly identify all non-built-in local administrator accounts in your environment (flag possible 'backdoor' accounts)		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
36	**PAM in HA**			
12.5		Ability to quickly identify private and public SSH keys, including orphaned SSH keys, on Unix/Linux machines, extracts key related data and ascertain the status of each key		
13	Notification Engine			
13.1		The solution should have capability to provide alerts and notification for critical PIM events over SMS & Email		
13.2		The solution should have capability to provide alerts and notification for all administration/configuration activities over SMS & Email		
13.3		Customizable notification for command executed on SSH and Telnet based devices		
13.4		Customizable notification for command/Process executed on Windows		
13.5		Notification on target being access on criteria like Line of Business or Groups		
13.6		Solution should have threat analytics and customised reporting capabilities		
14	Solution Workflow			
14.1		The solution should have inbuilt workflow to manage		
14.2		Electronic Approval based Password Retrieval		
14.3		Onetime access / Time Based / Permanent Access		
14.4		5 level approval workflow with E-mail and SMS notification with delegation rules		
14.5		Ability to provide for delegation at all levels in the workflow		
14.6		Mobile device support - ability to send a request to access a password, approve the request and retrieve the password, all from a hand-held mobile device e.g. smart phones		
14.7		Supports a workflow approval process that is flexible to assign multiple level of approvers based on product or model (i.e. require 2 or more approvals before access is allowed).		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
36	**PAM in HA**			
14.8		Supports a workflow approval process that requires approvers to be in sequence before final approval is granted.		
14.9		Supports a workflow approval process that requires approvers to be in sequence before final approval is granted.		
15	**Dashboard & Reporting**			
15.1		Dashboard Capabilities should include real-time view of activities performed by the administrators		
15.2		The system shall have the ability to run all reports by frequency, on-demand and schedule.		
15.3		The solution should provide detailed and scheduled reporting with the following basic report sets Entitlements Reports, User's activities, Privileged Accounts inventory and Activities log		
15.4		The solution should have ability to report on all system administrative changes performed by PIM Administrators with relevant auditable records		
15.5		The solution should be able to report password lockouts (failure logon attempts)		
15.6		Ability to report password checkouts on systems and users requesting passwords		
15.7		Ability to report password lockouts (failure logon attempts)		
15.8		Ability to report on password change following verification process		
15.9		Ability to report on password status		
15.10		Reports should be customizable		
15.11		Audit data can be exported for use for any BI Tool		
15.12		Reports shall be automatically distributed by email		
15.13		Access to audit reports (and report configuration) shall be restricted to "auditor" end-users		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
36	**PAM in HA**			
15.14		Ability to replay actual session recordings for forensic analysis		
15.15		The recorded session should be compressed and not take much space on storage and only active session has to be monitored		
15.16		Dashboard - for at a glance critical events and password policies.		
16	**UBA**			
16.1		Real time dashboard: Summary of all the alerts raised, user activity etc. on a real- time basis.		
16.2		User Analytic: Predicts user behaviour based on the activity trend. Generate alerts in case of anomalies		
16.3		Anomaly detection capabilities to spot unusual privileged activity		
16.4		Various Reports of user activities: User Activity Report, Privilege Behaviour Activity, User Watch List, Secret Event Clock, Secret Event Graph, Secret Event IP Map		
16.5		Real-time alerts for Investigation: Alerts will be sent to the Administrator/manager in case anomalies are detected		
16.6		The solution should be capable of recording all log on and log off events, including failed log on attempts.		
16.7		Ability to monitor privileged users through AI/ML for potentially harmful activity.		
17	**Brand and Technology**			
17.1		OEM Should have its own 24*7 support centre in India		
17.2		Solution must have at least 10000 active privileged user base in India		
17.3		The solution should have ISO 27001 and EAL 2 + certifications		
17.4		Solution should have been successfully implemented with government bodies.		
17.5		Solution should have been successfully implemented In India.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
36	**PAM in HA**			
17.7		The PAM solution should integrate with SCM		
17.8		OEM should have Privileged Access Manager installation & Commissioning for at least 1000 users/nodes		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
37	**L4 Load balancer in HA**			
1		Should support load balancing of 100G UDP & TCP traffic towards at least 100 Destinations IP addresses. Solution should be able to generate duplicate UDP & TCP packets to different destinations IP addresses.		
2		Each Load balancer must have minimum 4 X 100G Ports and should be fully populated with associated MPO based multimode QSFPs. Ports should be usable as 4x10G ports or 4x25G or 1x40G or 1x50G using breakout cables		
3		Should support load balancing traffic from an Sender/Source IP or Set of Sender/Source IP addresses to a group of Destinations IP addresses or End points		
4		• The solution must not have any single point of failure, including power supplies and fans.		
5		High availability should be achieved using identical make/models with the appropriate production licenses.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
37	**L4 Load balancer in HA**			
6		The system must operate in Active-Active mode.		
7		The load balancer appliance should be purpose-built hardware, specifically designed for load balancing.		
8		• The solution should have full support IPv6.		
9		• Should support multiple VLANs, LACP & Trunking of VLANs.		
10		• Should support Jumbo Frames (9600 bytes) longer frames than the standard Ethernet (IEEE 802.3) frame size of 1,518 bytes.		
11		• Should support complete STACK of Internet Protocols, i.e. IPV4, IPV6 and Dual STACK parallel.		
12		• Should support load balancing based on parameters of L3 & L4 protocols in IPV4 and IPv6 Incoming Packets		
13		• It should be a unified single box solution.		
14		• The load balancer should be able to do health check of destination server based on api, icmp, ping and should be able to load balance packet to other destinations if the destination is unhealthy.		
15		• Should be able to integrate with with TACACS+/ RADIUS/ LDAP/ ADFS for AAA		
16		• Should support transparent failover, the failover should be transparent to other networking devices and should support failover to reduce time in less than 3 second with all session's persistence without any manual intervention		
17		• Should support configuration sync to and from active and backup unit.		
18		• Should support the feature to force the active device to standby and back to active state; or force a device to offline mode.		
19		• The proposed appliance should provide minimum throughput of 80 Gbps (on single device)		
20		• The proposed appliance should support minimum 75 Million L4 concurrent connections.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
37	**L4 Load balancer in HA**			
21		• Solution should have throttling mechanism for downstream traffic - 1. Based on bandwidth - 2. Based on concurrent sessions on downstream server. 3. Based on on Load of the downstream server.		
22		• The max rate should be definable in bps, kbps, mbps and gbps. The solution should also be able to specifies the maximum amount of bandwidth that each session associated with the bandwidth control policy can use in bits per second (bps), kilobits per second (Kbps), megabits per second (Mbps), or gigabits per second (Gbps).		
23		• The solution should also be able to define a PPS based limit, where the user can define the rate in packets per second (PPS), kilo packets per second (KPPS), mega packets per second (MPPS), or giga packets per second (GPPS) this is helpful as DoS limiter		
24		• The solution should support monitoring of the Load Balancer via SNMP V1, V2, V3 and higher versions. (SNPM V3 support mandatory)		
25		• The solution should support SNMP pooling and traps.		
26		• The solution must have a web-based administration.		
27		• The solution should provide a RESTful Application Programming Interface (API).		
28		• Proposed solution should be manageable from a single management platform from the same OEM and should have provisioning to centrally manage multiple devices.		
29		• Should have a dashboard that should provide the following information along with historical view of Throughput, Connection, CPU Usage & Memory Usage		
30		• Graphs and details of the above data for the last 180 days should be available.		
31		• Should support role based admin access with roles like no access, Guest, Operator, Application Editor, Resource Administrator and Administrator.		
32		• Should have option to change the SSL certificate used for management of the appliance.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
37	**L4 Load balancer in HA**			
33		• Should have an OEM Online TAC 24x7x365 telephonic support and L3 resource support in India for onsite Support		
34		• Should support Syslog server over UDP		
35		• Bidder to provide all the components including network cables, power cables etc., that are required for the device to function properly.		
36		• All required licenses and peripherals should be included from day 1		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
38	**Anti DDOS Solution**			
1	Appliance	Anti DDOS functionalities. The solution must not be part of any UTM or NGFW or any white labelled or virtual solution running on third party hardware.		
2	Throughput	L7 Throughput or Legit Throughput : 10 Gbps		
3	Hardware Parameters	8 x 10G SFP+ from day 1. 8 x 10G SR fully populated from day one		
4	Management Port	Dedicated1 x 1G RJ45 Out-of-band Management Port and RJ45 Console Port		
5	Performance	SSL TPS 50K with RSA 2k keys or 25K TPS with ECC with SSL throughput of 10 Gbps		
6	Performance	DDOS should able to protect 2000Mbps of ISP bandwidth		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
38	**Anti DDOS Solution**			
7	DDoS features	Data should be publicly available. Must mitigate following types of attacks: DNS reflection, DNS Amplification, Floods attacks like TCP, UDP, ICMP, IGMP, ARP, Bad header floods, SMURF attack, tear drop attack, DNS caching poisoning, protocol anomalies-based attacks, DNS Tunneling attack, DNS based exploits		
8	DDoS features	Should protect UDP based attacks: UDP Flood, UDP Fragment Flood, UDP Fingerprint, Fraggle, UDP Large Packet		
9	DDoS features	Should protect HTTP & HTTPS based attacks: HTTP GET Flood, HTTP POST Flood, HTTP Slowloris, HTTP Slow POST, HTTP URL monitor, SSLHandshake, SSL Renegotiation		
10	DDoS features	Should protect DNS based attacks: DNS Cache Poisoning Defence, DNS Length Check Defense , DNS NxDomain Defence, DNS Query Flood Defence , DNS Reply Flood Defence, DNS TTL Check , DNS Source Authentication		
11	DDoS features	Zero-day attack protection by behaviour-based protection with automatic signature creation against unknown, zero day Network and DNS DDoS attacks, Full Layer 3 and Layer 4 DDOS. DDOS should prevent signature based and TPS based attacks at Network, DNS and SIP level.		
12	DDoS features	The solution should support the behaviour based DDOS mitigation.		
13	DDoS features	The solution should provide the traffic AUTO learning function for the DDOS traffic monitoring		
14	DDoS features	The traffic Auto learning threshold can be apply manually/ automatically after auto learning completed.		
15	DDoS features	The solution should provide the multi-level DDOS mitigation policy and different mitigation action based on DDOS traffic type.		
16	DDoS features	The solution should Access control list for IP, TCP, UDP, DNS, HTTP, URL, blacklist and whitelist.		
17	DDoS features	The solution should support Access control list based on inbuilt GeoIP with configurable duration.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
38	**Anti DDOS Solution**			
18	DDoS features	The solution should be able to import third party IP database through File or URL.		
19	LLB Features	Deleted		
20	LLB Features	Deleted		
21	LLB Features	Deleted		
22	LLB Features	Deleted		
23	LLB Features	Deleted		
24	IPv6 Dual Stack	The system should support IPv4 and IPv6 dual-stack without deteriorating performance		
25	High Availability	The solution shall have built-in high availability (HA).		
26	Architecture	The solution shall be able to immediately support both IPv4 and IPv6, and implements dual stack architecture.		
27	Routing	The solution shall be able to support IPv4 & IPv6 routing protocols for traffic mitigation.		
28	Management	The solution must be able to integrate with existing management system via SNMP version 3 and SNMP version 2		
29	Management	Should support High Availability.		
30	Management	The solution log shall contain the following information: Attack logging like Source IP, Destination IP, Destination Port, Group Name, Service Name, Protocol Attack Type, Action , Anomaly Count, DDoS Attack and logging to Syslog		
31	Management	The solution shall provide the flexibility of performing configuration via GUI and command base remotely.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
38	**Anti DDOS Solution**			
32	Management	The solution shall be able to export syslog to existing syslog server and SIEM system.		
33	Management	Proposed DDoS solution must be of same OEM as of hardware vendor and not a 3rd party solution integrated with hardware and supplied.		
34	Management	The solution shall be able to support user authentication based on Local Password, RADIUS & TACACS		
35	Reporting	The solution shall support the provisioning of the reports - Attack reports -top sources, targets, attack type, Attack Severity Distribution, Attack Source Region		
36	Reporting	The solution must be able to generate summary attack report of daily/weekly/monthly		
37	Reporting	The solution must provide packet capture for debugging.		
38	Reporting	The solution must support the generation of pdf reports containing the detailed statistics and graphs		
39	Reporting	The solution should provide online troubleshooting and traffic analysis.		
40	Certifications	Solutions Operating System should be tested and certified for EAL 2 / NDPP (Network Device Protection Profile)/NDcPP (Network Device collaborative Protection Profile)/ or above under Common Criteria Program for security related functions		
41	Warranty	All proposed softwares should be perpetual license from OEM.		
42	Warranty	The OEM should have a Technical Assistance Center (TAC)with India Toll Free Numbers		
43	Warranty	The OEM should have Support Centers / Service Center or 24x7x365 TAC Support.		
44	General	The document/cross reference provided by the OEM for each clause asked in the RFP must be available on a GLOBAL public domain and the proposed solution must support all technical features specified in the RFP from day 1		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
39	**Security Kiosk with CDR**			
1		The solution should be in the form of hardware kiosk.		
2		Solution should be able to scan the removable media for malwares and viruses.		
3		The removable media scanning station should be able to automatically transfer clean files to a network directory.		
4		The solution should be able to function on premises and no cloud integration should be required for any scanning functionality.		
5		The solution should be able to provide minimum 8 AV Engines.		
6		The solution should be able to support whitelisted USB Drives		
7		The solution should be able to remove/ quarantine malicious files.		
8		The solution should be able to sanitize files with content disarm & reconstruction technology supporting minimum 150 + file types		
9		The solution should be able to provide embedded built-in sandboxing capability.		
10		The solution should show users the malicious files detected.		
11		The solution should be able to support multiple removable medias like USB, SD Card, HDD, CD/DVD		
12		The solution should be able to support encrypted USB Drives		
13		The solution should be able to scan password encrypted files		
14		The solution should be able to support language localization		
15		The solution should be able to block application files by its country of origin		
16		The solution should be able to support multiple workflow. E.g. Different flow for employee / Guest		
17		The solution should have capability to allow users to select specific files or all files for scanning		
18		The solution must be managed by the same Central Management Console to manage configurations etc.		
19		Solution should be able to print/ send email reports after every scan session.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
39	**Security Kiosk with CDR**			
20		The solution should provide Active Directory and LDAP group-based administrative roles.		
21		The solution should have mechanism to validate and allow to connect removable media to Endpoints, only if media is scanned by Kiosk.		
22		The solution should also have a centralized repository that can be installed within the network from which both internal & external users can retrieve the clean files from the removable media and it should be accessible in easy to use GUI. Required server hardware/virtualization/OS to be provided to support the proposed solution. All required licenses should be factored from Day-1.		
23		The Kiosk should be able to transfer the clean files automatically to the centralized repository		
24		External users/Guests should be provided with unique code with which they can login to the centralized repository to retrieve the files		
25		Employees should be able to retrieve the files from centralized repository using the same AD account they used while scanning at the Kiosk station		
26		The centralized repository should ensure all the files are encrypted at rest with at least AES-256 Bit encryption		
27		The centralized repository should also have a scanning capability with multiple AV engines and should be able to perform periodic scan of all the files stored within the repository.		
28		The solution should have option to send files to secondary removable media		
29		The solution should be able to send email notification to administrators whenever a user scans a removable media		
30		The solution should be able to send logs to syslog server		
31		The solution should provide reports of scan sessions including the files scanned, removable media properties etc.		
32		The solution should have controls to ensure only scanned media can be used within the windows workstations		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
40	**Patch Management & Compliance Solution**			
1		The solution should meet the requirement by providing a Policy Management feature that allows to adhere to the configuration management process established at organization.		
2		The solution should meet the requirement as it allows performing on demand audit as well as scheduled audits of all the technologies on-boarded in the solution.		
3		The solution should meet the requirement as it provides real-time dashboards which provide granular information about the security configuration posture of the Organization.		
4		The solution should meet the requirement as it is flexible to audit the security configurations across private clouds, and legacy IT, and public clouds.		
5		The solution should meet the requirement as it can perform audit of the servers made available on VMware, Legacy IT including bare-metal servers and Public Clouds including AWS, Azure, Google Cloud and the IBM cloud		
6		The solution should meet the requirement by providing CIS based standards and can be customized to include DISA and NIST based standard too.		
7		The solution should meet the requirement by providing a Policy Management feature that allows to edit standard profiles to derive Organization Specific Profiles based on Organization CISO requirements		
8		The solution should meet the requirement as it enables an admin to assign specific profiles to users and assets as a part of user segregation.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
40	**Patch Management & Compliance Solution**			
9		The solution should meet the requirement as it enables admin to create organization specific profiles for various type of users, as per the requirement in line with the audit of the servers against the security configurations		
10		The solution should meet the requirement as it allows grouping of the assets, application wise and user profile can be assigned to the same.		
11		The solution should meet the requirement as it allows enrolling an asset in minimal time considering the integration with the PAM for asset on-boarding.		
12		The solution should meet the requirement as it allows to enrol an asset manually as and when required by a user with no changes in the user workflow (by users, assigned to perform asset management)		
13		The solution should meet the requirement by enabling the end user (based on assigned user role) to apply an approved security profile to a VM at the time of creation and by ensuring its compliance status by performing an on-demand audit.		
14		The solution should meet the requirement by providing a feature to configure a schedule to perform the audits of the critical asset.		
15		The solution should meet the requirement by enabling a user to perform on-demand audit of an asset		
16		The solution should meet the requirement as it allows performing the full remediation of unauthorized security configuration changes.		
17		The solution should meet the requirement as it allows performing the full remediation of unauthorized security configuration changes.		
18		The solution should meet the requirement as currently it allows uploading the exceptions manually in the system. Feature can be customized as per requirement.		
19		The solution should meet the requirement as currently it allows uploading the exceptions manually with timeframe in the system. Feature can be customized as per requirement.		
20		The solution should meet the requirement as it stores the results of the scan and remediation in MSSQL/MYSQL database.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
40	**Patch Management & Compliance Solution**			
21		The solution should meet the requirement as it provides on-demand audit ready reports documenting the state of the system at the time of all scans and remediation and change of state of the system between any two scans in items by means of Report comparison feature.		
22		The solution should meet the requirement as the tool will provide access to the API's which can be called by third party tools for performing the require remediation. For example, we can use Postman tool to satisfy this requirement. This feature is under development.		
23		The solution should meet the requirement as it is an agent-less tool and audit are performed by establishing a secured channel with the target server using the integral security component provided by HTTPS protocol.		
24		Being agent-less helps the solution to avoid any tampering in the audit data generation that may probably occur due to the presence of Malware in the target server.		
25		In addition to implementing HTTPS the solution also takes advantage of the WinRM's security components to securely initiate an audit.		
26		Further, the solution depends upon an SSL certificate for initiating an audit with the target server. The solution can only perform audit when the required SSL certificate is available in the target server. This mechanism provides additional security from audit data tampering.		
27		The solution should meet the requirement as it allows configuring MSP (multiple service provider) which allows to create multiple companies, under which multiple LOB's can be managed to segregate the users and assets.		
28		The solution allows configuring multiple gateways which communicates multiple datacentres of multiple companies/organization.		
29		The solution should meet the requirement as it is an agent-less tool		
30		The solution should meet the requirement as we can rapidly deploy the guideline updates provided by the industry bodies		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
40	**Patch Management & Compliance Solution**			
31		The solution should meet the requirement as it allows to group the assets and users as per the organization's requirement.		
32		The solution should meet the requirement as it allows applying multiple security profiles to a single server. The tool allows selecting a security profile while auditing the server. Also, the solution allows to implement on-demand remediation.		
33		The solution should meet the requirement as it allows concurrent assessment of multiple technologies, reducing the time frame required for the audit.		
34		The solution should meet the requirement as it uses a wizard based installer, which requires simple hosting and database restore.		
35		The solution should meet the requirement as it provides the required updates for the supported technologies to the organization within one month of the requirement being submitted to PAM application.		
36		The proposed solution should have an installation base of minimum 25,000 devices in India		
37		OEM should have its own 24*7 support with dedicated manpower in India		
38		The proposed solution should seamlessly integrate with PAM		
39		Required server hardware/virtualization/OS, in case needed , to be provided to support the proposed solution. All required licenses should be factored from Day-1.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
41	**Configuration Audit Tool**			
1		Automated analysis of network device configurations. Identification of misconfigurations, vulnerabilities, and compliance issues.		
2		Ability to audit configurations against industry standards and best practices.		
3		Support for multiple compliance standards, including PCI-DSS, NIST, STIGS, and others.		
4		Ability to customize compliance checks to meet specific organizational policies.		
5		Detection of security vulnerabilities in network device configurations.		
6		Risk scoring and prioritization of vulnerabilities based on impact and severity.		
7		Detailed descriptions of vulnerabilities with remediation guidance with prioritized remediation for the most critical non-compliances.		
8		Pre-built report templates for common compliance standards.		
9		Customizable report layouts to include specific data points and visualizations.		
10		Capability to generate detailed and executive summary reports.		
11		Historical data analysis to track compliance and security posture over time.		
12		Support for exporting audit results in various formats, including CSV, JSON, and XML.		
13		Should be capable to Automating accurate, on-demand router, switch and firewall configuration security assessments		
14		Should be capable to provide evidence based pass/fail compliance reporting		
15		Should be capable of Exception-based security reporting		
16		Should be capable of Remediation analysis to improve security posture		
17		Should be capable to provide Risk-prioritized view of configuration vulnerabilities		
18		Required server hardware/virtualization/OS, in case needed , to be provided to support the proposed solution. All required licenses should be factored from Day-1.		
19		Licensing required for 2000 nodes. Further it can be setup in 5 no. of instances. Instances can be increased as per requirement.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
42	**Attack Surface Management**			
1	**Solution Characteristics**			
1.1		Solution should be either a set of virtual or physical appliances and must satisfy following characteristics -		
1.2		A minimum of 4 x 1Gbps Ethernet interfaces.		
1.3		Database & Storage to support data retention for 180 days.		
1.4		A minimum of 1 x 802.11 a/b/g/n interface.		
1.5		A minimum of 1 x 802.11 ac/ax interface.		
1.6		Ability to back-up information in database/databases to external storage over the network.		
1.7		An ability to communicate with Internet Search API's for popular search engine/engines.		
2	**Deployment Options and Characteristics**			
2.1		Solution should support deployment in a data-centre environment and physically connect to multiple local network segments.		
2.2		Solution should support multipath routing and be capable of connecting to remote network segments using gateways available on any of the physically connected segments.		
2.3		Solution should be capable of automatically detecting assets present on the network segments and be able to analyze their service state, identify applications and libraries used to determine potential weaknesses without any human intervention.		
2.4		Solution should be capable of analyzing asset state irrespective of its platform, operating-system and, application used.		
2.5		Solution should support a dedicated out of band management port for configuration/management via a secure web and shell-based interface. No other traffic should be permitted to this out-of-band management port.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
42	**Attack Surface Management**			
2.6		Solution should be capable of preventing unauthorized incoming connections to the network interfaces.		
2.7		Solution should support the ability to detect unauthorized Wi-Fi access-points.		
2.8		Solution should be capable of synchronizing time with a centrally available NTP server.		
3	**Technical Specifications - Device Discovery**			
3.1		Solution should automatically identify devices on the network and perform activities pertaining to detection of weaknesses and exploitability without the need for human intervention.		
3.2		Solution should support discovery on multiple physical network segments or VLAN's.		
3.3		The assessment process should be non-intrusive and performed at regular intervals so as to maintain a near real-time state of visibility.		
3.4		Solution should support discovery of Wi-Fi enabled clients in the premise in different network segments.		
3.5		Solution may include one or more device/appliance as needed to detect Wi-Fi enabled clients in the organization's premise.		
4	**Technical Specifications - Analytics**			
4.1		Solution should be capable of discovering vulnerabilities, weaknesses and then leverage that information to identify attack vectors and likelihood of exploitability along with business impact of a compromise.		
4.2		Solution should leverage its knowledge of enterprise assets to identify devices that have connected to unsanctioned access points.		
4.3		Solution should be capable of leveraging insights from threat intelligence to ascertain which devices are likely at greater risk of compromise.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
42	Attack Surface Management			
4.4		Solution should support native integration with honeypots and decoy solutions to better detect presence of threat actors in local network and identify service, application, library, weakness being compromised or likely at risk.		
4.5		Solution should provide relevant intelligence about organization's assets that are easily available/accessible on the Internet.		
4.6		At no point, device data, services enumeration or detected vulnerabilities or weaknesses should be forwarded to a third-party entity or any threat intelligence service including the one used by the solution provider.		
5	**Technical Specifications - Artifact Discovery**			
5.1		Solution should be capable of discovering open printer/scanner interfaces, globally writeable shares and easily accessible documents that may contain sensitive information.		
5.2		Solution should be able to provide platform, operating system, applications and version history.		
5.3		Solution should periodically conduct such assessment to maintain near real-time visibility.		
6	**Technical Specifications - User Interfaces**			
6.1		The solution should be manageable using a secure web-based and secure-shell based user-interface.		
6.2		The solution should support multiple administrative and analyst users.		
6.3		The web-based user interface should support multiple dashboards to provide visibility using different views and targeted risk insights.		
6.4		When a risk is identified, the solution should provide clarity to the user about the risk, its likely business impact, relevant resource links and, guidance on mitigation.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
42	**Attack Surface Management**			
6.5		The solution should enable user to update the risk status of devices based on action-taken.		
6.6		The solution should enable user to create queries and filter relevant data.		
6.7		Solution should enable user to export data in file formats that are supported by other analytics frameworks (such as TSV, CSV etc).		
6.8		Solution should support historical timeline view of an asset's profile highlighting changes to assets configuration, platform, operating system, applications, weaknesses and risks/criticality.		
6.9		The solution should not cache user data and it should prevent the use of browser cache or any other mechanism to execute an unauthenticated/unauthorized query on the solution.		
7	**Technical Specifications - Monitoring**			
7.1		The solution should provide visual health indicators for critical components - power-supply, network-cards, CPU, RAM, Storage, Critical Processes, etc.		
7.2		The solution should support debugging and troubleshooting of various processes from the user-interface.		
7.3		The solution should be capable of raising alarms on any healt parameter misbehaving.		
8	**Technical Requirements - Integration**			
8.1		The solution should be capable of integrating with existing SIEM using standards based protocol and message formats.		
8.2		The solution should integrate with software bill of material tools to fetch relevant data and analyze risks.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
42	**Attack Surface Management**			
9	**Technical Requirements - Support & Services**			
9.1		The solution should be supplied with 5-year warranty.		
9.2		All updates, upgrades should be provided and, subscription to threat intelligence should be available during the warranty and support period.		
9.3		The OEM shall perform implementation and deployment of solution at the buyer's location.		
9.4		The OEM should provide a support escalation matrix and relevant contact information to reach to the support team.		
9.5		The OEM is responsible for driving an onsite quarterly audit of the deployment to ensure that system is functional and used optimally.		
10	**Detailed Requirements - Attack Surface Management**			
10.1		The solution should begin by profiling devices, applications, services and thereafter assess associated vulnerabilities (if any) and weaknesses.		
10.2		The solution should leverage threat intelligence and provide insights around possible ways in which a weakness/vulnerability can be exploited and how easy or difficult is for an attacker to compromise the organization's asset.		
10.3		The solution should highlight business impact arising out of a possible compromise of the affected asset.		
10.4		The solution should use its threat intelligence to determine which of the affected assets are currently (at that point in time) likely at higher risk compared to other assets so as to help prioritize remediation or patching.		
10.5		The solution should be bundled with a network decoy to provide real-time visibility into malicious insider activity.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
42	**Attack Surface Management**			
10.6		The solution should use the available information to assist the user prioritize remediation or a suitable response such as creating a user policy, a firewall rule or, any other mechanism.		
10.7		The solution should allow the administrator to view the changing state of assets in a set of summary dashboard or timeline views so as to provide a glimpse of the current state of risk and exposed attack surface along with organization's assets at greater risk of compromise.		
10.8		The solution should highlight Wi-Fi enabled devices at risk owing to their connections with unsanctioned devices.		
10.9		The solution should highlight organization's assets that are exposed to the public internet. The OEM should guide the organization on how best to handle or manage exposure beyond organization's boundaries or security control's purview.		
10.10		The solution should have an inbuilt response mechanism wherein it should be able to implement a kill-switch to disrupt network communication originating from offending nodes in the network without the need for any L2/L3 switch/router or security device integration.		
10.11		OEM should have atleast completed one project in India.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
43	**Web Proxy in HA**			
1		The Secure Web Gateway should be Hardware based, Reliable, purpose-built appliance with hardened operating system.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
43	**Web Proxy in HA**			
2		SWG appliance must have 4x10 GE SFP slots populated with multimode transceiver on each appliance from day one. All these interfaces should be available simultaneously from day one		
3		The solution should have complete license for web security, URL Filtering, Content Control inspection, Antivirus, SSL, and content inspection should be built in solution for user base from the first day in same appliance. The Solution should intercept user requests for web destinations (HTTP, HTTPs and FTP) for web security, Critical & Sensitive data upload and in-line malware scanning.		
4		The solution should provide proxy, caching, on box known malware inspection, content filtering, SSL inspection, protocol filtering, Web data leakage prevention and inline AV in block mode on the same Appliance, with application visibility and control.		
5		Proposed solution should be able to inspect malicious information leaks even over SSL by decrypting SSL natively. Solution should also provide the decryption bypass to be done for the privacy categories.		
6		The Solution should be designed in active-active mode with the appliances, managed through centralized management console on server platform.		
7		The solution should be capable of dynamically blocking a legitimate website which has become infected in real time when the threat has been removed for security categories and vulnerabilities. The solution should have ability to block anonymizer sites or proxy avoidance tools.		
8		The solution shall be able to support various form of user Authentication methods simultaneously, including: Local Database, LDAP, Windows AD, SAML, Terminal Server Agent support for Single Sign On		
9		The solution should have at least millions of websites in its URL filtering database and' should have pre-defined URL categories and application filters along with YouTube, Facebook and linked-in controls. Solution vendor should ensure that along with predefined categories from day-1, it should have ability to configure custom categories for organization.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
43	Web Proxy in HA			
10		The solution should support ICAP or API integration for third party inputs for web filtering database or threat feeds if required		
11		The solution must detect and block outbound Botnet and Trojan malware communications. The solution must log and provide detailed information on the originating system		
12		The solution should have cloud application usage and associated risk visibility and blocking the malicious cloud app.		
13		The solution should apply security policy for multiple protocols in multiple categories. This includes the ability to allow, block, log, and assign quota time for multiple security categories.		
14		The solution should have granular control over popular social web applications like Facebook, Linked in, Twitter, YouTube, and others. The solution should have social control Video uploads to Facebook and YouTube applications		
15		The solution should provide geo-location/threat information awareness for security incidents.		
16		The solution should be able to manage the complete solution through centralized management console which should be software or appliance based. Threat Dashboard feature should also be there to analyse the security risk of all the users participating the C&C and malware communication.		
17		The solution should support to have capability to differentiate between educational and entertainment videos		
18		The solution should support real time dashboard for the summary of web filtering activities. The solution should pre-built report templates which the administrator can use for generating reports.		
19		The solution should have capability to integrate to third-party SIEM applications like syslog/CEF, sys1og key-value pairs syslog LEEF or others & equivalent without any additional license.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
43	Web Proxy in HA			
20		The solution should provide native system health monitoring, alerting and troubleshooting capabilities. The solution should provide reports based on hits, and bandwidth.		
21		The Solution should have inbuilt reporting feature like real time monitoring, reporting templates and investigation drill down report.		
22		The solution must provide malware, anti-virus, anti-bot etc. scanning though inbuilt AV scanning engine in appliance.		
23		When SSL encrypted traffic from users will hit the SWG, then the proposed solution should have the capability to inspect & process that encrypted traffic with a minimum processing speed of 1 Gbps		
24		Each user traffic should hit the SWG solution when they are trying to access Internet & from day one the proposed SWG should be capable to handle minimum 40,0000 such session request from end-points on every seconds		
25		The proposed SWG solution should have a maximum capacity of keeping record for a total last 1 year at any point of time		
26				
27				
28		The SWG should support at least 250 concurrent users.,		
29		The proposed solution must be able to deliver at least 10 Gbps of throughput on full load after enabling multiple security modules together.		
30		The SWG should have both SSL/TLS Inspection capabilities		
31		The SWG shall provide role and profile based access control and should be able to map the same with Active Directory users. The solution should able to fetch the user data from Active Directory server automatically.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
43	**Web Proxy in HA**			
32		Proposed SWG must not require reboot to push security policies or any signature update.		
33		The solution should be able to ingrate with Radius/AAA/TACACS+ server for 2FA for console login		
34		The proposed system should have Web Content Filtering solution		
35		The SWG must have in-built Web Proxy functionality for HTTP/HTTPS and FTP protocols.		
36		The propose SWG system must support Transparent Web Proxy		
37		The propose unit shall be able to support the following configuration of explicit proxy: i Proxy FQDN ii Proxy Port iiiInterfaces that listen to proxy request		
38		The SWG shall allow administrators to override Web Filtering database ratings with local settings		
39				
40		The SWG must have advanced URL filtering categories to block access to Newly Registered Domains, Newly Observed/created Domains, and Dynamic DNS based websites.		
41		The SWG must have capability to filter YouTube videos by using channel ID		
42				
43				

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
43	**Web Proxy in HA**			
44				
45				
46		The proposed solution must be able to deliver at least 1 Gbps of Application inspection throughput		
47		The appliance should have at least 4000 application signatures database		
48		Should have the intelligence to identify & control of popular IM & P2P applications like Bit Torrent, Skype, You Tube, Facebook, LinkedIn etc along with VPN like Nord, OpenVPN, and Proton, Express VPN etc		
49		SWG must have capability to do Cloud application based routing not by means of manually adding IPs and or FQDNs i.e. appliance should have database of O365 readily available to select as destination address in security policy		
50		hould be able to block, allow or monitor only using AV signatures and file blocking based on per security policy based or based on authenticated user groups		
51		SWG should offer anti-virus scanning and anti-malware analysis		
52		SWG must include Anti-bot capability using IP reputation DB, terminates botnet communication to C&C servers also. Vendor needs to add additional license if it is required.		
53		SWG should allow to integrate with third party threat feed from url, http, https, Malware hash through API to STIX integration		
54				
55				
56				
57				

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
43	**Web Proxy in HA**			
58		The proposed system shall allow administrator to prevent sensitive data from leaving the network. 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. The DLP capability shall support the following protocol & activities: HTTP/HTTPS POST, HTTP/HTTPS GET		
59		The DLP capability shall be configured by creating individual rules or combining the rules into sensors, and then assigning them to profiles which in turn bind to policies		
60		The administrator shall be able to configure the following actions upon data matched:		
61		Block: prevents the traffic matching the rule from being delivered.		
62				
63		Ban: if the user is authenticated, will block all traffic to or from the user using the protocol that triggered the rule"		
64				
65		The SWG must support both Active-Passive and Active-Active High Availability options.		
66				
67		The HA solutions should support silent firmware upgrade process that ensures minimum downtime		
68		The SWG must have provision of fail-over mechanism for high availability		
69		The proposed SWG appliance should have minimum 250GB of internal or external storage capacity for storing the logs & generating reports. The centralized server proposed for log and management, at DC shall be used for all the SWGs of DC, DR and Head Office.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
43	**Web Proxy in HA**			
70		Support for Built-in Management for simple & secure management of the security appliances through integrated & Web-based GUI. All the above mentioned feature sets should be configurable through the GUI of the proposed SWG appliance.		
71				
72				
73		Should support both CLI and GUI configuration management.		
74		Solution must allow administrator to choose to login in read only or read-write mode		
75		Should capable to provide a convenient method for alerting administrators when critical events are encountered, by sending e-mail alert messages to administrator defined e-mail addresses		
76		Should have capability to provide APIs and log integration facility with other application for data exchange		
77		The solution should support advance malware detection through Sandboxing (on premise) if required in future.		
78		The solution should have capabilities to automatically deliver reports based on schedule to selected recipients.		
79		The solution should support configuring scheduled automatic backup of system configuration.		
80				
81		The OEM Warranty should include subscription & 365*24*7 Support online and onsite support with next business day.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
44	**SFTP Solution**			
1		The solution should act as a secure gateway & repository for files. It should ensure reliable, automated workflow and encryption for moving small to large files internally & externally		
2		It should provide SSL based GUI for users to exchange files		
3		The solution should be able to create separate user accounts for Employees, External Users, Guests		
4		The solution should be able define different permissions for Employees, external users & Guests		
5		The Solution should have supervisory approval creation process to review, preview supported file types before users exchange files		
6		The solution should ensure all the data at rest is encrypted with at least AES-256 Bit encryption		
7		The solution should perform regular scans to prevent malware outbreaks		
8		The solution should scan the files as soon as it is uploaded and the files should be available for download only after the security check for the files is completed		
9		The solution should be able to scan the files with at least 10 different Anti-malware engines to detect known threats		
10		The solution should have embedded sandbox to detect unknown threats		
11		The solution should be able to sanitize files using Content Disarm & Reconstruction technology to remove active components in common file types and should include but		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
44	**SFTP Solution**			
		not limited to .doc,.docx,.xls,.xlsx,.ppt,.pptx,.pdf,.jpg,.jpeg,.png, .rtf,.vsdx, htm, html, xml, xml-doc, vcs, icsbmp, tiff, svg, gif, etc.		
12		The solution should be able to scan & sanitize archive files. It should support well known file type like Zip, 7z, Jar, rar, rar5, tar, ISO, Gzip, .apk .gz .msi .tgz .tbz, bz2.		
13		It should recursively sanitize/scan embedded file in docx, pptx ,xlsx etc.		
14		It should be able to detect sensitive information in the files. It should be able to redact the sensitive information or block files containing sensitive information using Standard tempted & regular expressions		
15		The SFTP solution should be in HA.		
16		The solution should be able to send email notifications for file transfers & alerts		
17		The solution should be able to send logs to syslog server		
18		The solution should get integrated with Active Directory		
19		The solution should be able integrated using SAML for SSO		
20		The solution should provide language localization for the web console		
21		The solution can be software based or appliance based. Required server hardware/virtualization/OS, in case needed , to be provided to support the proposed solution for 96TB storage. All required licenses should be factored from Day-1.		
22		The solution should have capability to attach external storage on-prem or cloud storages for storing permanent, temporary & archived files		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
45	**SSL VPN Gateway**			
1		The appliance should be dedicated SSL VPN Gateway .It should have should have 1x1GbE port for management and 8x10 SFP+ ports Should be populated with its transceivers		
2		The appliance should have multicore CPU, 64GB RAM, 400 GB or higher HDD and dual power supply.		
3		The solution Should have dedicated hardware SSL card and should support 10 Gbps of SSL Throughput.		
4		The appliance should be capable of creating multiple virtual portals and support minimum 1000 concurrent users scalable to 5000 concurrent users on the same appliance without changing any hardware		
5		The device should support on demand provisioning of L3 VPN client, standalone and command line L3 VPN client support.		
6		The solution should support different network pools defined per user or group.		
7		The appliance should support 10 Gbps of compression throughput. This capability shall be compatible with most modern browsers, requiring no additional software.		
8		The appliance must use its own Hypervisor which should be a specialized purpose build hypervisor and NOT a commercially available hypervisor like XEN, KVM etc. It should NOT use Open Source/3rd party Network Functions.		
9		The solution should support following Authentication methods:		
10		a) Active Directory, b) LDAP , c) RADIUS ,d) Local database e) SAML f) Google O-Auth Support g) SMS		
11		The solution must provide ranking of at least 3 authentication methods for granular authentication of VPN users		
12		Appliance must support Access control options based on:- a) User and group, b) Source IP and network, c) Destination network ,e) Service/Port, f) Host name or IP address ,g) IP range, h) Subnet and domain, I) Day, date, time and range		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
45	**SSL VPN Gateway**			
13		The solution should provide comprehensive and reliable support for high availability with Active- active & active standby unit redundancy mode using standard VRRP (RFC-2338) or Equivalent for HA interconnection over network. Should support both device level and VA level High availability.		
14		The solution should provide online troubleshooting and traffic analysis tool where the administrator can take a snapshot of the config and upload it on web based diagnostic tool to check the health and vulnerability of the solution with the recommended solution provided on the knowledge base link.		
15		Solution should have access policy for MFA AD Auth + OTP using a built-in macro. Using existing backend HTTP AAA server connected to the SSL VPN to send OTPs using SMS gateway and AAA Active Directory Server configuration on the SSL VPN.		
16		The solution should also provide Step-up authentication. This feature allows a per-request policy to authenticate a user at any time during a VPN session. Per-request policy subroutine allows you to create time-limited sub sessions to allow user access to areas of an application based on a different gating criteria. the following authentication types for step-up authentication should be supported: Multi-factor authentication through Radius authentication Certificate-based authentication Password-based authentication		
17		The Solution should be able to support robust endpoint posture inspection and deny access for non-compliance endpoints. The Solution must support the following checks: * Able to perform Antivirus/Malware software checks, including checks for Enabled State, Engine & Database version, Last Scan, and Last Update of the antivirus software. * Able to perform domain check to auto connect to VPN when outside the office network. * Able to perform IP address / Geolocation check to restrict access from unwanted locations.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
45	**SSL VPN Gateway**			
		* Able to perform Operating System, Windows Registry, File or Process checks. * Able to check if mobile devices have been jailbroken.		
18		Proposed access security solution must offer granular & continuous checks to control the traffic. Security checks must be performed on per request basis instead of per session control. * Continuous posture monitoring of the devices for all user request (not session) identify the endpoints not inline to corporate security policy and must not have corporate access. * Per request-based application access instead of session-based application access.		
19		All the features asked should be available from day one and from same OEM. Any open source and third party solution is not accepted		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
46	**Enterprise Data Log Analytics Management with Application & Infrastructure Monitoring**			
1	**Platform Capabilities**	Proposed solution must be an open platform, agent based solution for infrastructure and hosts to be deployed centrally for monitoring endpoints that prevents from ransomware and malware, detects advanced threats, and arms responders with vital investigative context telemetry.		
		Proposed Solution must use the latest advancements in machine learning and AI with a powerful set of features to block unknown, polymorphic malware and ransomware to stop advanced threats with host-based behaviour analytics.		
		Proposed solution must bolster responders and analysts team efficacy by detecting threats centrally and minimizing false positives		
		Proposed solution must perform ad-hoc correlations, gather rich context with additional real time system queries along with invoking of remote response actions across distributed endpoints from centralized console.		
		Proposed solution must have capability to avert endpoint threats with signature less prevention, behaviour analytics, centralized detection, and informed response		
		Solution must have flexible licensing to adjust as per needs evolve there should be no per-endpoint restrictions or artificial data caps to limit the usage.		
		Solution must have capabilities to receive contextual alert notifications when anomalies are detected that meet certain conditions using case management or connect alerts to actions by using built-in integrations for workflow management.		
2	**Deployment, Configuration & Use case development**	Proposed solution must include data collection from 250 number of endpoints while ingesting Logs and Endpoint EDR telemetry which should be retained for 180 days for online querying. The minimum estimated data volume must be approximately 900 GB raw data ingestion per day. Any additional data must be processed without any drop or filtering.		
		Proposed solution vendor must leverage protections from their research labs and also provide access to global user community while sharing detection and protection content.		
		Solution must provide deployment choice to run fully on-prem environment with support for air gap deployment that suits our needs, all without compromising on functionality or performance.		
		Solution must secure windows, macOS, and linux systems and should have capability to stop ransomware before data is encrypted. The solution is intended to disrupt advanced threats with behavior-based prevention.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
46	**Enterprise Data Log Analytics Management with Application & Infrastructure Monitoring**			
		Proposed solution must enhance visibility by way of collecting data from every major OS and related workloads — all the way down to the kernel layer, and glean host insights with adhoc query mechanism for realtime threat response.		
		Proposed solution must also have capabilities to aggregate logs and alerts from numerous host security and IT tools to monitor host activity in the context of a holistic attack surface with turnkey integrations and related dashboards.		
		Proposed solution should be able to generate actionable alerts by continuously correlating host activity with broader environmental data.		
		Solution should provide platform to initiate hunts from anomalies spotted by prebuilt machine learning jobs.		
		Proposed solution must enable analysts to respond rapidly by empowering them with embedded context, interactive visualizations, and a easy to use terminal interface view for investigations.		
		Solution should enable security practitioners to analyse years of data, appreciably improving your security posture by way of Attack lookback for a robust security assurance.		
3	Platform Security	Solution must include native support for role-based and attribute-based access control to ensure that only those roles with access to data can see it, even for chat and question answering applications.		
		Solution must use and securely pass proprietary data over a network and between components with no data being shared to external networks or 3rd party entities		
		Proposed solution should have deployments supporting an air-gapped, private clouds, virtual machines, in an own premises environment supporting access to secure networks		
		Solution must provide users and access controls supporting at the minimum user/password, SAML, Open ID Connect, PKI, LDAP, Active directory etc.		
		Solution must provide a set of low-level REST API endpoints making it possible to check the health of a deployment, monitor its performance over time and to manage read-only mode for a deployment.		
4	Log Collection & Pipeline management	Proposed solution must have capabilities for collecting, analysing, and acting on log data from various sources including applications and infrastructure — compute, network, and storage etc.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
46	**Enterprise Data Log Analytics Management with Application & Infrastructure Monitoring**			
		Proposed solution should be able to ingest logs generated by many different systems and devices like firewalls, switches, routers, and load balancers virtual machines, platforms, windows, Linux etc.		
		Solution must provide capabilities for encrypted data transmission within the central log management platform and its components		
		Solution must ensure encrypted transmission of telemetry data in transit to the central log management system		
		Solution must collect, process and store structured, time-series event data		
		Proposed solution must allow managing Ingest pipelines that let you perform common transformations on ingested data before indexing. For example, pipelines should allow to remove fields, extract values from text, and enrich data.		
		Solution must provide a robust and reliable data collection mechanism		
		Solution must have data enrichment capability at collection and processing layer		
		Solution must have capability for customization/filtering of data collection		
		Solution must have Index time filtering or aggregation of event data for faster data retrieval and analytics		
		Proposed solution must have a centralized agent management that enables you to manage deployed Agent installations to configure and monitor agents, trigger agent binary and policy upgrades remotely etc.		
		Solution must provide robust REST API-based data collection		
	Detection & Response			
5	**Data Management**	Solution must be able to centralize environmental activity and context to enable uniform analysis with common data schema from collected endpoint Telemetry.		
		Proposed solution must allow policies to automatically manage indexed data according to our performance, resiliency, and retention requirements		
		Proposed solution must have built-in capabilities data to be rolled over, shrunk, force merged or deleted without any dependence on 3rd party tools		
		Solution must provide data isolation capabilities in a centralized log management system for logical separation		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
46	**Enterprise Data Log Analytics Management with Application & Infrastructure Monitoring**			
		Solution must have built-in features for a distributed log collection platform to handle compliance requirements		
		Solution must have detailed policy based retention capabilities for log data collected and indexed, including the logs that are not normalized		
		Solution should have built in capability that shows ingested data is correctly mapped during normalization		
		Proposed solution must provide entity risk scoring and asset criticality that help analysts detect changes in an entity's risk posture, hunt for new threats, and prioritize incident response.		
		Solution must provide policy applying log data retention templates		
6	**Deployment and Architecture flexibility**	Solution must have built in snapshot and backup/restore management		
		Solution must provide incremental backup and be able to restore data via UI.		
		Solution must have the ability to offload stored log data to third-party NAS, SAN and storage clusters		
		Solution must provide Field, index and document level access control		
		Solution must have built in functionality to monitor health and performance of the platform		
		Solution must have integration with external identity repositories for user authentication and authorization		
		Solution must provide delivery fully on-premises with air-gapped capabilities		
		Solution must have the ability to be deployed to collect logs and event data from virtual machines, containers, Kubernetes clusters etc.		
		Solution must support customisation of UI and vendor logo for brand customization		
7	**Threat Detection & Hunting**	Solution must have out of the box detection capabilities with visibility into rules logic or patterns at code level including comparison between version changes for prebuilt rules		
		Solution must provide Pre-built metric view on security events		
		Solution must have capability to create detection techniques based on aggregation and threshold of identified parameters		
		Solution must provide capability to add exceptions and customisation of rules to reduce false positive		
		Solution must have the ability to assign pre built analysis templates for the alerts		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
46	**Enterprise Data Log Analytics Management with Application & Infrastructure Monitoring**			
		Solution must have be capable of adding automatic severity scores for the generated alerts		
		Solution must provide automatic Risk scores for the generated alerts, entity, user and network data		
		Solution must provide step by step guides with the rules as best practice for Incident response workflow		
		Solution must have capability to integrate security alerts with third party systems		
		Solution must provide real time data monitoring with visualisation		
		Solution must provide retrospective data analysis with visualisation		
		Solution must have capabilities to automatically learn what activities are normal using Machine learning		
		Solution platform must support data query on historical data at speed and relevance within milliseconds.		
		Solution must be able to automatically expose unknown threats with anomaly detection powered by prebuilt ML jobs.		
		Solution must have embedded algorithms for data analysis, profiling and threat discovery		
		Solution must have an intuitive interface for data exploration and interactive analysis of data		
		Solution must include algorithms for real-time data modelling and stream anomaly detection		
		Solution must have capabilities to automatically learn what activities are normal		
		Solution must have ability to automatically detect abnormalities in the large dataset		
		Solution must have ability to stream historical events through the correlation engine and other real-time analytics		
		Solution must enable threat hunters with evidence-based hypotheses		
		Solution must provide out of box ML Based Anomaly detection models like below at the minimum:		
		a) password spraying, user enumeration, or brute force activity		
		b) Account takeover or credentialed access.		
		c) Unauthorized user activity during non-business hours.		
		d) Lateral movement when a compromised account is used		
		e) unusual user name in the authentication logs (rare Users)		
		f) suspicious login activity		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
46	**Enterprise Data Log Analytics Management with Application & Infrastructure Monitoring**			
		g) Rare and unusual errors		
		h) anomalous network activity		
		i) command-and-control, persistence mechanism, or data exfiltration activity.		
		j) unauthorized software, malware, or persistence mechanisms		
		k) Unusual network Destination: communicate with command-and-control (C2)		
		l) Denial-of-service attacks or traffic floods		
		m) Unauthorized software, malware, or persistence mechanisms.		
		n) Rare user: credentialed access or lateral movement.		
		o) Credential Harvesting: anomalous access to the metadata service by an unusual user		
		p) Unusual user context switches can be due to privilege escalation.		
		q) Unusual RDP (remote desktop protocol) user logins		
8	**Advanced Threat Detection**	Solution must have built-in endpoint detection and response capabilities using the single agent on endpoints		
		Solution must be able to collect full endpoint telemetry without any filtering		
		Solution must allow integration with asset management to populate and enrich context data during telemetry collection (asset role, location, ownership, etc.)		
		Solution must collect context data for use in correlation, enrichment, geo-tagging and reporting		
		Solution must periodically import Threat intelligence data from a trusted commercial & OSINT threat feed vendors from a TI provider API, in addition to Out of box integrations available		
		Solution must have ability to search and analyse data across collected Threat intelligence telemetry		
		Solution must have ability to search historical data for new Threat intelligence data for threat hunting		
		Solution must be able to retain and analyse historical threat intel data		
		Solution must support exporting threat indicators in structured format		
		Solution must support mapping of detection techniques to Security frameworks like MITRE ATT&CK and provide a detailed MITRE mapping view of TTP coverage at organization level		
		Solution must have threat match detection mechanism using detection on lookup with Indicators of compromise. [IOC]		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
46	**Enterprise Data Log Analytics Management with Application & Infrastructure Monitoring**			
9	Response Activities	Solution must provide functionality that lets you to query operating systems like a database supported for Linux, macOS, and Windows environments to perform real-time incident response, threat hunting, and monitoring to detect vulnerability or compliance issues.		
		Solution must provide a workspace for investigations and threat hunting adding add alerts from multiple indices to a Timeline view to facilitate advanced investigations.		
		Proposed solution must have built-in capability to use SQL to query operating systems (windows & Linux) like a database from the centralized console using the same deployed agent		
		Solution must provide prebuilt Timeline templates to Investigate endpoint, network, process, threat indicator, file-related, registry related alerts at scale		
		Solution must provide built-in case management and same should integrate and sync with external Incident management tools via a connector or web hook or API		
		Solution must provide a response console that allows you to perform response actions on an endpoint (agent deployed on affected machine) using a terminal-like interface.		
		Solution must provide response actions like isolate, release, kill-process, status, suspend-process, execute a command, upload a file etc.		
		Solution must also have integration of security alerts with external workflow or SIEM/SOAR system		
		Solution must support role-based access control for segregation of incidents and cases up to field level controls		
10	Alerting & Investigation	Solution should provide ability to detect when network interface is up or down even if the network device is up.		
		Proposed solution must have a built-in investigation tool that allows you to examine system process data according to the O.S logical event model, with processes organized by parentage and time of execution.		
		Solution should provide Analyze bandwidth utilization per user interface		
		Solution should provide Ability to choose between ports and protocols to monitor, and provide separate retention periods		
		Solution must allow to run live queries against any host with the agent deployed to access and evaluate more about the infrastructure and operating systems or attacks in progress.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
46	Enterprise Data Log Analytics Management with Application & Infrastructure Monitoring			
		Solution should provide Alert Policies Alert policies allow us to set thresholds for groups of applications with similar alerting needs.		
		Solution should provide Availability Monitoring verify customers can reach applications		
11	Reporting & Dashboards	The solution should be able to Integrate(Telemetry, Alerts & Topology) with leading network monitoring solutions		
		Solution should provide capability for Custom dashboards and reports and capability to query any data with no coding involved		
		Solution should be able to provide reports on network bandwidth Utilization reports Provide Top, Average, Max bandwidth utilization raw versus percentages.		
		Proposed Platform must provide you with several options to share saved searches, dashboards, Visualize Library visualizations in multiple formats like pdf, PNG, csv, direct link, Json etc.		
		Proposed solution must allow embedding fully interactive dashboards as an iframe on web pages.		
		Proposed solution must automatically generate PDF and CSV reports, or generate a POST URL and deliver via workflow like Email or other modes		
		Proposed solution must allow to plot the indexed or detected data on a geo-map with multiple layers and indices and present in the dashboard		
		Proposed solution must provide a robust reporting and monitoring to Track, visualize, and alert on assets. The map feature must plotting data in the form of layers via Heat map, Tiles, Vector, and geospatial data		
		Solution must provide a feature for graph analytics to enable analysts discover how items in an index are related. The graph analytics should help in a variety of applications, from fraud detection to recommendation engines		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
47	**Load balancer with WAF (ADC)**			
1		All the features asked should be available from day one. Must support high availability.		
2	General Specifications	Must support SNMP for polling of system statistics. Must support SNMP Traps for key system thresholds (specify). Must display a visual representation of authentication in the GUI. Must log all authentication events: Locally and Via syslog. Must support backup of the full system configuration via the GUI. Must support automated backup of configuration to an external location. Must support a local user database. Must have built-in tcp dump-like tool and log collecting functionality. Must support REST API for integration with 3rd party management and monitoring. Must provide detailed logs and graphs for real time and time based statistics. Must support multiple configuration files with 2 bootable partitions for better availability and easy upgrade / fall back. Must support led warning and system log alert for failure of any of the power and CPU issues The solution should support minimum 60/50 Gbps L4/L7 Throughput. The solution should support 35 Gbps SSL Bulk Encryption Throughput. The solution should support 50K TPS 2K SSL or 25K TPS ECDHE-ECDSA P-256 SSL transactions per second. The Appliance must support minimum two 40/100G SFP Slots and 8 * 10G SFP+ slots populated with 10G SR with transrecievers. The solution must be appliance based, 1U/2U rack mountable and it should be having internal redundant Power Supply from day one.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
47	**Load balancer with WAF (ADC)**			
3	Load Balancing requirements	The appliance Must support layer 2 to layer 7 load balancing. The appliance Must support server load balancing methods. Must support one arm, reverse and transparent proxy mode deployment scenarios. Must maintain server persistency. Must provide application & server health checks for well-known protocols. Must support layer4 and layer 7 load balancing for well-known protocols. Must support graceful shut down of real services. Must support content routing. Must support scripting		
4	Link Load Balancing requirements	Must support outbound Link Load Balancing. Must support outbound multi-homing Link Load Balancing.		
5	Global Server Load Balancing requirements	Must support load balancing of servers between different data centres. Must support dynamic proximity. Must support inbound Link Load Balancing. Must support cloud-based global server load balancing services. HiMust provide comprehensive and reliable support for high availability and N+1 clustering based on Stateful session failover with Active-active. & active standby unit redundancy mode.gh Availability Requirements. Must support communication link for real-time configuration synchronization. Must support floating IP address and group for Stateful failover support. Must support built in failover decision/health check conditions Must support configuration synchronization at boot time and during run time to keep consistence configuration on both units.		
6	SSL Offloading Requirements	Must provide secure online application delivery using hardware based high performance SSL acceleration. Must support certificate formats. Must support Certificate/Private Key backup/restore to/from local disk or remote TFTP server, and through Web UI. Must support self-generated CSR (Certificate Signing Request), self- signed Certificate		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
47	**Load balancer with WAF (ADC)**			
		and private key for specified host. Must support customization for SSL Error pages. Must support HTTP to HTTPS header rewrite for enhanced application delivery support. Must have end to end SSL support to act as a SSL Server and/or as SSL Client. Must support client certificate verification, CRL's (HTTP, FTP, LDAP) and OSCP protocol. Must support Elliptic Curve Diffie-Helman ciphers. Must support TLS SNI extension. Must support customizable SSL/TLS versions. Must support SSL Forward Proxy		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
47	**Load balancer with WAF (ADC)**			
7	Security and Application Acceleration	Must provide performance optimization using TCP connection multiplexing, TCP buffering. Must support IEEE 802.3ad link aggregation Must provide real time Dynamic Web Content Compression to reduce server load. Must provide selective compression for Text, HTML, XML, Java Scripts Mime types and pictures. Must provide Advanced high performance memory/packet based Web cache. Must provide support for customized cache rules including max object size, TTL objects, refresh time interval etc. Must provide detailed cache access statistics based on ip or http hosts. Must have security SYN flood protection. Must have the capability of Rate shaping & QoS Support. Must support Stateful firewall. Must support Web Application Firewall. Must support HTTP authentication. Must support IP reputation. Must support Geo-IP security for DDoS mitigation. Must support policy-based Connection limiting		
8	Certification	Solution Operating System should be tested and certified for EAL 2 / NDPP (Network Device Protection Profile)/NDcPP (Network Device collaborative Protection Profile) / under Indian Common Criteria Certification Scheme (IC3S) by STQC, MeitY, Govt. of India.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
48	**Active Directory Solution in HA**			
1	Device’s support required	2500 or higher		
2	User support	1000		
3	Hardware & Software	SI must provide desired hardware and software to meet solution requirement along with antivirus for **5 years with 200 CAL license**		
4	User Management	User life cycle management. Create, modify, move, unlock, enable/disable, delete, and restore the Single/Bulk Users without using any manual scripts. User Self Service portal to reset password and to unlock the account on their own. Delete the accounts automatically on expiry of validity period Automatically lockdown privileged accounts that are inactive for a period of time. Create privileged roles for task delegation and Audit the actions performed by these Delegates, including what action was performed on what object and when. Allow users to request access to privileged groups. Enhance security of privileged accounts by enabling multi-factor authentication. Protect privileged accounts from password attacks by enabling		
5	Computer Management	advanced password policy requirements, including a dictionary rule Create, modify, move, manage, enable/disable, delete, and restore the Single/Bulk Computers without using any manual scripts		
6	DNS Functionality	Yes		
7	Group Management	Create, modify, move and delete the Single/Bulk Groups without using any manual scripts.		
8	Group Policy Objects(GPO) Management	Create, modify, and manage the GPOs. Link the GPOs to users/Computers/Groups/OUs		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
48	**Active Directory Solution in HA**			
9	Delegation Management	Define the roles for User, Technician and Admin. Provide restricted privileges for a Technician to perform only specific tasks/roles.		
10	Administrator Management	Review-Approve facility for all admin activities. Privileged access for Users		
11	Clean up	The clean-up should be configured to run every month are as and when required to remove the users based on certain conditions and consolidated task reports to be sent to relevant stakeholders upon clean-up.		
12	Role-based access and privileged	Should be configurable with roles that can be used to delegate task to help desk technician and other department members		
13	Integration with other related systems	Yes, to achieve the required functionality such as for RBAC,DNS, etc.		
14	Backup and recovery	Facilitate backup of entire Active Directory setup including users and rights data. Automates the entire recovery process, including rebuilding the global catalogue & FSMO Role DCs. Solution should be able to restore entire forest from single console. Recovery solution must be enabled with automated backups, quick compare of backup to current values of AD to pinpoint differences, and instantly recover the desired data. Solution should be able to restore entire forest from single console.		
15	High Availability	Yes		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
49	**NAC (included AAA) Server**			
1		The solution must provide Authentication, Authorization and Accounting (AAA) services using TACACS/TACACS+, Profiling, Posturing, Guest Management from a single platform		
2		The solution should be software based (VM) or an appliance based solution. Required server hardware/virtualization/OS, in case needed , to be provided to support the proposed solution. All required licenses should be factored from Day-1.		
3		The solution should provide radius based AAA functionality		
4		The solution should authenticate and authorize users from wired, wireless & VPN network		
5		The Solution shall use Agent based approach for Desktops, Laptops, etc. and Agentless for other devices including Network Devices, Printers/Scanners, Wireless access points, etc., for detection of unauthorized access via network activities analysis from the endpoints		
6		The solution should support 802.1x authentication for domain joined devices for wired & wireless network		
7		The solution should support MAB authentication for headless devices like printers, scanners, IP phones etc.		
8		The solution should be able to block unauthenticated/rogue machine without any access to the network.		
9		The solution must support agent-based deployment should revolve around knowing “who, what, when and where” for devices and users on your network and controlling access to the data your company needs to keep secure.		
10		The solution should dynamically profile endpoints discovered on the network, based on the configured endpoint profiling policies, and automatically assign respective endpoint attributes		
11		The solution should support Deep Device Fingerprinting based on DHCP, Web Browser User Agent Identification, URL Fingerprinting, MAC Address OID		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
49	**NAC (included AAA) Server**			
		Fingerprinting and Input From External Sources Such As In-line Network Devices (Wireless Access Points, Firewalls) and Database Resources.		
12		The solution should dynamically authorize endpoints based on user group, profile & posture properties to respective vlan or network		
13		The solution shall be a vendor-agonistic solution suited for heterogeneous networks.		
14		The solution should support authentication protocols including PAP,MS-CHAP,PEAP and EAP-TLS and 802.1X Single Sign-On (SSO)		
15		The solution should be able to profile IoT /IIoT devices and assign relevant network		
16		The solution should integrate with AD/LDAP server for authentication		
17		The solution should provide wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments, URL redirect or equivalent.		
18		The Solution should support the following endpoint checks for compliance for windows endpoints -Check operating system/service packs/hotfixes . -Check process, registry, file & application . -Check for Anti-malware installation/Version/ Antimalware signature Definition Date -Check for windows update running & configuration -Check domain joined or not - Execute custom scripts - Check Vulnerable applications installed		
19		The solution should provide below Deep Compliance checks on minimum based on OESIS Framework from Day 1 on windows & mac-OS endpoints: 1) Check Specific Anti-malware product version and last signature update date 2) Threats detected by the installed Anti-malware product with option to configure threat exclusion. 3) Disk Encryption status of System & Local volume Encryption tool & its version.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
49	**NAC (included AAA) Server**			
		4) DLP application status 5) Local firewall status 6) EOL status of device operating system and last operating system update. Enforce policies based on the update availability 7) Detect Browser extensions 8) Maintain a inbuilt database of list of Potentially unwanted Application(PUA) and detect them 9) Ability to create playbooks to run specific tasks on endpoint and assign compliance status 10) Anti-phishing protection setting on default or all web browser installed		
20		The solution should provide the end user to request for temporary access in case of authentication/authorization failure that can be approved by a admin		
21		The solution shall provide self-enrolment of devices		
22		The solution should allow endpoint details to be added to a group manually or by bulk upload using csv file type		
23		The solution should provide Guest on boarding both self and sponsored		
24		The solution should allow endpoint to detect Man In the Middle (MITM) attack with/without using the agent		
25		The solution should be able to publish contextual intelligence to 3rd party devices		
26		The solution should provide threat enforcement based on the threats detected by external systems without any additional agents & quarantine the endpoints		
27		The solution should support distributed deployment options with clustering of nodes with a central management		
28		The solution should provide detail endpoint & authentication details		
29		The solution should provide role-based administrative access with dedicated roles for administrator, helpdesk operators etc.		
30		The solution should have http/SNI/VLAN proxy based remediation options		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
50	**Console Management Server**			
1		SI is responsible for overall SITC of all components of the solution which include hardware, software and accessories required for the solution to meet desired outcomes.		
2		The Solution shall be industrial-grade and comply with the following requirements: 1) Dual-core ARM Cortex-A9 MP Core with Core Sight OR Intel x86_64 multi-core 2) 1GB DDR3L RAM 3) 16GB eMMC Flash 4) 2 Gigabit Fiber SFP ports 5) Operating temperature of upto 60 degree Celcius. 6) 10/100/1000BaseT Ethernet interfaces on RJ45		
3		The equipment must support dual AC power supply and rack mountable		
4		Solution should provide secured Serial access to remote network devices over IP along with Auto-Pinout Discover and Fast configuration with Zero Touch Provisioning.		
5		The OOB equipment must support Serial (48 ports), Ethernet and SFP connections, Digital in, multiprotocol serial port.		
6		The Solution should provide combination of USB and RJ45 serial ports for target network devices		
7		The solution should support vendor agnostics and to be compatible with Serial and Ethernet connections of target devices from various network vendors.		
8		Both hardware and software components of the solution will have built-in Firewall for additional security which can restrict services to any interfaces, brute-force protection.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
50	**Console Management Server**			
9		**Console Management -** Sun break-safe (Solaris Ready Certified) Break-over SSH support Off-line data buffering – local and remote (NFS/Syslog/OEM management software) Level-based syslog filters Time stamp and rotations for data buffering Unlimited number of simultaneous sessions Simultaneous access on the same port (port sniffing) with ability to toggle Configurable event notification (e-mail, pager, SNMP trap) Customizable, global time zone support Multiple and customizable user levels of access		
10		Security – Preset security profiles–secure, moderate and open Custom security profiles X.509 SSH certificate support SSHv1 and SSHv2 Local, RADIUS, TACACS+, LDAP/AD, NIS and Kerberos authentication Two-factor authentication (RSA SecurID®) One-Time Password (OTP) authentication Local, backup-user authentication support PAP/CHAP and Extensible Authentication Protocol (EAP) authentication (for dial-up lines)		
11		Group authorization: • TACACS+, RADIUS and LDAP • Port access • Power access • Appliance privilege		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
50	**Console Management Server**			
12		IP packet and security filtering User-access lists per port System event syslog IPsec with NAT traversal support IP forwarding support Secure factory defaults Strong password enforcement		
13		**Port Access** – Directly by server name or device name CLI Command. Simultaneous Telnet and SSH access, HTTP/HTTPS		
14		**System Management** – Configuration wizard in Web for first-time users Auto-discovery for automatic deployment Command line interface (CLI) Web Management Interface (HTTP/ HTTPS) SNMP Internal temperature sensor Upgrades available on FTP site, no charge TFTP support for network boot		
15		The Solution must be able to provide remote power reset capability (reboot) of targeted devices and monitoring when integrated with IPDU (in case Switched PDU are provided)		
16		The solution must be capable of integrate with PDU major vendors		
17		The new console supplies must seamlessly integrate with existing installed Centralized Management software. Additional licenses to be considered. (No new hardware/software required).		
18		The management platform shall provide a single pane of glass, to access to any devices that is connected to it by means of secure CLI or IP access		
19		OEM or Manufacturer should be ISO 9001: 2000, ISO 14001, ISO/IEC 27001:2013 and ISO 45001 certified.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
50	**Console Management Server**			
20		Emissions, Immunity and Safety: • FCC Class A • UL & BIS • CE Class A • EN-60950 & IEC 62368-1 2nd Ed, 3rd Ed		
21				
22				
23				
24				
25		Feature Support -All the features asked should be available from day one		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
51	**Interactive Video Wall**			
1	Screen Size	55"x4		
2	Panel Technology	IPS(Inplane Switching)		
3	Back Light Type	Direct		
4	Aspect Ratio	16:09		
5	Native Resolution	1,920 X 1,080 (FHD) or High		
6	Brightness	500 nits or Higher		
7	Contrast Ratio	500,000:1		
8	Viewing Angle(H x V)	178 X 178		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
51	**Interactive Video Wall**			
9	Response Time (G to G)	8 ms		
10	Life time(Typ.)	60,000Hrs(Typ.) or High		
11	Surface Treatment (Haze)	Haze 28%		
12	Operation Hours	24Hrs		
13	Orientation	Portrait & Landscape		
14	Input Ports	HDMI -2, Audio,DP ,DVI-D,IR , RS232C , RJ45		
15	Output Ports	DP,Audio,RS232C, RJ45		
16	Bezel to Bezel (Gap)	0.88mm(0.44 Even Bezel)		
17	Special Features	Internal Memory 8GB ,Smart Calibration,Acceleration(Gyro) Sensor,BLU Sensor,Local Key Operation,Temperature Sensor,Auto Set ID,Crestron Connected,External Input Rotation,Fail over,Gapless Playback,Group Manager,HDMI-CEC,ISM Method,Local Contents Scheduling,Local Network Sync,Network Ready,No Signal Image,WebOS 4.1,Play via URL,PM mode,Pro:Idiom,RS232C Sync,Scan Inversion,Screen Rotation,Setting Data Cloning,SI Server Setting,Smart Energy Saving,SNMP,Status Mailing,Tile Mode Setting,Wake on LAN,webRTC,W/B Setting by Grey scale		
18	Operation Humidity	10 % to 80 %		
19	Operation Temperature	0 °C to 40 °C		
20	Power Supply	100-240V~, 50/60Hz		
21	Power Consumption-(Typ/Max)	200W/250W		
22	Software Compatibility	Connected Care, Super Sign Cloud, Super Sign CMS, Super Sign Control+, Super Sign WB		
23	Certifications	FCC Class "B" / CE / KC,ERP/Energy Star 8.0,, BIS		
24	Warranty	3 years		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
51	**Interactive Video Wall**			
25	**Controller -TECHNICAL SPECIFICATIONS**			
25.1	System	A configurable system to meet individual project requirements (requirements: 19" industrial Rack mount)		
25.2	Chassis	Lockable front door to protect drives		
25.3	Operating System Platform	Windows 7 / 10 - 64 bit / Win Server 20016/2019		
25.4	Processor options	Xeon / i3 / i5 / i7 / Others		
25.5	RAM	Std. 4 GB DDR3, higher on request Support up to minimum 2 HDD		
25.6	HDD	Std.: 500 GB , can be upgraded on request Dual-port Gigabit Ethernet Controller inbuilt		
25.7	Networking	Supports Add on copper/ optical fiber adapters		
25.8	RAID	RAID 0, 1, 5, 10 support		
25.9	Cooling	Forced cooling		
25.10	Indicators	LED's for HDD activity and Power status		
25.11	Input / Output support	USB/ LAN/ VGA/SERIAL SATA/IDE port		
25.12	Switches	Power On/Off and System Reset		
25.13	Monitoring options	CPU, FAN, Temperature and alarms		
25.14	Accessories	DVD +RW ,Keyboard and mouse		
25.15	Outputs	2 or higher		
25.16	Output Resolution support	DVI: 1920x1200 RGB: 2048x1536 , DP: 3840x 2160		
25.17	Universal Input Format	DVI /RGB/Component/HDMI		
25.18	Video Input Format	NTSC/ PAL/ SECAM		
25.19	Streaming Input	Hardware & Software Decoding of streaming media inputs		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
51	**Interactive Video Wall**			
25.20	Resolution Support for IP streams	4K, HD, D1, VGA, CIF & QCIF		
25.21	Format	MJPEG, MPEG-2 , MPEG-4, H.264, Custom formats		
25.22	Audio	High Definition Audio CODEC 4K / SD video / HD video / DVI / HDMI / RGBHV / VGA / Component video / HD-SDI / Streaming video / Network / RSS feed / Ticker		
25.23	Supported Input Type			
25.24	Redundancy support	Power Supply, HDD, Cooling Fan, LAN port & Controller		
25.25	Scalability	Display multiple source windows in any size, any- where on the wall		
25.26	Control functions	Brightness / contrast / saturation / Hue / Filtering/ Crop / rotate (1 + 1) Redundant AC-DC high-efficiency power		
25.27	Power Supply	supply AC Voltage 100 - 240V, 50-60Hz		
25.28	Temperature	Operating Temperature: 0° to 40°C (32° to 95°F) Non-operating Temperature: -40° to 70°C (-40° to 158°F)		
25.29	Humidity	Humidity: 10 – 90% non-condensing		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
52	**Non Smart Rack with Redundant PDU**			
1		~~A~~ Rack should be supplied with three phase 32 Amp PDU, 42U 800x1200mm (WxD)		
2		Front doors in Steel minimum (75%) perforation		
3		Rear doors in steel dual split, fully perforated		
4		The rack should be powder coated to avoid rusting and damage.		
5		Top cover with Cable entry provision		
6		Bottom Cable entry		
7		Fully reversible 19" mounting angles at front and rear		
8		Rear 19" mounting angles supplied as split pairs to allow easy adjustments for equipment of different depths.		
9		Side panels with Slam latches and Indents for improved strength and aesthetics		
10		Side panels 2000Hx1200D (set)		
11		Swing Handle with lock & Key		
12		Rear door mount Fans or Top mount Fans 230V, 90CFM 4No.s		
13		1U Cable managers 2No.s		
14		Cu Earth Rail		
15		Captive hardware pack of 20 Secure Screws		
16		Component Shelf 720mm Depth - 2 Nos		
17		Baying Kits		
18		Racks should be with all requisite accessories and parts including 1U/2U air guiding solution to be used in the network racks		
19		2 numbers of PDU (as per annexure) Metered PDU with minimum 24 sockets (C13/C19) each, Both Racks & PDU must be from same OEM For seamless integration, configuration and service support.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
52	**Non Smart Rack with Redundant PDU**			
20		Supply and installation/laying of all the required electrical cabling to the racks shall be carried out by the bidder as per standards. All accessories for successful installation of rack should be supplied by Bidder.		
21	**Technical Specifications (PDU)**			
21.1		Each rack should have 2 PDUs The 2 PDUs in each rack should have different chassis color / single black coloured chassis for identification of UPS source. Electrical rating – Input – 230V, 32A, 1 Phase, 3-meter-long input cable with Splash proof IEC60309 input plug. For all 3Ph PDU it must have the color-coded alternating outlets based on the circuit color to identify the phase and help phase balancing when used as a three phase PDU. High temperature grade, operating temperature up to 60°C.		
21.2		Output - PDU should have minimum 24 Nos. or higher; color coded outlets (Color coding w.r.t circuit breakers). PDU outlets must be of hybrid nature which can be utilized as either C13 or C19 outlet. All outlets should provide high retention to avoid accidental dislodging of power cords. The PDU outlets should meet electrical compliance and should be UL certified.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
53	KVM Console			
1		Proposed 18.5" or higher LCD console tray and 16 port IP KVM switch should be built in design Or May be separate units but must occupy only 1U space together in 19" standard rack. KVM Console should have provision to integrate with existing/deployed centralized monitoring software to monitor all KVMs.		
2		It should have 16x RJ45 port KVM switch built in at the rear side of the LCD console tray to save the U space in Rack.		
3		Both LCD console tray and the built-in KVM switch should have single/ separate power supply.		
4		Vendor should supply 16 number of KVM cableswith VGA, USB connectors.		
5		KVM cables should have LEDs to indicate Power and connection status.		
6		Built-in KVM switch should have 16 RJ45 port to connect KVM cable/dongle with CAT cable to extension at least up to 30Mt		
7		Supplied KVM cables should support Virtual media to map USB media devices to target servers remotely over TCP/IP and Smart Card(CAC).		
8		Built it KVM switch should have encryption 128-bit AES for keyboard, mouse and video signals and virtual media sessions, internal and LDAP external authentication.		
9		KVM Session should support Keyboard pass through.		
10		Built-in KVM switch should be cascaded with another KVM switch with max 30Mt CAT cable.		
11		Built-in KVM switch should have min. one VGA/DVI local console ports.		
12		LCD display should support brightness 250 cd /m2, contract ratio 1000:1 and 16.7million colors.		
13		LCD KVM console should support min. resolutions up to 1366 x 768 @ 60Hz; & KVM switch to support Local VGA up to 1920 x 1080 & Remote support up to 1600 x 1200.		
14		Operating temperature and Humidity of LCD console tray should be 0°C to 50°C and 10% to 80%		
15		LCD console tray should have 103 key keypad with number pad and touchpad.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
53	**KVM Console**			
16		It should have control buttons on the front of the monitor to adjust the characteristics of the image that is displayed.		
17		It should have two independent USB 2.0 compliant pass through ports at front/rear side.		
18		LCD console tray should be global certified by most of the agencies like UL/CE/ BSMI/ cUL/ IC/ UKCA / NOM/FCC Class A		
19		Bidder should provide two (02) Ethernet cable with each KVM. It should be noted that of each Ethernet cable should be atleast equal to the cater the distance two adjacent racks in left and two at its right side		
20		All the features asked should be available from day one		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
54	**Forensic Workstations**			
1	Processor	2x Intel Xeon 32 Core - 5th Gen or Latest, Gold, Base frequency 2.1 GHZ (minimum), Turbo 3.5Ghz (minimum)		
2	RAM	1TB 4800MHZ DDR5 ECC memory		
3	Boot Drive	1TB SSD NVMe SSD PCI Gen-4		
4	Storage	2TB SSD NVMe SSD PCI Gen-4		
5	Data Drive	5x10TB for Data in RAID 5 or 6 via RAID Controller		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
54	**Forensic Workstations**			
6	Operating System	Windows 11 Professional 64-Bit with Microsoft Office 2024 Professional License (Perpetual)		
7	Power	Maximum 1200 Watt power supply 80 Plus Gold Certified Fully Modular Power Supply		
8	GPU	NVIDIA RTX Quadro A5000/6000		
9	Networking	2 x 1G (Copper) 2x10GbE (Fiber)		
10	Forensic Bridge	Write blocked, Integrated With USB 3.0, SATA, IDE, SAS, FireWire, and PCIe Connections.		
11	Adapter kits	PCIe Card SSD adapter, PCIe M.2 SSD Adapter PCIe Adapter for Apple SSD, PCIe U.2 SSD Adapter Apple 2016+ PCIe SSD Adapter, 4" PCIe cable and Drive Adapter Kit		
12	Front Audio	2x Front Audio (Headphone and Microphone)		
13	SATA HDD Dock	1x Top Mounted SATA Dock for 3.5 & 2.5 Inch Drives		
14	Drive bay	Hot-swappable, interchangeable USB 3.1 connected drive trays 2.5" / 3.5" SATA drive tray, user selectable read/write or read only (write blocked) modes Forensic card reader tray for flash memory access, user selectable read / write or read only (write blocked) modes M.2 / NVMe PCIe SSD and M.2 SATA drive tray, user selectable read/write or read only (write blocked) modes USB 3.1 Forensic Dongle Vault with 5 USB 3.1 ports for secure (internal to tray) license dongle connections USB 3.1 hub tray, with five external USB3.1 port connections		
15	Dimensions	Maximum Width 12 inches, Height 30 inches, Depth 30 inches		
16	Keyboard	Mechanical keyboard (wired & 2.4GHZ wireless)		
17	Mouse	Optical 10,000 DPI minimum		
18	Wifi & Bluetooth	10/100/1000/2500 Mbps Ethernet LAN port.Intel WI-FI 6E AX211 M.2 + Bluetooth 5.3		
19	Warranty	Minimum 3 years Onsite OEM		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
54	**Forensic Workstations**			
20	Monitor	2x24 Inch IPS Full HD Monitor		
21	Software	Magnet Axiom Cyber Pre installed with licenses along the instructor led onsite training for 20 users.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
55	**Forensic Laptops**			
1	Processor	Intel Core i9-13th Gen HX series , 24 core, Minimum 5 GHz Turbo frequency		
2	Memory	64 GB PC5-38400 DDR5 4800 MHz		
3	Display	Minimum 15-inch UHD		
4	Operating system	Windows 11 Professional 64-Bit with Microsoft Office 2024 Professional License (Perpetual)		
5	Graphics	NVIDIA GeForce RTX 4080 GPU - 16GB GDDR6		
6	Storage	500 GB M.2 NVMe (OS), 2 TB M.2 NVMe Gen-4		
7	Write Blocked Forensic Imaging	Three UltraBlock write blockers (UltraBlock SATA/IDE, UltraBlock PCIe, UltraBlock USB 3.0), Forensic Media Card Reader, UltraBlock power supplies (2), and all required power/signal cables		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
55	**Forensic Laptops**			
8	Imaging Software	Tableau Imager (preinstalled)		
9	Charging	AC-IN 100-240V, 50-60Hz,300W minimum charger		
10	Media Card Reader	Forensic Media Card Reader – RO and RW switchable		
11	External Connections & Expansion	1 RJ-45 Port, 1 HDMI Output Port (with HDCP), 1 Mini DisplayPort 1.4, 2 USB 3.2 Gen 2 Port (Type A), 1 Thunderbolt 4 / USB 3.2 Gen 2 (Type C) DisplayPort, 1 Thunderbolt 4 (Type C), 1 2-in-1 audio (headphone output / microphone input)		
12	Adapters & Extras	Digital Intelligence SATA III to M.2 and mSATA SSD TDA7-2 M.2 SSD PCIe cable (4")		
13	Accessories	Removable 8-cell polymer battery , 99 WH minimum		
14	Hardcase	Air Tight, Water Tight, hard-sided cases with Write blocker case		
15	Technical Support	Life Time Technical Support , 3Yrs Warranty Onsite		
16	Wifi & Bluetooth	10/100/1000/2500 Mbps Ethernet LAN port.Intel WI-FI 6E AX211 M.2 + Bluetooth 5.3		
17	IR Kit	2TB 20Gbps Rugged Water-Resistant Portable SSD Forensic Card Reader, 115 in 1 Interchangeable Multipurpose Mini Screwdriver Set Magnetic Slot Wrench Bits Repair Tools Kit, Mobile, Tablet, and Laptop Premium Faraday Bags, USB to Ethernet Adapter, 256GB Dual USB Drive Type A and Type C with OTG support, 10nos Antistatic ESD Safe Static Shielding Bag with Zip Lock, Foresnsic Duplicator (Tableau) with feature to verify the integrity of the duplicated data, Trolley for Laptop and other Accessories and items with secure space for keeping items.		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
56	Fireproof Vault (200 Litres)			
1	Volume (Litres)	200 or more		
2	Type	Fire Resistant Safe, Water Proof , inner temperature remain at less than 118°C even while exposed to a flame of 1,030°C for an hour		
3	Lock type	Electronic		
4	Security	Dual Combination Mode(User Password & Mechanical Key)		
5	High Security Emergency Key	Yes(Unlock possible with mechanical keys when PIN lost)		
6	Auto Secure Mode	Yes (mechanical keys &Password)		
7	Certifications	UL Fire Rated, Conforms to UL Test Standards		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
57	Shredder Heavy Duty (for Disk)			
1		NSA/CSS listed hard drive destroyer - For effortless and time saving destruction of storage devices. With our unique Data Destruction Auditor logging system.		
2		Should allow operators to take pictures of media before and after degaussing.		
3		Destroys HDD's and SSD's		
4		Crushes a drive in only 15 Seconds		
5		32 Character LCD Display with counter		
6		Quiet, Office friendly design		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
57	**Shredder Heavy Duty (for Disk)**			
7		Easy to operate with built in safety features		
8		DIN 66399 Security Level: H-3 (HDD's) & E-1 (SSD's)		
9		Should include reporting software to capture the following details: Processing company Media serial number Degausser model and serial number Operator/Supervisor details Time and dates Pictures of media Pass/Fail results		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
58	**Degausser**			
1	Media Handling:	Standard PC, Laptop and Server 3.5", 2.5" & 1.8" Hard Drives.		
2	Longitudinal & perpendicular recording	Up to 2TB.		
3	All drive interfaces	IDE, SATA, SAS and Fibre Channel.		
4	Power Supply	220-240V 50Hz		

S. No.	**Description**	**Specification**	**Marked/ Highlighted Cross Reference of Specification with reference page no.**	**Compliance (Yes/No)**
58	**Degausser**			
5	Degaussing Force	7000 Gauss or higher		
6	Duty Cycle	20%		
7	Erasure Depth	-75dB on 1500 OE Tape, -90dB on 750 OE Tape		
8	Throughput	20 Hard drives or 40 tapes per hour typical		
9	Controls	On/Off, Security Key		
10	Indicators	On/Off Erase Field, Coil Power Supply Warning Light		

S. No.	**Description**	**Specification**	**Marked/ Highlighted Cross Reference of Specification with reference page no.**	**Compliance (Yes/No)**
59	**Heavy Duty Workstation**			
1	Processor	Intel 14th Generation Core i7 Processor or 8000-Series AMD Ryzen 7 or Higher.		
2	Cores	12 (minimum)		
3	OS	Windows 10/11 Pro with Latest Microsoft Office License (Perpetual) along with Antivirus (for 5 Years)		
4	RAM	64GB+, DDR5, 4500MHz		
5	Storage	512GB Solid State Drive (Boot) + 1TB HDD (Storage)		
6	***Monitor***	***23" inch or higher FHD IPS (1920 x 1080) Anti-Glare Narrow Border Infinity Touch/ Non-Touch Display***		
7	***Camera***	***FHD Camera in monitor***		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
59	**Heavy Duty Workstation**			
8	Ethernet	Dual 1000BASE- T Ethernet Adapter		
9	Ports	2 HDMI, 1 VGA, 2 Audio-in / out, 1 USB 2.0, 3 USB 3.0, 1 USB C		
10	CD drive	Internal CD/DVD drive		
11	Keyboard	Full size USB Keyboard (same OEM)		
12	Mouse	Two button wired USB Optical Mouse (same OEM)		
13	Headphones	Stereo USB ,Headset, Plug-and-Play USB-A, Built-in Noise-cancellation mic Adjustable Head Strap, Padded EarCushions, 360-degree Bendable mic,Tangle Free cable,Form Factor - Over Ear, On ear		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
60	**Heavy Duty Mobile Workstation Laptop**			
1	Processor	13th Generation Intel® Core™ i7 Processor or 7000-Series AMD Ryzen 7 or higher		
2	OS	Windows 11 Pro with Latest Microsoft Office License (Perpetual) along with Antivirus (for 5 Years)		
3	RAM	DDR5 32GB+, 4500MHz or above		
4	Storage	1TB+ NVME SSD		
5	Monitor	14'' inch UHD or above with Capacitive Touch screen		
6	Ethernet port	1G Ethernet port Inbuilt / With Dock		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
60	**Heavy Duty Mobile Workstation Laptop**			
7	USB Ports	USB 3, USB 2.0, USB Type-C		
8	HDMI Port	Yes		
9	Wireless	802.11ax 2x2 Wi-Fi + Bluetooth 5.0		
10	Camera	FHD Camera		
11	Speakers	Yes, In built		
12	Security	In built TPM 2.0, Finger Print Lock		
13	Battery	USB Type-C Fast Charging (60W or above), Minimum 8 Hrs backup with Standard Usage		
14	Accessories	Bag and Fast Charger (60W or above), Wireless Mouse		
15	Applications/Software(s)	Adobe Pro Perpetual License		
16	Warranty	3 years		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
61	**Business Notebook**			
1	Processor	10 core CPU (Minimum) with 10 core GPU (Minimum) Latest Generation along with Antivirus (for 5 Years)		
2	Memory	24 GB RAM Minimum		
3	Display	Minimum 14-inch , 3024x1964 resolution or higher		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
61	**Business Notebook**			
4	Operating system	Mac OS , Compatible MS-Office		
5	Storage	1TB SSD		
6	Keyboard and Trackpad	Yes, Backlit Keyboard with Touch ID		
7	Warranty	3Yrs		
8	Wifi & Bluetooth	10/100/1000/2500 Mbps Ethernet LAN port. Intel WI-FI 6E AX211 M.2 + Bluetooth 5.3		
9	Accessories	Note book bag, USB Type-C Charger 90W charger (minimum) , USB Type-C Dock with USB 3.0, HDMI, Ethernet Ports , SD Card(128 GB)		
10	Charging	Type-C Charging with 90W charger		
11	Slots	HDMI, USB4/Thunderbolt, SDXC card slot,		
12	Camera	Yes (Front Camera)		
13	Applications/Software(s)	Acrobat Pro Perpetual License		
14	Mouse	Wireless		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
62	**Portable Mobile Notebook**			
1	Processor	8 core CPU (Minimum) with 10 core GPU (Minimum) Latest Generation along with Antivirus (for 5 Years)		
2	Display	10 Inch or Above OLED		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
62	**Portable Mobile Notebook**			
3	Touch Screen Support	Yes		
4	Operating System	iPad OS		
5	Resolution	2420x1668 or higher		
6	Digitiser Pen Support	Yes		
7	Storage	256 GB +		
8	Memory	8 GB +		
9	Wifi	Wifi 6E , Dual band		
10	Accessories	Power Adapter (Minimum 20W), USB-C Charging Cable, Keyboard with touchpad attachment, Digitizer Pen/Pencil		
11	Charging port	USB-C with support for thunderbolt/USB4		
12	Front Camera	12MP or Above		
13	Rear Camera	12MP or Above		
14	Warranty	3 years		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
63	**Heavy Duty Color Printer with Supplies**			
1	Type	All In One, office Jet		
2	Device Function	Print, Copy, Scan		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
63	**Heavy Duty Color Printer with Supplies**			
3	Print Type	Colour		
4	Minimum Speed per Minute as per	Min. 25		
5	ISO/IEC 24734 in A4 Size Monochrome	Min. 25		
6	RAM	Min. 2GB		
7	Original Document Feeder Type	ADF, DADF/RADF, SPDF Or higher		
8	Scanning Feature Availability	Yes		
9	Wi-Fi	Yes		
10	Duplexing Feature Availability	Yes		
11	Networking Feature Availability	Yes		
12	Compatible OS: Win 10, Win 7	Windows 10 Pro/11		
13	Consumables Supplies	Applicable Consumables (not only limited to paper, ink/cartridges etc.)should be supplied for the duration of implementation & O&M. Should include the consumables (paper & cartridges etc) for a period of 36 months; considering 5 rim(s) of paper & 02 (two) set of all cartridges per quarter per supplied printer		
14	Warranty	3 years		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
64	**Color Printer with Supplies**			
1	**Print Resolution:**	**Color:** Up to 4800 x 1200 DP**I** **Monochrome:** Up to 1200 x 1200 DPI		
2	**Print Speed:**	**Color:** Up to 15 pages per minute (ppm) **Monochrome:** Up to 30 ppm		
3	**Monthly Duty Cycle:**	**Recommended:** Up to 3000 pages **Maximum:** Up to 30,000 pages		
4	**Paper Handling**	**Paper Formats Supported:**A4, A5, Letter, Legal, Custom sizes **Paper Capacity: Input Tray:** Up to 250 sheets **Output Tray:** Up to 30 sheets **Automatic Duplex Printing:** Yes		
5	**Connectivity**	**Wired Connections:** USB 2.0, Ethernet **Wireless Connections:** Wi-Fi, Wi-Fi Direct, Bluetooth **Mobile Printing:** Supports Apple AirPrint, Google Cloud Print, Epson iPrint		
6	**Operating System Compatibility**	**Supported OS:** Windows (various versions), macOS, Linux, iOS, Android		
7	**Dimensions and Weight**	**Dimensions (W x D x H):** 14.8 x 19.8 x 10.5 inches **Weight:** Approximately 18.5 lbs		
8	**Power Consumption**	**Power Requirements:** 100-240V **Energy Star Certified:** Yes **Power Consumption (Idle/Active):** 12W/20W		
9	**Consumables**	**Cartridge Type:** Refillable ink tanks **Yield per Ink Bottle: Black:** Up to 7,500 pages **Color:** Up to 6,000 pages (per color)		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
64	**Color Printer with Supplies**			
10	**Features**	**Control Panel**: 2.4-inch color touchscreen **Memory**: 128 MB **Scanning/Coping/Faxing**: Yes (Multifunction capabilities)		
11	**Warranty**	**Warranty Period**: 3 year		
12	Consumables Supplies	Applicable Consumables (not only limited to paper, ink/cartridges etc.)should be supplied for the duration of implementation & O&M. Should include the consumables (paper & cartridges) for a period of 36 months; considering 5 rim(s) of paper & 02 (two) set of all cartridges per quarter per supplied printer		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
65	**Miscellaneous Items**			
1		(Optical meter-5 qty., ethernet cable tester-5 qty., cramping tool-10 qty., console cable with USB to serial converter- 30qty, monitor trolly- 4 qty., USB 3.0 to ethernet converter-10 qty.,		
2		Media Converter (Fiber to Copper 1G) 20 qty,		
3		Visual Fault Locator for Patch Cords 2 qty,		
4		Cat 6 Cable (Bundle) 06 qty)		

S. No.	Description	Specification	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
66	**Any other item(s) felt necessary & essential to be quoted by bidder**			

Revised Annexure-1 (Technical Specifications) Cntd.

Part B (CAPEX – II)

S. No.	Description	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	**PATS (Physical Asset Tracking Solution) in HA**		
1	Solution should have a perpetual license & provide RU level Physical IT Asset Tracking within the RACK to optimize and keep a check on Datacenter IT inventory Tracking and audits.		
2	The system should be a RBAC (Role-based Access Control) based system with roles like read only, read-acknowledge & read-write over the application. The solution should allow 20 simultaneous (concurrent) users while performing the CPU & RAM intensive operations and a capability to support futuristic scalability requirements.		
3	It should be a web based solution deployable as a standalone on a hardware or on a VM.		
4	PAT Solution's Asset tag Features - Should be able to alert in real time, if an unauthorized movement of asset is made or an asset falls or there is an attempt to remove or forceful removal of tag from asset or has a low battery or in case any physical tampering is made to asset tag pasted on the asset or any physical tampering is made in between physical connectivity between asset tag to its asset tag locator module/strip or any tampering(physical/software level) tampering is made to solution. Specifically in case of wired solution, the asset tag connector should be able to capture accidental / intentional physical damage to the connecting cable (by detecting continuity		

S. No.	Description	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	**PATS (Physical Asset Tracking Solution) in HA**		
	tracing or other means), thereby clearly differentiating forceful removal of asset tags & cable/cord cutting incidents.		
5	PATS should be able to collect the information of IT assets and upload to a central database server provide Near Real time monitoring & tracking of the assets location up to rack level & precise RU Level via asset tags. It should be able to notify / alert the user(s) if an asset is added, moved, removed in an authorized or unauthorized manner from a U position in a RACK. For completeness & compactness of the solution, the Live Asset Tracker is also required to be integrated to EMS & IT Helpdesk. In case, it uses any other hardware in between (such as communication Gateways/Asset Locator Strip etc.) to communicate / integrate with EMS & IT Helpdesk, it should use encrypted communication techniques		
6	Communication mechanism in PATS should be wireless/wired in nature. The solution shouldn't use 2.4/5Ghz bands (Wi-Fi/ Bluetooth) and instead use Sub Ghz bands or wired connection. This will be responsibility of the bidder that frequencies used in this solution should not interfere with any of the supplied equipment frequency or hamper any of their operations.		

S. No.	Description	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	**PATS (Physical Asset Tracking Solution) in HA**		
7	PATS's Asset Tag form factor & mounting - Form factor of asset tags should be tamper proof & small enough to be able to easily & strongly attach to a IT asset but it should also be noticeable to naked eye. Should not be more than 86mm x 50mm x10mm with enclosure. Asset Tags / Solution should be operatable within 0 °C to +70 °C & Operating Humidity levels < 95% RH non-condensing . The tags should be tough(applicable for wireless tags), impact resistant and temperature stable		
8	PATS's Asset tag battery Life - Their battery should have Operational Life for at least 2 years from date of acceptance of the solution. In case the battery life of tag is less than 2 years, SI shall provide the battery replacements until 2 years (from the date of acceptance) duration for each of the supplied tags. (if applicable)		
9	PATS's Alarms & Notification from the Asset Solution- Solution should be able to provide real Time alarm & event notification. Should be able to Generate Alert in at least the following conditions: Addition & removal of Asset , movement of Asset from a RACK, Cage area, Store Room, Floor & DC/DR , Falling of an asset or there is an attempt to remove asset or a forceful removal of tag from asset or a physical / software level tampering is done to asset tag / asset tag solution's supplied accessories or if an asset tag has a low battery & needs battery replacement(wherever applicable) . Accordingly to the locations defined (such as RACK, Cage area, Store Room, Floor , DC,DR etc.) bidder may ascertain & accordingly include the number of Communication Gateways / locator modules required)		

S. No.	Description	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	**PATS (Physical Asset Tracking Solution) in HA**		
	RFID Asset Management solution should support tracking of assets on both front & rear side of the racks.		
10	In case of wired solution, PATS's Asset tag should not operate with batteries but should consume power from asset tracking hardware's power train.		
11	Assets Tags in PATS should have a 2D barcode/ QR Code to allow ease of configuration in PATS or physical audits. Supplied Handheld Tag readers should be able to read, configure barcode/ QR Code uniquely to an asset in PATS and save the information into the system about the asset. It should be compatible and integrated with the solution.		
12	The bidder is also required to provide two numbers of compatible 2D barcode / QR code printer along with consumables (Cartridge, DK Rolls stick able labels etc.) for2 year's duration. The Printer should have at least 300dpi printing resolution. Should support DK Rolls (DK die cut labels / DK Continuous Tape).		
13	The SI needs to also budget for ***a mandatorily replacement of battery*** (as a preventative maintenance of all asset tags with fresh battery in the last quarter of 2rd year of O&M. (if applicable)		
14	PATS's Built in Local Indicator on Tags/Rack level strips - All asset tags/ Strips should have in-built indicators to reflect working status / Asset placement status		
15	PATS's Asset solution should support TLS & SSL, adheres to FIPS, access is protected through username & password. The OEM needs to provide an undertaking for FIPS adherence.		
16	PATS's should have RoHS Certification		
17	PATS's should have Capability -Locate IT asset accurately with Rack Level & RU Level Accuracy		

S. No.	Description	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	**PATS (Physical Asset Tracking Solution) in HA**		
18	PATS's Battery (if applicable) in Asset tags must also be replaceable in nature & Tags should be reconfigurable/re-writeable		
19	PATS's Asset solution should have Scalability - System should support minimum of 2000 tags in an area of 30,000 sqft.		
20	PATS's Inventory Management module should be able to manage assets inventory as individual or bulk items, set re-order levels and amounts and keep a history of transactions. Able to provide ability to account for assets and components in inventory and facilitates maintaining appropriate levels of stock.		
21	PATS's Inventory management module should record OEM, Make, Model, Serial Number, Contract Details, Maintenance Details and link/maintain it in DB to each asset. User should be allowed to search the records/inventory based on any of fields / attributes.		
22	The system should allow to generate the reports containing inventory details as mentioned above and including the other details such as current assigned IP, device type, device name, location, RACK etc. Reports should include the available space, used space per rack. This report needs to be in PDF format; Otherwise Reports need to be available in pdf format, csv, excel . The html format of report is optional.		
23	Asset record detail: Provide a general tab that stores specific information about the device depending on the device type.		
24	Provide a Components tab that stores sub-components information of the asset, E.g. ID, Serial Number, Licenses, Version, Status, Category, Type, Item, etc. and also should support in SLA management , assist in a Help Desk call.		

S. No.	Description	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	**PATS (Physical Asset Tracking Solution) in HA**		
25	Provide a tab that stores information about different types of contracts and helps in Support, Warranty, Software, Maintenance , SLA, EoL, EoS etc.		
26	Provide a tab / column that stores custom fields per asset such as individuals or groups who are owners and users of the asset.		
27	Should be able to provide the asset's inventory details such as U Level location of Asset, rack, IP details (where ever applicable). It should support both IPv4 and IPv6 stack.		
28	Integration with EMS using REST APIs/SNMP / Non-Properitary Interfaces		
29	The software solution supplied to manage and monitor the U level Physical IT Assets Tracking, should be able to work as a standalone solution as well & should get integrated withEMS.		
30	The system should be integrated with IT Helpdesk solution, AAA / AD proposed by the SI.		
31	The solution must be an integrated solution with IT helpdesk, Change Management & EMS, so as e.g. movement of asset can be authorized change request, whose time taken for a change may be tracked via the Helpdesk manager.		
32	PATS's Integration - Should integrate with EMS, Helpdesk/Service Management & Change Management etc. modules of the system for several of its features such as authorization process of movement of an asset, raising alarms for unauthorized access/movement / tracking the assets.		
33	E.g. If there was a request to move an asset from a RACK To another RACK in the IT Helpdesk system, this will be tracked via a ticket/service desk ticket. Any change needs to undergo via change management workflow, which means this request		

S. No.	Description	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	**PATS (Physical Asset Tracking Solution) in HA**		
	will be reviewed and approved by different users. Upon approvals a change becomes an authorized change.		
34	Similarly, if there is an alarm that arises in Wired/Wireless Asset Tag due to movement of an asset, this alarm must be sent to EMS. An alarm in EMS will auto raise a ticket in IT helpdesk (based on certain criteria). The ticket may be closed by a user by referring / adding remarks to the ticket id w.r.t a ticket generated for authorized movement of asset as above. The alarm may be also acknowledged with this ticket id.		
35	The bidder needs to create such processes and perform similar integrations		
36	Data Integration - proposed solution should be able to route the data to EMS e.g. Alarm generated via an unauthorized movement of asset should be sent to EMS or any other alarm generated w.r.t Asset Management Functionality should be seen in EMS.		
37	Deployment Mode of the overall Solution: The PATS software module /Application(s) provided should be capable to be deployed on physical server and/or on virtual servers. It should run in HA mode with hardware level redundancy i.e. different physical servers.		
38	Updating of Patches, Bug Fixes within support period, upgradation of version during the support period is the joint responsibility of the OEM & SI. They must ensure to update the patches or provision the upgrades via the non-internet modes i.e. by following local update/upgrade mechanisms using HDDs/USBs .		

S. No.	Description	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	**PATS (Physical Asset Tracking Solution) in HA**		
39	The proposed solution should include hardware(s) and software(s) (including web application stack, database, any servers, any other relevant software etc. required for accomplishing the scope of work and requirements) with operating system(s). Bidders must keep in mind the future and scalability of requirements before deciding for a hardware configuration, preferably 25%-30% additional computing. 1. Also, the sizing of the computing in the proposed hardware should be sufficient enough to cater to futuristic projection of IT & Non-IT equipment mentioned in this bid. 2. Moreover, the specifications of the proposed computing hardware must be chosen so as to ensure that only 60% of the CPU and RAM are utilized at any point in time. In case a higher CPU / RAM than this defined threshold is observed for more than 60 seconds, the bidder shall upgrade/replace (with higher specifications) the hardware within 31 working days. Otherwise, equipment will be considered down and SLA/Penalty will be applicable. 3. The proposed hardware must be scalable in future for capacity upto 25%-30% from existing capacity.		
40	The proposed solutions/Modules for the sought requirements should be able to run on latest versions of Microsoft windows and Linux operating systems. All the updates and upgrades of the proposed solutions/Modules must also be supported on the upgraded / updated versions of OS during the entire contract period. The bidder also needs to provide the relevant software to ensure security of the provided hardware, software/ system.		

S. No.	Description	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	**PATS (Physical Asset Tracking Solution) in HA**		
41	The proposed solution should provide a secured console for asset monitoring. It may be noted that the live asset tracking is not required at remote location, Asset inventory should tracked and audited manually by SI as a scope of work.		
42	Proposed solution should provide current and historical reports for various statistics monitored. The solution must also allow for generation of customized reports in addition to default reports as per templates. System should be able to generate the current alarm/assets etc. reports for entire inventory or per device basis. Reports should allowed to be generated for the historical data with custom time period. Should allow sending out (emailing) of all types of reports on custom schedule such as daily, weekly, monthly basis etc. Reports should be allowed to be generated in various templates such as excel, csv, pdf etc.		
43	The SI is required to provide a clean VAPT report of the complete solution at the time of acceptance testing, where all categories of vulnerabilities are fixed in the deployed solution. Additionally, periodic VAPTs must be done as per sought in VAPT schedule.		
44	Integration of Wired or Wireless PATS (including its asset tags), EMS should be the joint responsibility of EMS OEM and bidder		
45	OEM**(s)** should be ISO 9001, ISO 14001, ISO 27001 certified.		
46	OEM should have atleast 01 project i.e. one Purchase Order / Commissioning(s) Certificate of PAT Solution with atleast 1000 nodes in a Project / a successful DCIM / PAT Solution integration experience with atleast 1000 nodes in a single Project .		

2	**Enterprise Management System with NMS in HA**
S. No.	**Description**
1	**General Requirements**
2	It should be a comprehensive SSL 256 bit secure web based IPv4 and IPv6 compliant solution, consisting of all standard features / modules of Enterprise Management Solution (EMS) such as fault management, performance management, configuration management, event management, an IT helpdesk / service desk to perform SLA management , Configuration Management Database(CMDB) ,incident, problem, document / knowledge management, asset management , IP address Management & Switch Port Management and has a inbuilt syslog server / capability to integrate a syslog server / or an integrated syslog server, so as to act as a sysLog aggregator.
3	EMS solution (including its various modules) should provide traffic analysis, service management & their respective functionality on all the Non IT and IT (network and server) infrastructure procured and/or deployed at different physical locations defined in scope of project.
4	The complete solution should have a perpetual license.
5	The proposed EMS solution and all modules (e.g. Configuration Management, network monitoring, server monitoring, asset management, IT Helpdesk, Change Management etc.) must be from a single OEM to fulfill the sought requirements & functionality. The final EMS solution with IPAM & Switch Port Management may be an integration of OEMs to fulfill the sought requirements. In case the IPAM solution is from other OEM(than EMS's OEM), the EMS OEM holds the responsibility along with bidder to accomplish the end to end integrated requirements of IPAM in EMS. Bidder holds the responsibility to ensure of testing the functionality of these components/modules before proposing a solution in the bid.
6	The proposed solution should be able to manage and monitor all the devices mentioned & planned as per requirements and scope of project.
7	Solution OEM(s) should have a development/development support center in India to facilitate quick issue / bug resolution/ any custom requests and upgrades. EMS Solution should be a GUI based support portal with all features mentioned in EMS Specifications

2	Enterprise Management System with NMS in HA
S. No.	**Description**
8	Proposed solution must provide role based access for each user / user groups. The access & privileges of users/user groups should be possible on per module/application basis. The users/user group's access should be possible on features within the modules/applications on Read only or Read-Write basis per feature.
9	The role based read/read-write privileged user /user groups should also be possible for various solution module(s) sought, device level groups (network groups, server groups etc.)
10	The RBAC (Role-based Access Control) system with fine control over access and restrictions on system elements/modules/functionality should be supported for all the supplied modules/applications. The module/application UI should support in provisioning the operators to configure these settings via an administrative login.
11	Integration: The system should be ready for AAA and AD based integration to support these features. Bidder must do the AAA and LDAP integration as a part of scope of work for achieving this role based requirements and AAA integration for authentication between EMS and Network devices must be performed prior to acceptance.
12	The users should have same login credentials to access these various modules while navigating across the solution. The access to various modules should be dependent upon privileges defined per user per module.
13	The proposed solution should include hardware(s) and software(s) (including web application stack, database, any servers etc. required for accomplishing the scope of work and requirements) with operating system(s). Bidders must keep in mind the future and scalability of requirements before deciding for a hardware configuration.
14	a. Also, the sizing of the computing in the proposed hardware should be sufficient enough to cater to futuristic projection of IT/Non-IT equipment mentioned in this bid.
15	b. Moreover, the specifications of the proposed computing hardware must be chosen so as to ensure that only 70% of the CPU and RAM are utilized at any point in time. In case a higher CPU / RAM than this defined threshold is observed for more than an aggregated 60 minutes per day, the bidder shall upgrade/replace (with higher specifications) the hardware within 31 working days. Otherwise, equipment will be considered down and SLA/Penalty will be applicable.
16	c. The solution should be able to manage devices sought in BoM from Day1 and should be scalable upto 25% of the sought devices without any hardware change.
17	d. The proposed solution (hardware+software) must be scalable in future. The application should be 64-Bit Application and run on 64-bit architecture.
18	Note: However, it may be noted by bidder before proposing the solution that no server or any other hardware is allowed to kept at remote locations for monitoring or management i.e. w.r.t EMS.

2	**Enterprise Management System with NMS in HA**
S. No.	**Description**
19	The overall solution should be provided in local High Availability mode. There should be seamless automatic successful switchover/handover (in failure cases) between the two instances. The each instance of applications / modules should execute at different physical servers. The servers should be of industry standard and data center compatible. Instances at DC shall be able to monitor and manage DC / DR &/or Remote Sites. Instances at DR shall be able to monitor and manage DR / DC &/or Remote Sites. When the DC instances are down / don't have MPLS connectivity at DC ; DR instances should be able to manage & monitor Remote Sites; Data generated/updated during this period at DR should be able to synced up to DC. & Vice Versa is applicable when DR connectivity is down. Each instance should be able to manage & monitor complete infrastructure at DC / DR &/or Remote Locations. Remote Sites shouldn't go unmonitored .
20	SI must ensure the sync of all relevant data amongst the different data bases of the instances. SI to adhere the RPO & RTO defined.
21	The SI & OEM must budget to ensure to sync the delta (i.e. changed part) everytime to maintain whole database sync.
22	It must be noted that HA is provided on two instances running on different physical servers , SI must ensure :
23	The solution should be deployed in High Availability within DC and DR both. In total there will be 4 instances of EMS will be deployed.
24	The bidder should deploy the EMS in consultation with OEM with Industry best practices.
25	• SI must create Standard operating procedure document for (if required) replicating the data (from all of the supplied modules) from DC to DR on regular basis with a periodicity allowed to be defined (between 30min to 5 days).
26	Note1: Each instance of the application provided e.g. One instance of the EMS solution while working in HA mode (as an example) should be able to manage and monitor the 100% of the infrastructure (mentioned above i.e. all Infra at DC, DR & remote locations irrespective of its location of execution on a physical server.
27	Note 2: Bidder may propose an alternate design / solution in combination full-filling the sought requirements, if required. SI may add any other third party components (such as a backup solution etc.) to achieve this requirement.
28	The solution should allow 100 simultaneous (concurrent) users while performing the CPU & RAM intensive operations and a capability to support futuristic scalability requirements.
29	The OEM/OEM(s) should have their own IP rights on the solution being supplied, so as any customization required in solution may be possible by them. This will include integration with third-party Non-EMS / EMS applications over REST APIs /any other interface. The integration should be bi-directional in nature.
30	Should have the Asset management module which should be able to manage the all IT devices and Non IT devices. This asset management solution should be a comprehensive solution that allows to manage all devices as assets.

2	**Enterprise Management System with NMS in HA**
S. No.	**Description**
31	The solution should be accessible via the intranet and internet in the secured manner. However, the solution i.e. any of the modules should not connect to Internet for accomplishing any required features asked in this solution e.g. fetching geo-maps for any functionality, and not even for the updates / upgrades etc. It should have in-built or capability to use custom maps as background and the updates/upgrades of the solution should be possible via non-internet mechanisms.
32	Solution be bundled with Data base Encryption & Documents encryption and decryption using AES 256 bit cipher.
33	The solution should only be accessed by any browser supporting SSL 128 bit / SSL 256 bit encryption ciphers .The solution must have in-built AES 256bit encryption for monitoring data and session within the platform.
34	Deployment Mode of the Solution: The Module / Application provided should be capable to be deployed on physical server and/ or a virtual server.
35	Solution should be OEM agnostic & should by default support integration with major OEMs of Network and server equipment and natively support SNMPv3 for other devices.
36	**Enterprise Management Solution (EMS) Specs**
37	The solution should support monitoring of devices preferably via agentless mechanism. The scenarios which are not supported via agentless mechanism should be covered via agent. For such scenarios permission should be sought before deploying any agent. The agent or agent less communication should be secured.
38	The EMS solution should support REST API to integrate with 3rd party solutions.
39	Should provide Network performance monitoring (NPM) via reports and dashboards. It should support the reporting, status, threshold breach reports for all monitoring parameters for servers, Network elements. It should have features for proactive monitoring of network performance.
40	Additionally, the diagnostics module of EMS should support ping check, telnet or ssh access, traceroute route checking and Device logs analysis.
41	The proposed solutions/Modules for the sought requirements should be able to run on latest versions of Microsoft windows or linux operating systems. All the updates and upgrades of the proposed solutions/Modules must also be supported on the upgraded / updated versions of OS during the entire contract period.
42	In case of any updates/upgrades of base OS, the supplied solution(s) must be updated/upgraded free of cost during the entire contract period. Also any bug fixes within support period must be supported.

2	Enterprise Management System with NMS in HA
S. No.	**Description**
43	SI must ensure to update the patches or provision the upgrades via the non-internet modes i.e. by following local update/upgrade mechanisms using HDDs/USBs.
44	Should allow & perform integration with other third-party applications (such as AIM, PATS etc.) through REST APIs. It must be ensured that all alarms arising out of any module of the solution should be sent to EMS and its database. E.g. If there is an alarm that arises in PATS, it must be sent to EMS. The EMS must serve as an all alarm and event data base.
45	Also, there should be a provision for Northbound and Southbound Integration Adaptors, gateways or CLI based integration for seamless integration and customization possibilities.
46	System should have Node Tags for device grouping and resource/interface tagging for element grouping. Apart from Node Tags additionally system should have options to do device grouping based on default fields and customer fields. No restriction in the number of level of grouping for the devices. Provides the option to create the grouping based on the service offered to customer and map all the devices involved in the specific service till the component / resource level. It may be noted that "node tags" refer to - a tag whereby devices having similar characteristics can be grouped inside it for the devices at DC, DR and Remote locations.
47	The current performance state of the entire network & system infrastructure shall be visible in an integrated console of proposed solution
48	It should provide a secured single login with unified console for seamless cross-functional navigation for all functions of components/modules offered across multiple areas of monitoring & management.
49	Should be able to monitor network traffic by capturing flow data from network devices, such as but not limited to Cisco NetFlow v5 or v9, Juniper J-Flow, IPFIX, sFlow, sampled NetFlow data and Cisco ASA NetFlow.
50	Should support Network device or configuration management by supporting with Automated Backups of configurations, Change management in Real-Time, Allow execution of special Scripts (e.g execute sequence of commands in different devices for troubleshooting & creation of such scripts) , Compliance auditing & Automation of repetitive configuration management tasks .
51	The scripts should be allowed to run on single NE or can be issued in bulk on different set of NEs.
52	The scripts may be used for upgrading the Firmware in NEs.
53	Additionally, the scripts functionality may be used for changing configurations, running and executing commands for troubleshooting or, so as it can automate configuration management, device management etc. by giving convenience to an operator / user for executing self-created scripts.
54	Should also provide a feature of Remote Firmware upgrade on single or bulk devices

2	Enterprise Management System with NMS in HA
S. No.	**Description**
55	Should monitor hardware and software health for Data Center Network & Server Equipment and should allow alarms, alerts and reports on hardware and software monitoring e.g. over system resource use beyond threshold limits, fault / alarm upon excessive network usage. May perform Hardware monitoring using Trap based integration with existing hardware monitoring solutions or element management solution supplied / asked from OEMs in this bid's scope of work.
56	Should be an integrated solution for managing & monitoring devices, bandwidth utilization, configuration management.
57	Should be able to perform Near Real-time monitoring of each of the alarms and resources (but not limited to such as CPU, Memory, Disk, IO, network etc. aspects) of physical and virtual servers including the other network devices
58	The solution should have self-monitoring ability to track status of its critical components & parameters such as Up/Down status of its services, applications & servers, CPU utilization, Memory capacity, File system space, database Status, status monitoring between primary and secondary system and event processing etc. It should provide this information in real-time through graphical dashboards, events/alarms as well as in the form of historical reports.
59	Reports shall contain visualizations utilizing the applicable graphic types such as Bar Chart, Gauge , Pie Chart, Scatter Plot, Simple Value, Table, Time Series, User Image, User Text etc.
60	The proposed solution should be able to monitor Physical Servers running UNIX, Linux, windows or any other operating systems & also Virtual Servers on VMware or any other Hypervisor-based Virtual Network Function infrastructure network management must also be supported .
61	Supplied Solution should monitor the devices/VMs continuously and identify & capture the faults/alarms from each of it.
62	Users must be able to choose the thresholds (high and low) for when an alarm and/or warning will activate, along with the points for the severity level. Users must be able to acknowledge and filter alarms. Alarms should have a way to prioritize more important alarms. The solution shall include an alarm history page where all system alarms are stored. Users should be able to search for previous alarms by site, device, or point. Should be able to manage and display alarms/events/alerts, store them and should allow creation of new alarms/events/alerts from scratch with customizable threshold limits. The threshold may be applied to any valid parameters which are being monitored per device.
63	Should Support Assignment of Alarms/events/Alerts to System Administrators for processing and completion via a Helpdesk / Service Desk feature. It must also allow the logging/recording of solution/Actions during Alarm/event/Alert Completion/closure.

2	Enterprise Management System with NMS in HA
S. No.	**Description**
64	As a hypothetical example, after the analysis of Alarm/event/Alert, if solution requires a change in configuration at a Network Element (NE), this change in configuration should flow via the change management system for ensuring appropriate approvals and recording. A ticket for this alarm should be created in helpdesk, which should trigger a Change Request in Configuration Change Management system. Upon various approvals, the CR is implemented in the system and only then CR, ticket and alarm are closed. CMDB is updated with this configuration change for future records. User must also be able to map an Alarm/event/Alert with a ticket as well as CR.
65	Should support to have various actions that can be taken, including but not limited to, sending out emails, forwarding SNMP traps, sending SMS text alerts, playing sound, emailing any type of reports generated etc.
66	Should Support Incident/ Alert Escalation through defined Escalation Metrics
67	Should Generate Green Alerts / automatic update the alert status as down / indicate the new status after successful alert processing
68	Should support variables in alert email messages to make message self-explanatory
69	Should be able to define relationships (based on topology created manually/automatic, etc.) between servers and services/applications to avoid false-positive email alerts in case of outage
70	Proposed monitoring solution should provide current and historical out-of-the-box reports for various statistics monitored. The solution must also allow for the customized reports in addition to default reports as per templates. System should be able to generate the current alarm reports for entire inventory or per device basis. Same for the historical data with custom time period.
71	Should allow advanced customization in reports allowing options to extract custom data from database
72	Should allow sending out (emailing) of all types of reports on custom schedule such as daily, weekly, monthly basis etc, i.e allow to Schedule Report Generation. It shall allow to schedule execution of tasks allowing automation.
73	Should allow Creation of Customized dashboards as per requirement
74	Solution should provide feature that facilitates suppression/reduction of alarms displayed by means of alarm suppression feature. For example, during a maintenance, it should allow to suppress alarms from devices. The system must support filtering options by alarm status, device type/category to facilitate quick actions.
75	The proposed system shall integrate network, servers or other equipment alarm/performance information in a single console/dashboard and provide a unified reporting interface for each category of components.
76	Alarms should be mapped to the live topology views and real time updates to topology based on alarm occurrences. System can support one click alarm masking capability.

2	Enterprise Management System with NMS in HA
S. No.	**Description**
77	Should trigger (pre-configured and customized) automated actions based on incoming events / traps. These actions can be automated scripts/batch files. Scripts/batch files should be customizable.
78	Should support out of the box network Trap Analytics
79	Should provide the comparison views for configuration versions e.g. Original Configuration Vs Latest Configuration
80	Should provide option to provide standard compliance checks w.r.t Configuration, OS version, software process/services running state across all target devices, etc.
81	EMS solution proposed should have capability to fetch / receive alarms from other Network Monitoring tools / Systems monitoring tools / other domain monitoring tools like AIM , PATS supplied as a part of this bid and including equipment from other locations / bid as defined earlier in this document and /or as per scope of work.
82	Alarm Filtering should allow flexible filtering rules for users to filter the alarms by category, severity, elements, duration, by user, by views, by location or by any other custom field of choice present in the alarm object
83	The discovery processes may be configurable to perform continuous and auto discoveries. Should be able to auto discover, monitor devices installed and commissioned at different Physical locations
84	Should have an Asset management system for maintaining and managing the all assets as defined in the scope of work.
85	The EMS solution should be integrated with PATS to detect physical assets movement from racks and for receiving alarms from PATS.
86	Should be able to integrate with modules serving other monitoring/ management purposes and consolidate the information into a single view such as should be able to integrate with the AIM solution over REST APIs/other mechanisms to receive alarms from AIM.
87	Should be scalable to allow the addition/integration of new instances of devices to be added in future
88	Should allow information from multiple instances of application to be consolidated into a single view
89	The EMS solution should integrate with Network Equipment's OEM supplied Element Management systems. Bidder needs to provide the Network Equipment's OEM supplied Element Management systems along with the NEs. Also, SI may budget to integrate the proposed EMS in this bid with other Element Management Systems / Network Management Systems solutions to be supplied w.r.t other Infra Solutions referred in this bid.
90	It should monitor performance across heterogeneous networks
91	The tool should automatically discover different type of heterogeneous devices (all SNMP supported devices i.e. Router, Switches, Servers etc.) and map the connectivity between them with granular visibility up to individual ports level. The tool shall be able to assign different icons/ symbols to different type of discovered elements. It should show live interface connections between discovered network devices. It must support auto Discovery of network inventory and create a network topology

2	Enterprise Management System with NMS in HA
S. No.	**Description**
92	The solution should allow for discovery to be run on a continuous basis which tracks dynamic changes near real-time in order to keep the topology always up to date. This discovery should run at a low overhead, incrementally discovering devices and interfaces.
93	EMS should provide the compliance management report in the integrated view showing network topologies. Proposed EMS should adhere to guidelines so that the CERT can stay compliant with its current day industry standards .The minimum security guidelines to be adhered are: a.) All the data stored or getting communicated over LAN should be encrypted as per encryption level mentioned in detailed technical specifications. b.) Malicious code test certificate to be provided. Solution should be OWASP / SANS certified by CERT-In empanelled vendor. c.) VAPT – Ensure VAPT is done immediately after the software is deployed but before taking the system into production. d.) To provide regular hot fixes/updates to ensure the system security. e.) The Software to be integrated with AD and AAA as well to ensure the strong access control measures. The SI is required to provide a clean VAPT report of the complete solution (i.e. including all modules) at the time of acceptance testing, where all categories of vulnerabilities are fixed in the deployed solution. Additionally, periodic VAPTs must be done yearly from the date of acceptance and additional VAPT should be done, upon any major upgrade in solution or solution's respective modules.
94	EMS's Network Configuration Analysis feature should allow Network Configuration Analysis Reports that help to diagnose and resolve faulty configurations such as reports on all network devices that have a startup-running conflict (don't have a sync) as well as the ones that have their startup and running configurations in sync. It should also be able to provide reports on Configuration Change Trend –a report that provides the historical trend of all configuration changes during a specific time period, aiming to allow to manage network better by performing extensive / in-depth configuration analysis on all device types in network.
95	The system must be able to build and visualize network topology using SNMP, information in ARP tables from routers, MAC tables from layer 2 switches. The discovery should be automated and continuous.
96	It should support various discovery protocols to perform automatic discovery of all L2, L3 Network devices across MPLS and or any further Network connectivity's planned in future.
97	The tool should support dual-stack (IPv4&IPv6) shall be able to discover IPv4 only, IPv6 only as well as devices in dual-stack. In case of dual stack devices, the system shall be able to discover and show both IPv4 and IPv6 IP addresses.

2	**Enterprise Management System with NMS in HA**
S. No.	**Description**
98	The tool shall also be able to work on SNMP v1, v2c & v3 based on the SNMP versions so as proposed solution is able to monitor and manage the supplied equipment/devices as per the RFP. It shall provide an option to discover and manage the devices/elements based on SNMP as well as ICMP. It should also support extensive discovery mechanisms and must easily discover new devices using mechanisms such as SNMP Trap based discovery.
99	Solution must also allow for inclusion and exclusion list of IP address or devices OR allow to specify list of IP address or devices to be discovered from such discovery mechanisms
100	The proposed solution must provide a detailed asset report, organized by vendor name, device type, listing all ports for all devices.
101	Should be able to create and allow management of Service requests by integrating with the IT Helpdesk solution/module. Must have Email-to-Incident feature, allowing automatic conversion of emails to tickets if a person sends an email to helpdesk. Must maintain a history tab against all the communication happened on a ticket and/or maintains a thread not only on per ticket Id basis. but also on email sender, cc responses to that email chain.
102	Must have the following Device (especially for Networking Devices) Monitoring Capabilities. Should be able to generate alarms based if any of the parameters being monitored goes out of threshold range. These parameters should be allowed to record in a report for a selected time duration. The reports should be allowed for performance issues observed while monitoring during a specified period of time (performance reports). The performance reports should also be allowed for only a specified group of devices.
103	i. Device Monitoring parameters such as a Device status and Availability , b CPU Load Data , c Device Disk Space Data ,d Memory Utilization etc.
104	ii. Device Hardware Monitoring such as a Device Fan Monitoring , b Device Temperature Monitoring ,c Power Supply Monitoring etc. Note - optional meaning that if this parameter is there in the MIB or provided by the respective element management system, this has to be implemented at EMS.
105	Link Monitoring: Graphically represent the various links over geographical maps. Each link's information on status and latest alarms generated shall be presented to give a quick bird's eye view of entire link health. These parameters should be allowed to record in a report as well. Should be able to generate alarms based if any of the parameters being monitored goes out of threshold range.
106	Solution should allow per link parameters such as a Link Availability Monitoring b Average Response Time Data for each link (optional) c Bandwidth Utilization Monitoring d Network Latency Data e Network Topology f Packet Loss Data g Network Discard Data, Error Rate etc. Note - optional meaning that if this parameter is there in the MIB or provided by the respective element management system, this has to be implemented at EMS.

2	**Enterprise Management System with NMS in HA**
S. No.	**Description**
107	Should allow to generate Link Monitoring Reports with parameters such as a Performance Data Analysis, b Performance Data Collection, c Performance Report Generation, d Traffic Analysis e Utilization and Error Rates.
108	Should support Bandwidth Monitoring with parameters such as : a Network flow analysis ,b Netflow collector , c Sflow collector d Jflow collector e Real time monitoring f Bandwidth Utilization etc.
109	Should support bandwidth Monitoring Reports with parameters : a. Device Grouping b Single click instant reports ,c Usage history based on hours minutes days , d Top talkers report , e Top Listeners report , f Top users report , g Top hosts report , h Protocol/Application level reports , i Interface level reports , j Customised reports , k Customised email alerts, l Application Mapping, etc.
110	Solutions should allow to maintain Logs such as: a Historical Logs in respective modules, b Interface Error Data/ logs, c Syslog Messages Solution should have an inbuilt feature of an integrated SysLogServer, i.e. EMS solution should be configured to receive individual syslogs from different systems/solutions/devices. It should be able to parse the SysLogs based on the parameters defined/configured and is able to show the alerts/critical/alarms etc. as per configuration in EMS. In case of no inbuilt feature of a SysLog Server, the OEM may integrate an enterprise grade Syslog server, test and create a customized solution for above requirement.
111	Should monitor Virtual Private Networks (L3, L2), VLANs, MPLS service availability and inventory. It should support view of IPSec tunnels. It should support monitoring of connectivity of all the network elements / servers / other IP equipment as per scope of work
112	EMS solution must have the capability to import MIBs of 3rd party Data Center components so as trap monitoring can be enabled.
113	Access Privileges and Roles for different users/operators
114	Each user/ operator should be allowed to provide with user roles that should include operational service views enabling operators.
115	The system should integrate with Helpdesk / Service desk tool for automated incident logging and also notify alerts or events via e-mail or SMS besides GUI/browser.
116	Permissions and Features to access the system should be defined within the roles / based on roles and access privileges definer per user basis.
117	Should be able to send e-mail or Mobile –SMS to pre-defined users for pre-defined faults.
118	Besides the alarms per device the solution should be able to provide per device virtual visualization of interfaces, management interfaces, interface status, link status etc.
119	In addition, provided the device's MIB supports, the solution should be able to provide the power (ON/OFF) status of each supplied device in the bid. In case of multiple power modules per device, multiple power status per device should be shown wherever the MIB allows this feature.

2	**Enterprise Management System with NMS in HA**
S. No.	**Description**
120	Provides Layer 2 and virtual LAN (VLAN) network information. Should be allowed to be exported to reports
121	EMS module shall allow all types of reports to be exported to .pdf & comma-separated values (.CSV) formats.
122	Reports generation should be customizable, so as to allow to choose the fields/columns/parameters per report.
123	Should provide agentless discovery and shall use Industry-standard protocols such as WMI, SNMP, JMX, SSH etc. to perform discovery
124	The solution must have the ability to add network devices into inventory via auto discovery or the auto discovered devices into the inventory (if not yet added to inventory)
125	**Network Traffic Flow Analysis System**
126	It shall be able to capture, track & analyse traffic flowing over the network via different industry standard traffic capturing methodologies viz. NetFlow, jflow, sFlow, IPFIX etc.
127	It shall provide key performance monitoring capabilities by giving detailed insight into the application traffic flowing over the network.
128	It shall be able to monitor each interface status per device, network fault at device level, per device basis - network traffic utilization, packet size distribution, protocol distribution, application distribution, top talkers etc. for network traffic. It should be able to generate reports for above stats.
129	It shall collect the real-time network flow data from devices across the network and provide reports on traffic based on standard TCP/IP packet metrics such as Flow Rate, Utilization, Byte Count, Flow Count, TOS fields etc.
130	The platform must provide complete cross-domain visibility of IT infrastructure issues
131	The platform must consolidate monitoring events from across layers such as Network, Server, Database, 3rd party tools (monitoring solutions to monitor key DC elements like wires / cables etc.)
132	The solution should support single console for automated discovery of enterprise network components e.g. network device, servers, virtualization, cloud, application and databases
133	The solution must support custom dashboards for different role users such as Management, admin and View-Only/other users
134	The solution must allow creating custom data widgets to visualize data with custom preferences
135	The solution must support multiple visualization methods such as gauge, grid, charts, Top N etc.
136	The solution should provide top level view of infrastructure health across system, networks, application and other IT Infrastructure components into a consolidated, central console

2	**Enterprise Management System with NMS in HA**
S. No.	**Description**
137	Bidder needs to integrate EMS with proposed Element Management solutions provided by OEM’s w.r.t NEs proposed in this bid & also incorporate the MIBs of NEs proposed in this bid.
138	Upon the integration with PATS, the EMS solution should have the capability to present critical metrics w.r.t Assets.
139	The solution must support visually representing network outages and other error conditions on the topological map. In General, Solution should be able to generate alarms based on if any of the parameters being monitored goes out of configured threshold / threshold range.
140	Provision the following Device Performance Monitoring Capabilities for Servers (Application/Historical /others) & Integration with OEM's Element Management solutions to achieve described monitors from installed servers, is also the scope of requirements.
141	1 Physical Server Monitoring parameters such as a. Server Status and Availability , b. CPU Utilization c.Memory Utilization d. Process Monitoring e. File System Monitoring f. Disk Utilization etc.
142	2 VMware and ESXi Host Monitoring parameters such as a. Status and Availability b.CPU Utilization c. Memory Utilization d. Monitoring of Virtual Hosts e.Disk Utilization f.Network Utilization g. Hardware Monitoring h.Performance Dashboard i.VM Replication Monitoring etc.
143	3 Linux server Monitoring parameters such as a. Server Status and Availability , b. CPU Utilization , c. Memory Utilization ,d. Process Monitoring ,e. File System Monitoring ,f. Disk Utilization ,g. Network Interface Monitoring etc.
144	4 Windows server Monitoring such as a Server Status and Availability b CPU Utilization c Memory Utilization d Process Monitoring e File System Monitoring f Disk Utilization g Network Interface Monitoring h Event Log Monitoring etc.
145	5 Database Monitoring parameters such as a Database Availability b Database Process and Logs c Locks and Buffers d Tablespace/Database e Sessions/Connections f Database Memory h SQL Statistics i Database Jobs etc.
146	6. SLA Management parameters such as a Customized SLA for Applications , b SLA escalation ,c SLA Reporting feature to provide downtime per equipment , link etc. primarily for cases, where tickets due to alarms are sent to ticketing tool etc.
147	EOL and EOS Management - Keep track of all devices (networking, servers and other equipment) for their end of Life , end of Sale, and end of Support.
148	Should be able to integrate with Service Desk module to support and handle large volume of incident, event, service requests, changes, etc.
149	**Network Configuration Module**

2	Enterprise Management System with NMS in HA
S. No.	**Description**
150	Should allow Network Configuration change management on multiple vendor devices for all the network devices such as router, switches & firewall. Change management should include the tracking and version maintenance of configuration changes in real-time on each of them.
151	It should allow to audit configurations and deploy configuration updates in single or multiple devices at once. From the scalability perspective, purposed solution should support managing configurations of hardware of more than 180 different OEMs, including all major OEMs .
152	It should have enhanced network security by preventing unauthorized configuration changes and notifying the admin about any changes.
153	The proposed management solution's network configuration module, should be able to automatically backup configurations (for both text based and binary configuration files etc.) from routers, switches, firewalls and other network devices to EMS. The trigger to automatic back up may be allowed to be setup in EMS , such trigger could be upon a detection of a configuration change and/or an automatic timer based. The configuration change should be recorded with the date-time stamp along with the user info. All configuration data needs to maintained as encrypted. The EMS should bring the backup of these configuration files for Firewall and Access Point or other networking equipment, provided the OEM / OEM's Element Management System allows an automatic mechanism and a standard interface for backup of configuration files from these devices.
154	Should be able to backup, compare and restore network configuration for all the networking devices defined as per scope of work of this tender. Backup system should allow to store for atleast 1 year of historical data. Further, it should be a provision on the tool for configuring the data retention and log archival so that operator(s) may be able to control as per its discretion.
155	Should be able to make single or bulk configuration changes across multiple devices. For example: such as change community strings, update ACLs etc. Also, in case a user changes the configuration on a NE, the EMS's Configuration change management module should be able to detect this change per user basis. It should be able to display the new configuration , show its difference with old configuration version and also show which user made the changes at what time etc.
156	The system should be able to clearly identify configuration changes / policy violations / inventory changes across the network of networking devices from multiple OEMs .
157	The system should support secure device configuration capture and upload and thereby detect "running" and "start-up" configurations and alert the administrators.

2	Enterprise Management System with NMS in HA
S. No.	**Description**
158	The proposed system should be able to administer configuration changes to network elements by providing toolkits to automate the administrative tasks (such as mentioned below) of effecting configuration changes to network elements: a) Capture running configuration b) Capture start-up configuration c) Upload configuration d) Write start-up configuration e) Upload firmware
159	The proposed solution must able to push configuration changes to multiple network devices
160	Should allow automated and scheduled backups of configuration files , it should tend to eliminate manual configuration management , by allowing features such as and not limited to - scripts , automation etc.
161	Should allow to Encrypt and store configuration files in enterprise standard and internationally complaint standards. The users session and data on the storage should also be encrypted including the support terminal session or shell session .
162	Should allow to setup / mark a configuration as the best working "Baseline Configuration" , so as to allow for a quick backup during a disaster / crisis event.
163	Should follow configuration versioning and comparison between saved versions
164	Should support Network Configuration Analysis: Should allow side by side comparison of configurations.
165	In the integrated Configuration Analysis module it should allow to perform configuration analysis for network equipment's like router's and switches. The configuration management module should also be integrated with AAA/AD server for providing RBAC. The solution should be completely multi-tenant in every module for allowing RBAC. There should be logging of each command performed at any NE by the users . This should be logged and reported at AAA server.
166	The system should be able to capture the configurations in the database/datastore.
167	The system should be able to differentiate the old and current configuration with version control.
168	The system should be able to capture exact configuration change with color coded highlights, and date and time of addition, modifications, removal or change in the configuration.
169	The system should be able to provide the reports for various actions described under Network configuration management feature. The reports may include status and summaries of different activities such as device configuration details, changes in configuration (within a specified period / per user basis), network inventory, conflict between startup and running configuration, device audit details, policy compliance details etc.

2	**Enterprise Management System with NMS in HA**
S. No.	**Description**
170	The system should be able to export the configurations in TXT, CSV, PDF formats.
171	**Asset Inventory Monitoring & Management**
172	An asset management module should be in-built part of proposed EMS from same EMS OEM.
173	System shall have an ability to track (automatic/manual/via integration with other modules of overall system) and manage all data center and remote location assets including but not limited to IT/IoT/Non IT/Software(s) - Racks, Network equipment, IT equipment, Intelligent PDUs, sensors, application(s) etc.
174	System should allow to search / locate a data center asset based on various filters/fields, it should also provide detailed information about the assets. It should allow a provision / feature with ability to define down time for Assets to conduct Maintenance activities.
175	The solution should allow for discovery to be run on a continuous basis which tracks dynamic changes near real-time in order to keep the topology always up to date. This discovery should run at a low overhead, incrementally discovering devices and interfaces.
176	The tool shall be able to work on SNMP v1, v2c & v3 based on the SNMP version supported by the device. It shall provide an option to discover and manage the devices/elements based on SNMP as well as ICMP. It should also support extensive discovery mechanisms and must easily discover new devices using mechanisms such as SNMP/ Trap based discovery.
177	Solution should be able to integrate with EMS to auto discover the IT Assets via its scan/discovery process
178	Solution should allow to manage the physical aspects of all IT assets & Non IT Assets —from request of movement, to their end of Life , Sale, & Support related timely triggers, making it easier to optimize costs, and compliance risks.
179	Assets and Non IT Assets will include category of devices as defined in scope of work such as Network switches, routers, firewalls, application servers, historical servers, packet brokers, etc.
180	The Asset system should allow Role based access.
181	While performing discovery, solution must also allow for a feature that allows to include and exclude OR allows to specify IP addresses / subnets or devices OR from auto discovery.
182	The proposed solution must provide a detailed asset report with different filters mechanisms, organized by vendor name, device type, listing all ports for all devices. Should be able to create Service requests for each of the asset.

2	Enterprise Management System with NMS in HA
S. No.	**Description**
183	Tool should provide the information about equipment's dependency on each other. This affects the overall performance of the datacenter. Performance data of each equipment in the datacenter should be available for analysis. Thus any product vendor for an underperforming asset can be alerted and the inventory is either repaired to perform or replaced in time. Alerts for such scenarios should be generated in EMS system
184	It must easily and automatically discover newly add devices to the n/w.
185	The system shall provide an easy method of searching and locating assets and asset groups
186	The system shall support an importing of asset list from a 3rd party tool in CSV format into an asset database. If a specific asset in not defined, the tool shall be able to create it.
187	The system should allow the user to create Asset profile with unique serial no, asset tag, asset owner, asset life, details of assets etc. The assets must be searchable with any of the parameters such as serial number, asset tag. It must allow to list out assets based on owners , location etc.
188	The system should allow the user to search & track assets at any time to know the status of an asset – location, assigned to which user, contracts/warranty/AMC renewal for maintenance etc.
189	Overall system's solution should support virtual installation or server based installation. This should not be a proprietary hardware based or embedded based solution.
190	**Change Management (CM) Module Requirements**
191	The CM solution could be a module within EMS supplied. The CM solution should be web based, must also work in HA mode.
192	Solution should allow to create different roles (preferably after integrating with AAA/AD) with different privileges such as Change Requester, Change Record Authorizer, Change Implementer, Change Advisory Board Member, Change Manager , Post Implementation Reviewer , Customer Approver , Customer Tester , WorkFlow Administrator etc. This will ensure the restricted access to devices. Different privileged users should be able to play the role of implementers, reviewers, approver etc. , so as to allow a workflow w.r.t change request. Change management must be implemented in conjunction with configuration management, so as wherever required, a view of the infrastructure may be provided to assess an impact of a change.

2	Enterprise Management System with NMS in HA
S. No.	**Description**
193	CM should allow to Create, View, Edit the Change Requests (CRs).
194	Each CR must be allowed to follow a chosen / predefined workflow . The solution may also allow to create work flow for CR.
195	The solution must facilitate Assigning of roles to ensure that a change process workflow is started, managed, and implemented by the right people .
196	The solution must provide Change history: Captures the change history of all the fields and can be viewed for each record. Audit trails like changes done by the user, modification time, current value and previous values.
197	The solution should have CR correlation: Linking of CRs to related incidents, problems, assets, Cis
198	CRs must support Multi Stage custom based approvals.
199	The solution should Achieve complete visibility into which CIs have changed.
200	The solution must have defined Standard Reports
201	CRs should be authorized by Authorizer before taken up further in CM system
202	Change Advisory Board Member is able to sign-off, reject, or recommend changes necessary for anything that need to be processed.
203	Should be able to provide the status of all CRs (Open, Close, etc.) in a view . It should be filterable per user basis .
204	The system shall have integrated ITIL v4 or higher processes complied Operations Management System for Helpdesk, Ticketing, Maintenance and Configuration Management Database (CMDB). The system shall enforce best practices workflow and meet ITIL framework guidelines. All monitoring elements should be stored and accessed from a central datastore. This also should be have RBAC.
205	Change Implementer Implements the change and updates the status. In General, the status change of a CR triggers the email request to its configured workflow owners and assigns the new 'action owner'
206	Change manager is able to review all the CRs, sets Change Record Authorizers, forwards the CRs to the CAB, issues Change Schedules related with CRs , reviews all the implemented CRs, and Generates Regular Reports
207	Customer Approver(s) is able to review and approve the CR before the CR is implemented.
208	Customer Tester is able to update the result for a CR
209	The solution must Assign downtime time start and end for a CI(Configuration Item)
210	The solution should be able to allow Assign Priority, impact, urgency and risk to CRs
211	Solution should have its own application and data base . It should be a web based portal hosted in an on premise manner.
212	CM Module should allow the end users to create, update, search and get status update of change requests. It should allow the attachments of documentation (such as pdfs etc.) with the CM requests

2	Enterprise Management System with NMS in HA
S. No.	**Description**
213	It should be able to use IMAP, POP3 ,SMTP protocols to provide email integration and able to send emails for CRs status as configured . The solution must be able to use IMAP, POP, protocols & should be able to automatically convert service request emails into help desk tickets.
214	CMS should be integrated with overall solution or be in-built as a part of EMS.
215	Supplied solution should have a standard search , advance search mechanism on the fields for enhanced productivity.
216	Should be able to well integrate with the supplied IT Helpdesk / Service Management solution to achieve the overall functionality. This is to ensure that a mapping between Ticket & CR can be made. On same lines, in case the CR is created in the Change Management Solution it should trigger an automatic Ticket creation in IT Helpdesk solution.
217	Supplied solution should be able to generate insightful reports on changes, compliance, inventory and other vital network parameters.
218	Supplied solution should allow atleast backup / history database maintained for atleast 1 year including but not limited to configurations, alarms, services , assets, asset locations, network performance related database
219	The EMS system as a whole should be able to send notifications on GUI, email and SMS
220	The supplied CM solution should be provided with a hardware capability to support 15000 service requests in a day with at least 100 simultaneous users . Hardware supplied should be capable enough to store data at least for 1 year.
221	Features for IT Service Management (ITSM) / IT helpdesk solution for managing the day to day Operations
222	The solution should have its own IT Service Management (ITSM) / IT helpdesk solution which is certified on ITIL v4 atleast 5 practices.Should provide an GUI interface w.r.t emails. Documentary proof of the ITIL certification, for the covered processes, should be provided at the time of bidding to verify compliance and ensure the solution's adherence to ITIL best practices."
223	The ITSM system shall be capable of assigning, tracking tickets to users manually as well as automatically based on predefined rules, and shall support notification and escalation over email. E.g. A ticket with 'Network fault' as a keyword(s) tickets gets automatically assigned to a user whose role is configured network technician.
224	IT Service Management solution must be an industry standard, enterprise grade web based solution that enables end users to create service requests and must be placed in High Availability Mode as sought in General requirements.
225	The ITSM solution proposed should be designed & architectured so as to allow to use ITIL framework and processes across sought modules including PATS / EMS , Alarm / Incident Management, Asset Management , CMDB etc. , so as unique data and workflows can be maintained for overall solution.

2	**Enterprise Management System with NMS in HA**
S. No.	**Description**
226	The ITSM solution should automatically provide suggested knowledge base articles based on Incident properties/attributes/tags/keywords etc.
227	The ITSM solution must integrate with all the supplied and required modules such as PATS,EMS,AIM,CMS,AAA solutions etc .
228	There should be a database in place to store data w.r.t integrated Tickets, Alarms , Incident & Problem management, Service Level management/ targets , configuration data base etc. The ITSM tool should allow to export the ticket reports in different formats such as csv,HTML,PDF ,Excel etc.
229	The ITSM solution should support multi-tenancy with complete data isolation as well as with ability for analysts based on access rights to view data for one, two or more organizational units.
230	The system should be able to create service desk tickets/ work orders/approval receipts for any work to be done in data center. For example - mounting a new server, connecting it to specific ports on network, powering it ON from specific outlets of the iPDU etc. This workflow should have various pre-defined approvers/reviewers / implementers etc , who should be able to approve/ disapprove/ comment(add remarks etc.) . The tickets templates should be customizable .
231	The system should allow to edit , assign , search and track these tickets. It should allow to provide dash boards with different filtering options that also allow to take out customized reports such as w.r.t ticket status , groups / user wise assignments etc.
232	System should also allow to search a ticket and track its historical details of various actions performed on same.
233	The ITSM solution should provide to browse through Configuration Management Database (CMDB) which should offer powerful search capabilities for configuration items (CIs) and services, enabling to quickly find Configuration Item as well as their relationships to other CIs.
234	Configuration item should get automatically attached with the ticket to enable the support team for faster resolution.
235	ITSM solution should provide an option for adding new workflows/catalogues with custom SLAs & multistage approvals. The workflows / catalogues may be based on hierarchy, roles , category of service request per catalogue. It should include notification and escalation capability if approval is not performed within the defined time period. Tool should be able to send alerts . Also, Optionally, it may support SMS based alerts , XML notifications, Pop-up window or Audio alert(s).
236	The ITSM Solution should be a web based solution and should be accessible via the browser.
237	ITSM solution should provide categorization, as well as routing and escalation workflows that can be triggered based on criteria such as SLA, impact, urgency, CI, location, or customer. Solution should be able to provide the aging reports of the tickets based on various types/categories of tickets. The Notification mechanism should allow administrator to define notification channel per time of day and trigger multiple notifications per person.

2	**Enterprise Management System with NMS in HA**
S. No.	**Description**
238	The solution should be able to record the actions of users per session basis including details such as time stamp etc. as per user for audits and records purposes.
239	Integrates with any underlying service management solution including Service Desk, Change Management, Service Level Management and CMDB for request fulfilment.
240	**Description for IP Address Management (IPAM) & Switch Port Management**
241	The IPAM Solution must support 15,000 IP Address Management for both IPv4 & IPv6 together. It should be scalable upto 1,50,000 without any hardware change.
242	The solution must be agentless can be an pre-integrated module of EMS or it could be a separate module . It may be noted that the functionality and specifications sought via IPAM and Switch Port Management Module may be fulfilled as an integrated module of EMS.In either cases , it must allow the secured access via the browsers using SSL certificates(128 bit &/or 256 bit encryption). The final EMS solution with IPAM & Switch Port Management may be an integration of OEMs to fulfill the sought requirements. In case the IPAM solution is from other OEM, the EMS OEM holds the responsibility along with bidder to accomplish the end to end integrated requirements of IPAM in EMS. Bidder holds the responsibility to ensure testing of complete functionality of these components / modules before proposing a solution in the bid.
243	The IPAM solution must be run on high availability as per previously suggested architecture for HA in this document.
244	The solution must be flexible to allow the creation of custom fields for objects in IPAM. This must be configurable via the Web GUI.
245	In General, the overall system should support REST APIs(PUSH and PULL) for integration with 3rd party systems if required.
246	The IPAM solution should be able to seamlessly integrate with DNS and DHCP records using standard non properiratary protocols.
247	It should support the features such as : Creating groups, Subnet ,Adding subnet to group , Automatically detect devices , Manually adding the device, Display Interface name with IP address , Scanning devices in the network , IP address scanning within the subnet or IP address scanning within the group etc.
248	The IPAM solution should be able to create its own widget / report to display customized subnet reports that should include details such as free IP, used IP and per IP Address details such as DNS name, Last alive time, Status(Used, Unused) etc. i.e any other custom fields added
249	The IPAM solution should have the ability to locate the available subnets inside a Supernet. This is to provide assistance to users when creating subnets inside an aggregated Network. IPAM system should support VLSM (Variable Length Subnet Masks)

2	Enterprise Management System with NMS in HA
S. No.	**Description**
250	IPAM user interface must be web-based without specific browser vendor requirements
251	In General , the history and backup data w.r.t IP Address Management Tool and Switch Port Management Tool should be saved for atleast 1 year.
252	IPAM system should be able to export reports in PDF, CSV format and in any other formats
253	IPAM system should have support for workflow process for various administrator roles and should include a change approval oversight capability. It must allow to create different user profiles with different level of permissions. Preferably, it should integrate with AAA/AD to achieve this feature.
254	The system's audit records should contain a timestamp, username and record modified.
255	The system's reporting engine should include audit reports.
256	The system should support granular rights administration, limiting the functions and rights to user and/or Zone level by integrating with Active Directory.
257	The tool should show up and map the devices plugged into each switch port in near real-time
258	Should allow admins to find out which devices were connected to a particular switch at a specified period of time
259	Advanced search mechanisms should allow the devices searching by MAC, IP Address, DNS Name etc.
260	Allow grouping of switches for easy identification and control
261	The IPAM tool should be able to perform and track address space allocations.
262	Should provide notifications upon Switch port status changes
263	Should allow to Manage Switch Port using SNMP/SSH by allowing administrators to block or unblock a switch port
264	The IPAM component must perform host discovery using a variety of methods including ping, TCP port 80 connections, Address Resolution Protocol (ARP), cache data, and device OS mapping etc.
265	MAC Address Scan – The tool must have the ability to scan a given range of IP Addresses and display the MAC addresses for various devices available in the given range. Also must display the IP address, port number, community, MAC address, DNS name, system name(optional), and system type(optional).
266	DHCP Scope Monitor – The tool must be fully integrated with the DHCP system and support the capability to fetch all the scopes that are defined in the DHCP Server and display the total, used, and available IP Addresses in each scope. When the number of available IP addresses falls below a defined value, the display should indicate the criticality.
267	The IPAM must have the capability to find free address space across a range.
268	The IPAM must scan multiple subnets simultaneously . It should be able to make out which IP address have been assigned statically .

2	Enterprise Management System with NMS in HA
S. No.	**Description**
269	It must provide the requisite information to build and visualize network topology using information in ARP tables from routers. It may also use the information of MAC tables from layer 2 switches as well for this feature.
270	The system must have the capability to group the subnets in a hierarchical tree format
271	It should be able to handle Device/Network templates (Creation, Deletion, Modification & Uploading) and the system must automatically discover the network's subnets or import them from a CSV file
272	DNS Resolver – The IPAM tool must provide the host name of any node whose IP Address is known and vice versa with additional details like the default net mask, network type, and the status for the forward and reverse lookups by integrating with DNS solution
273	DNS Scan – Using this tool one must be able to scan a range of IP addresses by integrating with DNS solution to see whether the forward and reverse lookup actions are working fine for the devices. It may also show the response time. In cases where an IP is not used in the network, the tool must prompt that the system does not exist in the network.
274	The IPAM shall support appropriate logging functionality on itself as well as on external source like Syslog servers. All the activities made by administrators must be logged inside an Admin Audit Log Report.
275	The IPAM must provide integration with Vmware, HyperV, Openstack etc. and discover the VMs with clientless integration . The solution must provide details of virtual servers / VMware server running Linux or Windows as deployment of a virtual appliance
276	**General Features II**
277	The EMS solution should be able to group devices into different categories.
278	The EMS solution must display the topological information in graphical form representing nodes and groups of nodes on a realistic/custom static geographical map.
279	Uses the communications channel with enhanced security features, audit logs, and access control policies to provide direct connections to servers in any location.
280	The system (IT Helpdesk system, etc.) shall allow to create request i.e Tickets or work orders (and approvals) with customizable task details and timelines so as to allow measurement of the time taken for a task/work completion or equipment / service downtime and hereby allowing the calculation of SLA and penalties via the tool. The IT Helpdesk system should allow the attachments of documentation (such as pdfs etc.) with the CM requests .
281	The IT Helpdesk system should also be integrated with AD/LDAP for providing the access to users
282	The system should support filtering options to search and list down tickets.

2	**Enterprise Management System with NMS in HA**
S. No.	**Description**
283	The system should have a SLA Management module. The system should provide the operator ease of access on SLA creation for nodes and services. Escalation should be configurable and optimized for day-to-day operations. It should allow to add formulas for helping any calculation in SLA / downtime . SLA module should be customizable to provide the penalty details as per SLA criteria mentioned in the tender. The provided reports are ready to be used for penalty calculations.
284	Document Management/Collaboration / Knowledge-based module - The system should also have knowledge-based module built in for the operators for quick issue identifications and resolution, thus minimizing the time and efforts. This will should server as a historical database of documents and can be used for training of new recruits, resolution of alarms, resolution of certain specific issues. Users should be able to add information, categorize it, add files to it. The proposed storage for Collaboration and Knowledge-based module artifacts should be scalable. It must sufficient enough by default to store data for the complete contract period. In case of any shortage of storage , SI will be required to immediately(within 1week notice) provide the double the original capacity storage base.
285	The applications (solution) per hardware should be installed as follows and must work in High Availability Mode: The bidder may also suggest the optimized solution for effective/smooth execution of modules/application. However , it will be decision of ERNET India will be final in this regard. Server#One to host apps: EMS (including its all components such as Network Device Management, Device Configuration Management, Network Performance Management, IPAM, Switch Port Management, Change Management, Network Asset Management etc.) . Server#Two to host apps: IT Helpdesk Tool. A replica of above is to be provided at DR. OEMs having all required modules of EMS in a single software, is allowed to provide all EMS modules on a single server.
286	OEM of EMS Solution should be SOC2/SOC3/ CMMI Level 3, ISO 27001&ISO 27034 certified
287	OEM should have performed the installation / commissioning of atleast 2 projects with minimum 2000 nodes in each project in India.
288	EMS OEM of this bid needs to integrate EMS with the existing EMS & provide the information on the existing EMS's dashboard. Mostly all the existing EMS information will be provided over REST APIs by existing EMS; However if required EMS OEMs(both old and new) may also use other secure & Safe integration mechanisms.
289	OEM need to develop & provide a page (in new EMS) that maps the link/circuit id , configured bandwidth & other detail of a remote site with its corresponding ipsec tunnel id(s) at Data center & other relevant information. The OEM needs to ensure that real time

2	Enterprise Management System with NMS in HA
S. No.	**Description**
	utilization of these links can be monitored in EMS & accordingly the alarms(& accordingly tickets) pertaining to above or below the particular threshold of link utilization should be enabled .

Annexure-1 (Technical Specifications) Cntd.

PART-C (OPEX & Databases GeoIP, VPN Services)

S. No.	Description	Marked/ Highlighted Cross Reference of Specification with reference page no.	Compliance (Yes/No)
1	**Databases GeoIP, VPN / Proxy Services**		
1	The specifications for this service are required for the period of 36 months and are as follows : **Global GeoIP Location Database:** IPAddress,Country,Region,City,Latitude,Longtitude,ISP,Time Zone,Domain,Net Speed,IDD & Area Code,ZIP Code,Weather Station,Mobile Carrier,Mobile Country Code,Mobile Network Code,Elevation,Usage Type,Address Type,Category,District **Global IP Proxy Database** IP Address ,Virtual Private Networks (VPN),Tor Exit Nodes (TOR),Public Proxies (PUB),Web Proxies (WEB),Hosting Provider, Data Center or Content Delivery Network (DCH),Search Engine Robots (SES),Residential Proxies (RES),Enterprise Private Networks (EPN),Consumer Privacy Networks (CPN),Proxy Country,Proxy Region & City ,Proxy ISP,Proxy Domain,Proxy Usage Type,Proxy Type,Proxy ASN,Last Seen,Threat,Provider Note: Databases GeoIP, VPN / Proxy Services are required w.r.t Global prespective		

Asset Details in Existing DC, DR and Remote Sites.

Annexure- C

Sl. No.	ITEM	Equipment Quantity (approx.)	Unit of Measurement	Make & Model
		(A)	(B)	
1	Server Category-1	165	no.	Netweb
2	Server (category 1,3,4,5)	103	no.	Dell
3	Server Category -2	355	no.	Netweb
4	Server Category-3	30	no.	Netweb
5	Server Category-4	30	no.	Netweb
6	Server Category-5	15	no.	Netweb
7	Server Category-6	200	no.	Netweb
8	Server Category-7	6	no.	Netweb
9	Server Category-9	20	no.	Netweb
10	Server Category-10	16	no.	Netweb
11	Server Category-11	12	no.	Netweb
12	Server Category-13	8	no.	Netweb
13	Server Category-14	2	no.	Netweb
14	Server Category-16	2	no.	Netweb
15	DC- DR Spine Switch	4	no.	Juniper
16	DC -DR Leaf Switch	320	no.	Juniper
17	DC-DR OOB Core Switch	4	no.	Juniper
18	DC-DR OOB Access Switch	160	no.	Juniper
19	DR CE Router / Internal WAN Router	2	no.	Juniper
20	DC-DR Border Leaf Switch	4	no.	Juniper
21	DC-DR Internet Router	4	no.	Juniper
22	DC-DR Interconnect Switch - Type 1	4	no.	Juniper
23	DC-DR Interconnect Switch - Type 2	4	no.	Juniper
24	DC-DR WAN Switch	4	no.	Juniper
25	Remote Router/ Firewall – 2Gbps (In Remote Sites)	350	no.	Juniper
26	Flow Gen (Network Traffic Metadata Generation System)	25	no.	Inspark
27	Packet Broker / Packet Aggregator	20	no.	IXIA
28	Internet Firewall with IPS	4	no.	Fortinet- Fortigate
29	DR Internal Firewall	4	no.	juniper
30	DC-DR Solution/Application Firewall	4	no.	juniper
31	AAA Appliance Server	4	no.	Ivanti
32	Load balancer	2	no.	Array
33	Privileged Access Manager (in HA Mode)	2	no.	Arcon PAM
34	IPS/IDS	4	no.	Trellix Trellix Network Security
35	SSL VPN Gateway	4	no.	Array

36	Active Directory Solution	4	no.	Microsoft Microsoft
37	Console management server	4	no.	Vertiv
38	KVM Console	61	no.	Vertiv
39	Portable KVM console adapter	15	no.	Aten'
40	Monitoring and management tool for servers	2	no.	Netweb
41	Fireproof Vault (200litre)	4	no.	Ozone
42	Degausser	5	no.	VS Security SV91M
43	Data Diode *	5	no.	Chipstrip
44	Intelligent Cabling+AIM for 150 Racks	1	lot	Commscope
45	Smart Rack *	5	no.	Vertiv
46	Non Smart Rack with Redundant IPDU*	5	no.	Vertiv
47	65 Inch LED Display	2	no.	LG UH5J-H
48	Heavy Duty Workstation	35	no.	Acer
49	Heavy Duty Mobile Workstation Laptop	30	no.	Acer
50	Heavy Duty Color Printer	4	no.	Epson WorkForce Pro WF-C579R
51	10G SFP SR of appropriate OEM server(s)	100	no.	Netweb
52	10G SFP LR of appropriate OEM server(s)	40	no.	Netweb
53	5% patch cords[$] (DC,DR & Remote)	1	lot	Commscope
54	Layer-3 Access Switch (48 Ports)	20	no.	Juniper
55	Data Center Infrastructure Management (DCIM), RLPAT Solution & Heat Humidity Sensor Solution	2	Set	Vertiv
56	RF Id based Physical Asset Tracking Tags with one on each IT Element (Network/servers) at DC & DR as per scope of work & technical specs.	1800	no.	Vertiv
57	RF Id Rack Identifiers as a part of Physical RF Id based Asset Tracking Solution at DC & DR .	150	no.	Vertiv
58	RF Id Based Heat and Humidity Sensors for Racks at DC & DR as per scope of work & technical specs. Note: should include sensors tags for Phase-1 equipment at DC as well.	450	no.	Vertiv
59	1. Communication Gateways for Communication on RF with Asset and Heat-Humidity tags & on ethernet/WiFi with respective Software Solution at DC and DR (Based on number of Asset and Heat- Humidity sensors provided.) 2.Compatible Handheld scanner to read barcode / QR codes at DC & DR 3. Barcode Printer / QR codes with consumables(3Yrs Duration) at DC & DR.	2	no.	Vertiv
60	EMS Solution Total IT Elements = 2800, monitoring of MPLS Link of 250 locations	2	Set	Infraknit