

Response of Bidders Queries

S.N.	RFP Section	Page Number	Tender Clause	Change Request / Clarification/Bidder Query	Justification	Suggested Changed Clause	Response
1	SOR-C- Network –C-2 –End point protection for end user, Point no. 1	40	The bidder shall propose dedicated end point based solution to protect systems Advanced Targeted Attacks and APT's	As per specification you have asked for protection from Advanced Targeted Attacks/APT's and to achieve holistic protection from known and unknown threats a sandbox solution will be required.	EPP solution does not have compute where they can simulate endpoint environments to detonate objects carrying malicious codes. Hence a sandbox technology will be required which is specifically meant to cater unknown/Zero day attacks by simulating your endpoint environment i.e. OS, browser, MS office versions etc. Hence its a humble submission to incorporate sandbox solution with proposed solution to cater APT attacks. Clause should read as : The bidder shall propose dedicated end point based solution to protect systems from Advanced Targeted Attacks and APT's by integrating with sandbox solution supporting customised images having 60 virtual analyzers.		As per RFP
2	SOR-C- Network –C-2 –End point protection for end user, Point no. 2	40	The proposed solution shall work on a signature-less mechanism to stop threats without relying on a database to be present at the endpoint	Considering current threat landscape which is changing very rapidly and dynamically just relying on single technique is not adequate and will work as a single point of failure	As you have already considered the importance of Gartner in this RFP which itself said in his report that merely relying on single technique can not give you required protection also this is completely violating MoUD, NCIIPC, NIST and Cert-In guidelines. Hence considering defense in depth strategy a proposed endpoint solution should consist combination of both detection as well as prevention techniques to avoid single point of failure. Hence it is requested to incorporate prevention techniques as well instead of merely relying on detection techniques. Clause should read as : The proposed solution shall work on machine learning\signature-less mechanism\Behavior monitoring also use Firewall, Device control, Variant protection, Census check, crypto malware, fileless malware, Portable Executable files control, CVE number visibility, Application/Process control, Virtual patching and Data Exfiltration capability in a single unified agent to stop threats holistically.		As per RFP

3	SOR-C- Network –C-2 –End point protection for end user, Point no. 5	40	The proposed solution shall utilize layered and defense in depth approach, wherein the solution cannot be of the same make as existing endpoint AV	The proposed solution should co-exist with existing AV that is something you have already required as per point no. 4 of specification, now specifically mention that existing AV vendor can not participate by just giving justification of defense in depth approach is not logical	This point is restrictive in nature and not allowing our participation as EPP does consists multiple features and modules those do not have any dependency on each other and completely adhere defense in depth approach. Hence its a humble submission to dilute this clause to allow our participation also to achieve threat protection holistically. Clause should read as : The proposed solution shall utilize layered and defense in depth approach by incorporating multiple security layers i.e Application/Process control, Virtual patching and Data Exfiltration, Machine learning and Behavior Monitoring capability in a single unified agent avoiding sinlge point of failure.		Corrigendum-III
4	SOR-C- Network –C-2 –End point protection for end user, Point no. 8	40	Security vendor should have a dedicated research organisation that is focus on vulnerability research and should actively contribute to discoveries of new vulnerabilities exploited in the wild.	As you have understand the criticality and importance of contribution towards undisclosed vulnerabilities those are not even discovered by other infrastructure/security vendors. Public discloser is important to see how much contribution vendor has done in terms of vulnerbilty discloser also it should be achnowledge by microsoft and Adobe those are being widely used in industry and vendor should be recognised by pioneer threat research institution.	Vendor's contribution towards discloser of undisclosed vulnerability lie in commercially available application/OS is need of the hour and this capability give you proactive shield from sophisticated attacks which can use these open vulnerabilities not discovered by even vendors i.e. Microsoft, Adobe, etc. but how much contribution these vendors are making is something very crucial. Hence its a humble submission that vendor should publish these statistics of thier vulnerability disclosers and same should be acknowledge by other vendors i.e. Microsoft, Adobe, etc. also vendor should got recognised by Forrester who is leader in vulnerability research. Clause should read as : Security vendor should have a dedicated research organisation/vertical that is focus on vulnerability research and should actively contribute to discover undisclosed vulnerabilities and vendor should be in leader quadrant as per Forrester Wave Endpoint Security 2019 report.		As per RFP

5	SOR-C- Network –C-2 –End point protection for end user, Point no. 9	40	Software footprint should be small <50MB and should support interactive and/or silent install. Total of 39000 Licenses should be factored for this End Points from Day- 1. Proposed solution should support 100,000 concurrent end points from day-1 by purchasing additional Lic in future.	Defining any limit on endpoint footprint will going to restrict participation as every OEM is having its own architecture to deliver higher performance with security effectiveness	This point is restrictive in nature and not allowing our participation as every OEM is having its own architecture and methodology to deliver required security effectiveness along with higher performance without impacting user experience. Hence instead of defining limit on endpoint footprint specification should be focus on bringing required security effectiveness with higher performance. Hence its a humble submission to dilute this to allow our participation. Clause should read as : Software footprint should be small and support interactive and/or silent install. Total of 39000 Licenses should be factored for this End Points from Day- 1. Proposed solution should support 100,000 concurrent end points from day-1 by purchasing additional Lic in future.		Corrigendum-III
6	SOR-C- Network –C-2 –End point protection for end user, Point no. 26	41	The solution shall be capable of working in Windows, Windows Server & Linux operating systems	Are you using Linux OS at your endpoint (Laptop/Desktop) machines ? as EDR capability at endpoints running on Linux platform will provide very limited feature which will completely not going to server the purpose.	This point is restrictive in nature and not allowing our participation. Hence its a humble submission to dilute this to allow our participation. Clause should read as : The solution shall be capable of working in Windows, Windows Server & Mac systems		Corrigendum-III
7	SOR-C- Network –C-2 –End point protection for end user, Point no. 27	41	The endpoint solution shall be able to pinpoint vulnerable versions of popular applications installed in Endpoints	A proposed solution should have capability to prevent installation of any malicious application/process in your endpoint environment and by merely "pinpoint" vulnerable application will not going to server the purpose.	Proposed solution should be capable to blocking any malicious application initiating any illegitimate process which can work as a platform to host and perform malicious activities in network. Hence its a humble submission to dilute this clause and consider our recommendations. Clause should read as : The endpoint solution shall be able to block malicious applications/process to installed in Endpoints		Corrigendum-III

8	SOR-C- Network –C-2 –End point protection for end user, Point no. 29	41	The proposed solution should not be dependent on a network sandbox for its detection as it takes up bandwidth and affects productivity and shall provide the option of choosing which files to be submitted for sandboxing, to administrator	Most of the APT vendors are using Sandbox solution in offline mode which will not impose any latency on user experience and complete process is automate in nature. As you have already asked for mitigating Advanced Targeted Attacks and APT's based attack a sandbox solution is required.	APT solution placement is crucial for delivering security effectiveness along with higher performance without impacting user experience and it also depends on the vendor's approach and architecture as well. Most APT vendors sit in offline mode and inspect malicious objects passively to give their verdict of unknown threats which do not impact network performance. Hence it's a humble submission to incorporate sandbox solution which should tightly integrate with proposed solution and sit in offline mode. Clause should read as : The proposed solution should have network sandbox solution having 60 customised sandbox images simulating endpoint environment for its detection of Advanced Targeted Attacks and should natively integrate with proposed solution with complete automation of file sharing.		Clarification: Proposed EDR solution should have its own Sandboxing feature and should not be dependent on any Network level Sandbox.
9	SOR-C- Network –C-2 –End point protection for end user, Point no. 32	41	Solution should allow Users to choose to preview the new Policy UI.	This clause is restrictive and not allowing our participation and moreover why user interaction is required ?	This clause is restrictive and not allowing our participation as favoring particular OEM. Hence it's a humble submission to delete this clause. Clause should read as : Solution should have both web based as well local management console for administrator policy and investigation purpose.		Corrigendum-III
10	SOR-C- Network –C-2 –End point protection for end user, Point no. 32	41	Suggestion	Suggestion	As you have already considered the importance and recognition of Gartner for other components in this RFP. Hence it's a humble request you to consider Gartner recognition for proposed Endpoint protection solution as well which will allow participation of best in the breed solution providers and bring required security effectiveness. Clause should read as : The proposed solution should be positioned in the leader quadrant from last three published Gartner Magic quadrant report for Endpoint Protection		As per RFP
11	1	19	The offered storage should be a true symmetric active-active storage	The offered storage should be a Dual active-active controller storage or higher. In case of any controller failure, the workload from failed controller should automatically failover/move to the active controller without any manual intervention.	Clarifying the functionality required from the active-active controller configuration		Clarification: Our requirement is to achieve enterprise class storage functionalities wherein host can access all the luns through all the controllers simultaneously. Asymmetric/ALUA, in case of failover might require more storage system resources and a longer response time per I/O.

12	2	19	The Storage Systems should be supplied with minimum 600TB Usable capacity using 500 TB capacity on SAS/NLSAS Drives on RAID6 and 100TB using SSD on RAID 6 and scalable up to 1PetaByte usable capacity using SAS/SSD.	The Storage Systems should be supplied with minimum 1100TB Usable capacity using 1000TB on SAS/NLSAS Drives on RAID6 and 100TB using SSD on RAID 5. The Storage should be scalable up to Double of usable capacity or higher.	* The rack server speciifications also asks for 480TB usable capacity to be added on the SAN Stroage. Hence the capacity needs to be changed to ~1100TB (600TB + 480TB). * Also request you to remove the 480TB Capacity requirement from the rack server specifications.		Corrigendum-III
13	4	19	The Storage should be scalable to at least 800 SFF/LFF disk drives on the same set of controllers.	The Storage should be scalable to at least 1500 SFF/LFF disk drives or higher.	The specifications asks for 1100TB of usable capacity on day one hence the storage should be power enough to support large number of disk drives to support scalability in future.		Clarification: As per RFP, However bidder may propose higher storage scalable capacity.
14	8	19	Storage should be equipped with 8*32 Gbps FC ports, 4*10Gbe port for host connectivity. Required SFPs/Optical Module to be populated from day one	Storage should be equipped with 8x32Gbps / 16 x 16 Gbps FC ports and 4 x 10Gbe SFP+ port for host connectivity. Required SFPs/Optical Module to be populated from day one The ports should support both Block (FC & iSCSI) and File (NFS & CIFS/SMB) protocols.	The RFP specification asks for a unified storage while the specifications does not mentions about NAS/File protocols. Hence request you to please add the same in this clause.		As per RFP
15	17	19	The proposed storage system should support at least 24000 LUNs or volumes	The proposed storage system should support at least 6000 LUNs/ volumes or higher	In the current project, the required usable capacity (expandable) is ~2000TB. If the average size of each volume is 20TB then the max. volumes/LUNs which can be created are 100. Even if we consider 5 times the number of volumes to be created then also the max. volumes required is 500. Hence we request you to please change the clause as requested to increase bidders participation.		Corrigendum-III
16	25.I	20	Proposed storage system should support third-party storage virtualization natively or using another headers in High availability from day1. Necessary licenses and hardware on High availability should be supplied from day1.	The solution should include data migration from old/existing storage to the new/proposed storage system without any data loss. The migration and data protection during migration responsibility lies completely with the bidder. RAILTEL will assist the migration team with support related to the existing infrastructure for the data migration purpose.	The primary purpose of this clause is to get the data migrated from the existing storage to the new storage without any data loss.		Corrigendum-III
17	8	23	12Gbps PCIe 3.0 with RAID 1, 5, 6,10, 50 with 2GB cache	Request to amend the clause as - "12Gbps PCIe 3.0 with RAID 1, 5, 6,10, 50 with 2GB cache OR 12Gbps PCIe 3.0 SAS HBA"	The vSAN certified ready servers come with 12Gbps SAS HBA for pass-through functionality as per vSAN deployment guidelines. vSAN solution deployment doesn't require hardware RAID controller and needs only a pass-through SAS HBA as per vSAN architecture and compatibility.		Corrigendum-III
18	9	23	2 nos. of 960GB SATA M.2 in mirrored configuration for OS	Request to amend the clause as - "2 nos. of 480GB or higher SATA M.2 in mirrored configuration for OS"	960GB SATA M.2 Boot Flash disks are not available with all the leading OEMs. Moreover 480GB capacity is more than sufficient for vSphere hypervisor and OS installation.		Corrigendum-III
19	5	24	The switching OEM should be part of latest Gartner's Leader Quadrant for Data Center networking.	The switching OEM should be part of latest Gartner's Magic Quadrant for Data Center networking.	Most of the OEMs are in Latest Gartner report on Data Centre Networking, but may not in a leaders position, in order to have a healthy competition, we request to allow OEMs from Challengers/Visionaries quadrant as well.		Corrigendum-III

20	12	25	Switch should have a minimum 40MB buffer of more.	Switch should have a minimum 32 MB buffer of more.	Request for Change to 32 MB Buffer for us to participate		As per RFP
21	40	26	Switch should support MPLS segment routing and VRF route leaking functionality from day 1.	Switch should support VRF route leaking functionality from day 1.	MPLS is required on Wan Routers or Sdwan CPE and not inside Data Centre fabric In Page 18 Tender RFP DC Network Connectivity diagram MPLS is terminated on DC router so MPLS is not required in Internal Data centre Fabric		As per RFP
22	5	35	The switching OEM should be part of latest Gartner's Leader Quadrant for Data Center networking.	The switching OEM should be part of latest Gartner's Magic Quadrant for Data Center networking	Most of the OEMs are in Latest Gartner report on Data Centre Networking, but may not in a leaders position, in order to have a healthy competition, we request to allow OEMs from Challengers/Visionaries quadrant as well.		Corrigendum-III
23	12	36	Switch should have a minimum 40MB buffer of more.	Switch should have a minimum 32 MB buffer of more.	Request for Change to 32 MB Buffer for us to Participate		As per RFP
24	40	37	Switch should support MPLS segment routing and VRF route leaking functionality from day 1.	Switch should support VRF route leaking functionality from day 1.	MPLS is required on Wan Routers or Sdwan CPE and not inside Data Centre fabric MPLS is terminated on DC router so MPLS is not required in Internal Data centre Fabric		As per RFP
25	4. Scope of Work-Point XII	15	Any Management switches required for the proposed solution will be provisioned by the bidder in redundant topology.	Please clarify if each rack will have dedicated Management switch (2 nos in HA) to connect to all out of band Management port of all servers and switches on Rack . This switch will then Uplink to Dual 24 port 10G Aggregation Switch on 10G multimode fiber .	Please specify the qty of Access Management switch 24 port Gigabit with 2x 10G uplink and 2 Nos 24 Port 10G Aggregation Switch . No of Access Management Switch= N (No if racks) in HA mode 2 nos required per Rack , 2 nos Aggregation Switch 24 x 10 G Please specify qty as it will be equivalent to all to Bidders . Also For full redundancy in Management network , dual Access Management Switches to be proposed per rack .		Clarification: Bidder needs to provide Minimum 2 numbers of management switch in DC and Two numbers in DR. 48 port 10/100/1000 BaseT with 4x10G uplink Switch with Redundant Power supply and stackable Switch. If in case bidder requires more ports as per the solution proposed , bidder to provision accordingly.
26	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 1	20	Backup software proposed should be in Gartner's leader quadrant of the latest gartner Magic Quadrant report for Data Protection / Backup Software.	Backup software proposed should be in Gartner's leader quadrant of the latest gartner Magic Quadrant report for Data Center Backup & Recovery Solution published in year 2019.	Request you to please modify considering the latest report from Gartners.		Corrigendum-III
27	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 4	21	Backup software should be totally agentless but should support application aware backups for MS SQL, Oracle, SAP HANA, Exchange transaction logs with non-staged granular recovery of all these applications. It should support crash consistent VM level backup for all other workloads.	Backup software should be totally agentless with VM image level backup and should support application aware backups for MS SQL, Oracle, SAP HANA, Exchange transaction logs with non-staged granular recovery of all these applications. It should support crash consistent VM level backup as well.	Request you to please modify this clause being language used here is single OEM specific. Hence, we request you to please accept the changes suggested here.		Corrigendum-III

28	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 5	21	The Data protection services should be hosted on Scale out solution using software defined storage. The solution should be Multi-controller architecture to be quoted with 4 controllers/Nodes having 256GB Cache/Memory per Controller/Node.	The Data protection services should be hosted on Purpose built backup appliance (PBBA). The solution should be Multi-controller architecture to be quoted with 2 controllers having 768 GB RAM per Controller.	PBBA is widely accepted technology by world leading organizations in India as well as National Informatics Center using PBBA in multiple National Data Center's & Mini Cloud in many states in India.		Corrigendum-III
29	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 6	21	Backup solution should be provided for 500TB usable Disk based backup storage capacity (only at DC) leveraging 10TB NL-SAS drives on erasure coding or equivalent with protection of data against simultaneous 2 (Two) disk Failure with rack awareness and encryption functionality.	Backup solution should be provided for XX TB usable capacity purpose built backup appliance storage capacity (only at DC) leveraging 8TB NL-SAS drives with RAID 6 protection of data against simultaneous 2 (Two) disk Failure with one hot spare drive per disk shelf enclosure and encryption functionality.	PBBA is widely accepted technology. Hence we suggest here to include PBBA instead of commodity storage. Also request you to place front end data need to be backup here in place of XX.		Corrigendum-III
30	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 7	21	Backup solution shall be able to scale more than three times the current proposed usable capacity in a scale-out fashion.	Backup solution shall be able to scale more than Two times the current proposed usable capacity.	Scale out architecture is used in unstructured data storage and does not have any relevance to PBBA and backup solution. Hence we request you to please modify this clause to make leading backup solution OEM's to propose the backup solution.		As per RFP
31	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 8	21	The Software defined storage solution should provide multiprotocol support NFS, SMB & S3 and should have native protection from ransomware attacks or include third party antivirus scanning system using ICAP protocol any hardware required should be quoted from day 1	The proposed purpose built backup appliance should provide multiprotocol support CIFS, NFS, FC, VTL & OST and also provide methodology framework to safeguard backup data from ransomware/malware attacks.	SMB & S3 protocol is used in NAS or commodity storage. All leading backup solution OEM's provide PBBA with suggested protocols. OST & VTL protocol are standard protocols of backup solution.		Corrigendum-III
32	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 10	21	Backup software should provide best RTOs and RPOs through booting of Virtual Machines directly from the Backup to reduce the downtime.	Backup solution should provide 10 minutes RTOs and RPOs as per the last successful backup by booting of Virtual Machines directly from the Backup appliance to reduce the downtime. Purpose built backup appliance should be capable to boot minimum 30 VM's simultaneously.	Backup solution should have capability to provide enough random IOPs to support Business Continuity thru backup data. Hence, we request you to please accept the changes suggested here.		As per RFP
33	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 11	21	Backup software should have integrated data de-duplication engine with multi-vendor storage support to save space by storing de-duplicated copies of data. The deduplication engine should also facilitate IP base replication of de-dupe data. All necessary hardware and software required to support this functionality should be supplied along with other components	Backup solution should have integrated data de-duplication engine to save space by storing de-duplicated copies of data. The deduplication engine should also facilitate IP base replication of de-dupe data. All necessary hardware and software required to support this functionality should be supplied along with other components	Request you to please modify this clause being language used here is single OEM specific. Hence, we request you to please accept the changes suggested here.		Corrigendum-III

34	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 13	21	Backup software must have a feature of data validation, whereby a workload is powered-on in a sandbox environment and tested for its recoverability.	Backup solution must have inbuilt feature of data validation, where data validation is continuous process. This ensures backup data written on PBBA is can't modified and can be restored in the same state.	Request you to please modify this clause being language used here is single OEM specific. Hence, we request you to please accept the changes suggested here.		Corrigendum-III
35	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 14	21	Recovery verification should automatically boot the server from backup and verify the recoverability of VM image, Guest OS and Application Consistency.		Request you to delete this clause being the same requirement is mentioned in Point No. 13. Hence, we request you to please accept the changes suggested here.		As per RFP
36	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 15	21	The software should support varieties of backup mechanisms like Full, Incremental, and Differential etc. at different frequencies i.e. yearly, monthly, weekly, daily, hourly etc. as per defined policy. It should also have calendar-based backup scheduling. The restoration should also be supported accordingly.				As per RFP
37	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 16	21	Proposed backup Software shall support seamless integration with existing Backup solution for a wholistic view and better Management.	Proposed backup appliance shall support seamless integration with existing Backup solution for a wholistic view and better Management.	Two different backup cannot be managed by single console, however the purpose built back appliance can integrate with multiple leading backup software OEM's. Like wise Dell Data Domain can integrate with Veeam, Networker, etc.		Clarification: Bidder is allowed to quote new Backup solution (Existing & New requirement) on a new platform to provide single Management console.
38	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 19	21	The proposed Backup software must allow to configure the maximum acceptable I/O latency level for production data stores to ensure backup and replication activities do not impact storage Availability to production workloads		Request you to delete this clause since it is forfeiting the backup performance and restore of backup data.		Corrigendum-III

39	New Point to be added - Functional requirement of backup solution	New		The offered Purpose-built backup appliance should be sized appropriately for backup of front-end data of XX TB (XX % File System and XX % DB) as per below mentioned backup policies: - oDaily Incremental Backup – retained for 28 Days in the backup appliance. - oWeekly Full Backup for all data types – retained for 4 Weeks in the backup appliance. - oMonthly Full Backups – Retained for 12 Months in the same backup appliance. - oYearly Full Backups - Retained for 5 years in the same backup appliance. The offered purpose-built backup appliance should be quoted with at least XX TB usable capacity post RAID 6 and hot-spare penalty using 8TB or lesser capacity drives. The proposed backup appliance must be sized for adequate capacity with 10% YoY data growth and 2% daily change rate for the contract period. Any additional software or backup storage capacity (in addition to minimum XX TB usable capacity) or any other component required as per sizing needs to be provided by the OEM & bidder during the time of bidding for entire warranty period of 5 years.			As per RFP
40	New Point to be added - Functional requirement of backup solution	New		The proposed Purpose-built backup appliance should support retention lock (WORM) feature which ensures that no user and administrator is allowed to data is deleted accidentally and support for point-in-time copies of a LUN or volumes with minimal performance impact. Even Administrator should not be able to delete the data deliberately or accidentally till the retention of the backup get expired. The offered backup appliance must have the ability of inbuilt target side data deduplication, WORM (Write Once Read Many), Replication and Encryption using AES 256 bit for data at-rest as well as in-flight while supporting VTL, CIFS, NFS and OST protocols over IP as well as FC.			As per RFP
41	New Point to be added - Functional requirement of backup solution	New		The offered backup solution must complete all backup within 8 hours backup window and the bidder must provide all the hardware and software to meet this requirement.			As per RFP

	RAILTEL/TENDER/OT/CO /ITP/2020-21/ DC Solution /540	13	Veeam is the existing incumbent in the Backup Space. It would be recommended to have Backup Solution co-exist with incumbent solution and enhance the backup capacity. However bidder may propose any other backup solution which needs to be integrated with existing backup solution i.e. Veeam Backup Solution or propose entirely a new backup solution comprising existing and proposed solution capacity.		Two different backup software cannot be managed by single console and co-exist. Hence we request you to please remove Veeam reference from this RFP and ask the entire new backup solution and follow the standard terms of RFP.		As per RFP
43	12.2 Eligibility Criteria for Bidder:	64	The tenderer should have executed Single order showcasing supply, installation, testing, commissioning, implementation and operations projects for Data Center solutions commercially costing not less than 35% of the tendered value during last preceding 3 financial years (i.e. current year and three previous financial years) from the date of opening of tender. The bidder shall also furnish Supply/ work completion certificate issued by customer/s for the Purchase Orders/ Work Orders Copy of work orders supported with relevant documentary evidences for the same and the completion certificates issued by customer/s for the Purchase Orders/ Work Orders. Documentary evidence should clearly indicate the nature of systems implemented for each project.	We would request to Relax/ amend the clause as under: The tenderer should have executed Single order showcasing supply, installation, testing, commissioning , implementation and operations projects for Data Center solutions commercially costing not less than 35% of the tendered value during last preceding 3 financial years (i.e. current year and three previous financial years) from the date of opening of tender. OR Bidder should have executed single OR Multiple orders for IT&ES/ICT/IT Products. OR under execution of Command Control Center project/DC-DR. The bidder shall also furnish Supply/ work completion certificate issued by customer/s for the Purchase Orders/ Work Orders Copy of work orders supported with relevant documentary evidences for the same and the completion certificates issued by customer/s for the Purchase Orders/ Work Orders. Documentary evidence should clearly indicate the nature of systems implemented for each project.	By mentioning single order for supply, installation, testing, commissioning, implementation and operations projects for Data Center solutions commercially costing not less than 35% of the tendered value is restricting to the prospective bidder to participate in your valuable tender. We would request to kindly relax the clause as requested for larger participation.		As per RFP
44	SOR-B, B-3	5	Software defined Storage, Virtualization Virtual Cloud Foundation& Site Recovery License as per Technical Specification given in chapter-3A	Based on the requirement kindly amend this line for clarity as: "Software defined Storage, Cloud Management Platform, SDN & Site Recovery License as per Technical Specification given in chapter-3A"	Amendment required for more clarity and to avoid any ambiguity		As per RFP
45	SOR-B- Cloud Solution –B-3- Software defined Storage, Virtualization Virtual Cloud Foundation & Site Recovery License:	29	SOR-B- Cloud Solution –B-3- Software defined Storage, Virtualization Virtual Cloud Foundation & Site Recovery License:	Based on the requirement kindly amend this line for clarity as: "Software defined Storage, Cloud Management Platform, SDN & Site Recovery License as per Technical Specification given in chapter-3A"	Amendment required for more clarity and to avoid any ambiguity		As per RFP

46	4. Scope of Work-xiii	15	xiii. Bidder needs to integrate the cloud platform with existing LDAP solution in RailTel. xvi. Offered cloud solution version should be latest and bidder needs to perform the migration/upgradation activity of the existing cloud solution to maintain uniformity of entire cloud solution.	Kindly add following clause "VMware cloud management paltform is already setup in existing private cloud at RailTel. For VMware solution, scope will be to 1. Prepare new servers being procured as part of this tender and add them as part of existing cloud setup for expansion . 2. Migrate existing NSX-V to NSX-T 3. Integration of cloud portal with Multi factor authentication solution being procured in this tender	We understand that for VMware solution all this activities are not be applicable as VMware cloud management paltform is already setup and as part of scope new servers being procured as part of this tender neds to be prepared and added in existing cloud setup for expansion.		Clarification: Complete scope of work has been defined considering both scenarios that bidder may propose Vmware CMP or may propose entirely new CMP platform . If bidder is proposing Vmware CMP than high level SOW to be read as but not limited to " VMware cloud management paltform is already setup in existing private cloud at RailTel. For VMware solution, scope will be to 1. Prepare new servers being procured as part of this tender and add them as part of existing cloud setup for expansion . 2. Migrate existing NSX-V to NSX-T 3. Integration of cloud portal with Multi factor authentication solution being procured in this tender 4. Implement SSO for cloud management software components for 15 to 20 administrators. 5. Replicate cloud management components to DR site " If Bidder propose new CMP platform , then bidder has to perform all the activities as defined in tender."
47	7-iv	17	iv. Integrate Virtualization Manager with Cloud Management Platform (CMP), Software Defined Network (SDN) & Software Defined Storage (SDS). vi. Create Virtual machines for Linux OS or Windows, Virtual machine templates, Virtual machine configured in High Availability mode in cluster, affinity group creation of virtual machines and virtual machine backup configuration (Snapshot and Clone). vii. Configure storage policies to automate provisioning and balancing of storage resources to ensure that each VM gets the specified storage resources and services. viii. Bidder shall perform integration of HCI with the supplied backup solution and should enable integration with VM to perform backup of VM data and configuration files.	4. Implement SSO for cloud management software components for 15 to 20 administrators 5. Replicate cloud management components to DR site "			

48	8	17	"i. Bidder should integrate the CMP fully with the supplied HCI solution i.e., integration with manager of the hypervisor, Software Defined Network, Software Defined Storage, etc." "ii. The bidder should create policy-based controls of cloud resources and should configure Rolebased policy management, administration and enforce role- based policies." "iii. The bidder should create workflow and blueprints for IaaS, PaaS as defined in Functional Requirements" "iv. The bidder shall also create basic & necessary reports for the analysis of resources (CPU, Memory, Storage and Network) utilization and available resources." v. Bidder should configure auto-scaling of resource as per demand "vi. The bidder should configure CMP with, backup software to enable configuration of backup and restore through self- service Dashboard."				
49	SOR-B	29	The solution should have capability to automate the bring-up process of the entire software platform, including deployment of infrastructure VMs, creation of the management cluster, configuration of VLANs, virtual storage, virtual network, and cluster creation and provisioning.	We understand that VMware cloud management platform with management cluster is already setup in existing RailTel private cloud. So this clause is not applicable. Kindly confirm.	VMware cloud management platform along with management cluster is already setup in existing RailTel private cloud. So bring-up of software platform, management cluster, infrastructure VMs is not required		Clarification: Specification given considering the scenario that bidder may propose the extension of VMware CMP or may propose the entire new CMP.
50	SOR-B	32	The solution should provide true multi tenancy, Each tenant needs to be able to create their own profiles/blueprints, share them to a public catalog, and not be able to see other tenant's build profiles, compute resources, or managed machines. At least 3 tenants will be required to be configured during the Cloud deployment.	Kindly amend this as "The solution should provide true multi tenancy, Each tenant needs to be able to create their own profiles/blueprints, share them to a public catalog, and not be able to see other tenant's build profiles, compute resources, or managed machines. At least 3 Business Groups will be required to be configured during the Cloud deployment."	As per our understanding in present setup different departments are onboarded with business groups. More business groups can be created as per requirement of this clause.		As per RFP
51	SOR-B	31	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.	Request to kindly remove this clause	This feature is not part of the components asked at section 4 page 15 point xvi. Also kindly note this feature is not a part of currently running stack in RailTel eoffice project.		As per RFP

52	SOR –D Licenses for OS, DB and NMS/EMS	41	EDB PostGre SQL support system for DB servers - 860 Nos.	Kindly make it open and amend as "EDB/ VMware PostGre SQL support system for DB servers - 860 cores"	Amendment required to make it open and for wider participation		Corrigendum-III
53	SOR –D Licenses for OS, DB and NMS/EMS	41	EDB PostGre SQL support system for DB servers - 860 Nos.	Kindly mention the segregation for cores for active, passive, DR, reporting instances	Clarification required		Corrigendum-III
54	4. Scope of Work-xvi.	15	VMware Site Recovery Manager Standard Latest edition (25 VM Pack) or equivalent -6 Nos.	Kindly amend as "VMware Site Recovery Manager Enterprise Latest edition (25 VM Pack) -6 Nos."	Existing setup has Site Recovery Manager Enterprise edition		Corrigendum-III
55	4. Scope of Work-xvi.	15	VMware vSAN 6 or latest Enterprise for 1 Processor or equivalent - 105 Nos.	Kindly amend as "VMware vSAN Advanced 6 or latest for 1 Processor or equivalent - 105 Nos."	Existing setup is with vSAN Advanced.		Corrigendum-III
56	SOR-B	32	The solution should provide automatic private cloud metering and consumption analysis. The Cloud portal will be configured with Multi factor authentication during the deployment.	VMware Cloud portal already setup for RailTel e-Office will be configured with Multi factor authentication solution being procured as part of this tender. Supported authentication types are listed on this link. Would request that the asked MFA solution should be compatible as per this list. https://docs.vmware.com/en/vRealize-Automation/7.6/com.vmware.vra.prepare.use.doc/GUID-D16CB962-78B9-4FAD-92D5-E16613A381FF.html?hWord=N4lghgNiBclC4HcD2ACAZmAxnJAnFYArnABYcmAdnAJaZg1UgC+QA			Clarification: The solution should support following protocols for integration including Radius, SAML, RestAPI, OIDC, Web SDK etc or equivalent for providing MFA services.
57	SOR-B	33	There should be single portal to manage all the Cloud based management software using single sign on functionality.	We understand that this functionality is required for RailTel administrators and there would be 15 to 20 such users. Kindly confirm if we can propose the solution for 20 users.			Corrigendum-III
58	12.1.1	64	12.1.1 The Equipment offered by the OEM or equipment of the same series/family from the same OEM should have been satisfactorily working in Government/PSUs/Telecom Service Providers network for at least 12 months as on date of opening of tender, in India or Abroad. The certificates from the actual users will have to be submitted along with bid.	Kindly amend "12.1.1 The Equipment offered by the OEM or equipment of the same series/family from the same OEM should have been satisfactorily working in Government/PSUs/Telecom Service Providers network for at least 12 months as on date of opening of tender, in India or Abroad. The certificates from the actual users or publically available references/ case studies will have to be submitted along with bid."	Kindly amend to accept the publically available customer references/ case studies		As per RFP

59	12.1.2	64	12.1.2 The OEM should have supplied at least 35% of the tendered value/SOR Value of the equipment offered or equipment of the same series/family during last preceding 3 financial years (i.e. current year and three previous financial years) as on opening of bid to Government/PSUs/Telecom Service Providers. OEM should submit self-certificate with proper contact detail of clients along with PO reference and amount supplied (Firm Name, Contact person, Designation, Telephone Number, Fax, Official mail id etc.). The same should be issued by authorized signatory.	We understand that Global Government/PSUs/Telecom Service Providers references will be acceptable. Kindly confirm			Corrigendum-III
60	SOR-C- Network –C-2 –End point protection for end user	41	27. The endpoint solution shall be able to pinpoint vulnerable versions of popular applications installed in Endpoints	The endpoint solution shall be able to protect vulnerable versions of popular applications installed in Endpoints with multi-layered prevention.	Protection is key for all applications and processes. By identifying attacker behaviour with Tactics, Techniques and Procedures organizations can stay ahead of vulnerabilities by having multi-layered prevention of these behaviours.		Corrigendum-III
61	SOR-C- Network –C-2 –End point protection for end user	41	22. The proposed solution shall have the capability to quarantine the malicious application/program/file automatically without quarantining the entire user machine from network which would affect business productivity of the user	The proposed solution shall have the capability to quarantine the malicious application/program/file automatically without quarantining the entire user machine from network which would affect business productivity of the user. The solution should also include the capability to isolate the host if required to protect from lateral movement.	Host Isolation provides an additional layer of security control where is a user or endpoint is remote, it enables the security team to quickly isolate the endpoint on incident detection (for critical incidents) until they inspect for forensics and next steps.		As per RFP
62	SOR-C- Network –C-2 –End point protection for end user	41	23. The proposed solution shall have the capability to work with Indicators of Compromise (IOC's)	The proposed solution shall have the capability to work with Indicators of Compromise (IOC's) and correlate MITRE ATT&CK Tactics Techniques & Procedures (TTPs)	IOC's are post-breach or reactive in nature. Tactics, Techniques and Procedures enable organizations to hunt proactively for attacker behavior and are now a widely adopted standard across all endpoint security solutions. Reference: attack.mitre.org		As per RFP
63	SOR-C- Network –C-2 –End point protection for end user	41	28. The proposed solution shall be able to identify the threat root cause of incidents, child processes of malwares and parent file disposition	The proposed solution shall be able to identify the threat root cause of incidents, child processes of malwares and parent file disposition, network connections, registry modifications, scripts executed and targets injected.	Metadata such as network connections, registry modifications, injections and script executions are crucial to uncovering all stages of the attack and artifacts from a single console.		As per RFP
64	SOR-C- Network –C-2 –End point protection for end user	41	32. Solution should allow Users to choose to preview the new Policy UI.	The solution should allow administrators to identify policy effects based on historical data before apply the Prevention policy.	It should enable administrators to intelligently push policies that work with minimal disruption to the end user by identifying possible conflicts or business application effects of enabling a specific feature Using the historical data that is gathered by the solution.		Corrigendum-III

65	SOR-C- Network –C-2 –End point protection for end user	40	Additional Clause	The proposed solution should include the capability for security admins to remotely connect to endpoint via secure shell for live forensics, data collection and remote remediation even when the endpoint is off the corporate network.	Remote shell capability will enable Railtel to remotely triage, investigate and gather forensics from endpoints not on the corporate network - such as a WFH scenario / on field scenario.		As per RFP
66	SOR-C- Network –C-2 –End point protection for end user	40	Additional Clause	The proposed solution should have the capability to perform threat hunting based on MITRE TIDs, Tactics, Techniques & Procedures and IOCs.	Hunting on TIDs / TTPs enables Railtel to hunt proactively in the environment for suspicious behaviors, while IOC hunting identifies breach artifacts. Both are essential in identifying todays modern attacks.		As per RFP
67	SOR-C- Network –C-2 –End point protection for end user	40	Additional Clause	The proposed solution should include actionable threat intelligence capabilities on the latest attack campaigns - including observed TTPs, policy recommendations, IOCs.	Actionable threat intelligence will enable Railtel team to stay ahead of emerging attacks and enrich existing security stack.		As per RFP
68	3.5	60	For AMC he will be paid @ 3.5% per annum only. If the Tenderer quotes a higher base rate for AMC, he will be paid at his quoted rate per annum and five-year differential cost shall be added to offered cost. AMC would have to be valid for minimum period of 5 years after the warranty.	1) Kindly remove this clause, as a Software OEM, we do not offer AMC for our Software licences at this rate per annum. This is not the Industry standard for AMC for Software. 2) Also please advise if the total Comprehensive Support period is 5 years (Warranty period to be taken as per Page 77, Clause 2)	In this clause it is mentioned 5 years after the warranty period.		As per RFP
69	1	19	The offered storage should be a true symmetric active-active storage	The offered storage should be a Dual active-active controller storage or higher. In case of any controller failure, the workload from failed controller should automatically failover/move to the active controller without any manual intervention.	Clarifying the functionality required from the active-active controller configuration		Clarification: Our requirement is to achieve enterprise class storage functionalities wherein host can access all the luns through all the controllers simultaneously. Asymmetric/ALUA, in case of failover might require more storage system resources and a longer response time per I/O.
70	2	19	The Storage Systems should be supplied with minimum 600TB Usable capacity using 500 capacity on SAS/NLSAS Drives on RAID6 and 100TB using SSD on RAID 6 and scalable up to 1PetaByte usable capacity using SAS/SSD.	The Storage Systems should be supplied with minimum 1100TB Usable capacity using 1000TB on SAS/NLSAS Drives on RAID6 and 100TB using SSD on RAID 5. The Storage should be scalable up to Double of usable capacity or higher.	* The rack server speciifications also asks for 480TB usable capacity to be added on the SAN Stroage. Hence the capacity needs to be changed to ~1100TB (600TB + 480TB). * Also request you to remove the 480TB Capacity requirement from the rack server specifications.		Corrigendum-III
71	4	19	The Storage should be scalable to at least 800 SFF/LFF disk drives on the same set of controllers.	The Storage should be scalable to at least 1500 SFF/LFF disk drives or higher.	The specifications asks for 1100TB of usable capacity on day one hence the storage should be power enough to support large number of disk drives to support scalability in future.		Clarification: As per RFP, However bidder may propose higher storage scalable capacity.

72	8	19	Storage should be equipped with 8*32 Gbps FC ports, 4*10Gbe port for host connectivity. Required SFPs/Optical Module to be populated from day one	Storage should be equipped with 8x32Gbps / 16 x 16 Gbps FC ports and 4 x 10Gbe SFP+ port for host connectivity. Required SFPs/Optical Module to be populated from day one The ports should support both Block (FC & iSCSI) and File (NFS & CIFS/SMB) protocols.	The RFP specification asks for a unified storage while the specifications does not mentions about NAS/File protocols. Hence request you to please add the same in this clause.		As per RFP
73	17	19	The proposed storage system should support at least 24000 LUNs or volumes	The proposed storage system should support at least 6000 LUNs/ volumes or higher	In the current project, the required usable capacity (expandable) is ~2000TB. If the average size of each volume is 20TB then the max. volumes/LUNs which can be created are 100. Even if we consider 5 times the number of volumes to be created then also the max. volumes required is 500. Hence we request you to please change the clause as requested to increase bidders participation.		Corrigendum-III
74	25.1	20	Proposed storage system should support third-party storage virtualization natively or using another headers in High availability from day1. Necessary licenses and hardware on High availability should be supplied from day1.	The solution should include data migration from old/existing storage to the new/proposed storage system without any data loss. The migration and data protection during migration responsibility lies completely with the bidder. RAILTEL will assist the migration team with support related to the existing infrastructure for the data migration purpose.	The primary purpose of this clause is to get the data migrated from the existing storage to the new storage without any data loss.		Corrigendum-III
75	8	23	12Gbps PCIe 3.0 with RAID 1, 5, 6,10, 50 with 2GB cache	Request to amend the clause as - “12Gbps PCIe 3.0 with RAID 1, 5, 6,10, 50 with 2GB cache OR 12Gbps PCIe 3.0 SAS HBA”	The vSAN certified ready servers come with 12Gbps SAS HBA for pass-through functionality as per vSAN deployment guidelines. vSAN solution deployment doesn’t require hardware RAID controller and needs only a pass-through SAS HBA as per vSAN architecture and compatibility.		Corrigendum-III
76	9	23	2 nos. of 960GB SATA M.2 in mirrored configuration for OS	Request to amend the clause as - “2 nos. of 480GB or higher SATA M.2 in mirrored configuration for OS”	960GB SATA M.2 Boot Flash disks are not available with all the leading OEMs. Moreover 480GB capacity is more than sufficient for vSphere hypervisor and OS installation.		Corrigendum-III
77	5	24	The switching OEM should be part of latest Gartner's Leader Quadrant for Data Center networking.	The switching OEM should be part of latest Gartner's Magic Quadrant for Data Center networking.	Most of the OEMs are in Latest Gartner report on Data Centre Networking, but may not in a leaders position, in order to have a healthy competition, we request to allow OEMs from Challengers/Visionaries quadrant as well.		Corrigendum-III
78	12	25	Switch should have a minimum 40MB buffer of more.	Switch should have a minimum 32 MB buffer of more.	Request for Change to 32 MB Buffer for us to participate		As per RFP
79	40	26	Switch should support MPLS segment routing and VRF route leaking functionality from day 1.	Switch should support VRF route leaking functionality from day 1.	MPLS is required on Wan Routers orSdwan CPE and not inside Data Centre fabric In Page 18 Tender RFP DC Network Connectivity diagram MPLS is terminated on DC router so MPLS is not required in Internal Data centre Fabric		As per RFP
80	5	35	The switching OEM should be part of latest Gartner's Leader Quadrant for Data Center networking.	The switching OEM should be part of latest Gartner's Magic Quadrant for Data Center networking	Most of the OEMs are in Latest Gartner report on Data Centre Networking, but may not in a leaders position, in order to have a healthy competition, we request to allow OEMs from Challengers/Visionaries quadrant as well.		Corrigendum-III

81	12	36	Switch should have a minimum 40MB buffer of more.	Switch should have a minimum 32 MB buffer of more.	Request for Change to 32 MB Buffer for us to Participate		As per RFP
82	40	37	Switch should support MPLS segment routing and VRF route leaking functionality from day 1.	Switch should support VRF route leaking functionality from day 1.	MPLS is required on Wan Routers or Sdwan CPE and not inside Data Centre fabric MPLS is terminated on DC router so MPLS is not required in Internal Data centre Fabric		As per RFP
83	4. Scope of Work-Point XII	15	Any Management switches required for the proposed solution will be provisioned by the bidder in redundant topology.	Please clarify if each rack will have dedicated Management switch (2 nos in HA) to connect to all out of band Management port of all servers and switches on Rack . This switch will then Uplink to Dual 24 port 10G Aggregation Switch on 10G multimode fiber .	Please specify the qty of Access Management switch 24 port Gigabit with 2x 10G uplink and 2 Nos 24 Port 10G Aggregation Switch . No of Access Management Switch= N (No of racks) in HA mode 2 nos required per Rack , 2 nos Aggregation Switch 24 x 10 G Please specify qty as it will be equivalent to all to Bidders . Also For full redundancy in Management network , dual Access Management Switches to be proposed per rack .		Clarification: Bidder needs to provide Minimum 2 numbers of management switch in DC and Two numbers in DR. 48 port 10/100/1000 BaseT with 4x10G uplink Switch with Redundant Power supply and stackable Switch. If in case bidder requires more ports as per the solution proposed , bidder to provision accordingly.
84	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 1	20	Backup software proposed should be in Gartner's leader quadrant of the latest Gartner Magic Quadrant report for Data Protection / Backup Software.	Backup software proposed should be in Gartner's leader quadrant of the latest Gartner Magic Quadrant report for Data Center Backup & Recovery Solution published in year 2019.	Request you to please modify considering the latest report from Gartner's.		Corrigendum-III
85	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 4	21	Backup software should be totally agentless but should support application aware backups for MS SQL, Oracle, SAP HANA, Exchange transaction logs with non-staged granular recovery of all these applications. It should support crash consistent VM level backup for all other workloads.	Backup software should be totally agentless with VM image level backup and should support application aware backups for MS SQL, Oracle, SAP HANA, Exchange transaction logs with non-staged granular recovery of all these applications. It should support crash consistent VM level backup as well.	Request you to please modify this clause being language used here is single OEM specific. Hence, we request you to please accept the changes suggested here.		Corrigendum-III
86	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 5	21	The Data protection services should be hosted on Scale out solution using software defined storage. The solution should be Multi-controller architecture to be quoted with 4 controllers/nodes having 256GB Cache/Memory per Controller/Node.	The Data protection services should be hosted on Purpose built backup appliance (PBBA). The solution should be Multi-controller architecture to be quoted with 2 controllers having 768 GB RAM per Controller.	PBBA is widely accepted technology by world leading organizations in India as well as National Informatics Center using PBBA in multiple National Data Center's & Mini Cloud in many states in India.		Corrigendum-III
87	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 6	21	Backup solution should be provided for 500TB usable Disk based backup storage capacity (only at DC) leveraging 10TB NL-SAS drives on erasure coding or equivalent with protection of data against simultaneous 2 (Two) disk Failure with rack awareness and encryption functionality.	Backup solution should be provided for XX TB usable capacity purpose built backup appliance storage capacity (only at DC) leveraging 8TB NL-SAS drives with RAID 6 protection of data against simultaneous 2 (Two) disk Failure with one hot spare drive per disk shelf enclosure and encryption functionality.	PBBA is widely accepted technology. Hence we suggest here to include PBBA instead of commodity storage. Also request you to place front end data need to be backup here in place of XX.		Corrigendum-III

88	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 7	21	Backup solution shall be able to scale more than three times the current proposed usable capacity in a scale-out fashion.	Backup solution shall be able to scale more than Two times the current proposed usable capacity.	Scale out architecture is used in unstructured data storage and does not have any relevance to PBBA and backup solution. Hence we request you to please modify this clause to make leading backup solution OEM's to propose the backup solution.		As per RFP
89	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 8	21	The Software defined storage solution should provide multiprotocol support NFS, SMB & S3 and should have native protection from ransomware attacks or include third party antivirus scanning system using ICAP protocol any hardware required should be quoted from day 1	The proposed purpose built backup appliance should provide multiprotocol support CIFS, NFS, FC, VTL & OST and also provide methodology framework to safeguard backup data from ransomware/malware attacks.	SMB & S3 protocol is used in NAS or commodity storage. All leading backup solution OEM's provide PBBA with suggested protocols. OST & VTL protocol are standard protocols of backup solution.		Corrigendum-III
90	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 10	21	Backup software should provide best RTOs and RPOs through booting of Virtual Machines directly from the Backup to reduce the downtime.	Backup solution should provide 10 minutes RTOs and RPOs as per the last successful backup by booting of Virtual Machines directly from the Backup appliance to reduce the downtime. Purpose built backup appliance should be capable to boot minimum 30 VM's simultaneously.	Backup solution should have capability to provide enough random IOPs to support Business Continuity thru backup data. Hence, we request you to please accept the changes suggested here.		As per RFP
91	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 11	21	Backup software should have integrated data de-duplication engine with multi-vendor storage support to save space by storing de-duplicated copies of data. The deduplication engine should also facilitate IP base replication of de-dupe data. All necessary hardware and software required to support this functionality should be supplied along with other components	Backup solution should have integrated data de-duplication engine to save space by storing de-duplicated copies of data. The deduplication engine should also facilitate IP base replication of de-dupe data. All necessary hardware and software required to support this functionality should be supplied along with other components	Request you to please modify this clause being language used here is single OEM specific. Hence, we request you to please accept the changes suggested here.		Corrigendum-III
92	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 13	21	Backup software must have a feature of data validation, whereby a workload is powered-on in a sandbox environment and tested for its recoverability.	Backup solution must have inbuilt feature of data validation, where data validation is continuous process. This ensures backup data written on PBBA is can't modified and can be restored in the same state.	Request you to please modify this clause being language used here is single OEM specific. Hence, we request you to please accept the changes suggested here.		Corrigendum-III
93	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 14	21	Recovery verification should automatically boot the server from backup and verify the recoverability of VM image, Guest OS and Application Consistency.		Request you to delete this clause being the same requirement is mentioned in Point No. 13. Hence, we request you to please accept the changes suggested here.		As per RFP

94	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 15	21	The software should support varieties of backup mechanisms like Full, Incremental, and Differential etc. at different frequencies i.e. yearly, monthly, weekly, daily, hourly etc. as per defined policy. It should also have calendar-based backup scheduling. The restoration should also be supported accordingly.				As per RFP
95	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 16	21	Proposed backup Software shall support seamless integration with existing Backup solution for a wholistic view and better Management.	Proposed backup appliance shall support seamless integration with existing Backup solution for a wholistic view and better Management.	Two different backup cannot be managed by single console, however the purpose built back appliance can integrate with multiple leading backup software OEM's. Like wise Dell Data Domain can integrate with Veeam, Networker, etc.		Clarification: Bidder is allowed to quote new Backup solution (Existing & New requirement) on a new platform to provide single Management console.
96	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 19	21	The proposed Backup software must allow to configure the maximum acceptable I/O latency level for production data stores to ensure backup and replication activities do not impact storage Availability to production workloads		Request you to delete this clause since it is forfeiting the backup performance and restore of backup data.		Corrigendum-III
97	New Point to be added - Functional requirement of backup solution	New		The offered Purpose-built backup appliance should be sized appropriately for backup of front-end data of XX TB (XX % File System and XX % DB) as per below mentioned backup policies: - oDaily Incremental Backup – retained for 28 Days in the backup appliance. - oWeekly Full Backup for all data types – retained for 4 Weeks in the backup appliance. - oMonthly Full Backups – Retained for 12 Months in the same backup appliance. - oYearly Full Backups - Retained for 5 years in the same backup appliance. The offered purpose-built backup appliance should be quoted with at least XX TB usable capacity post RAID 6 and hot-spare penalty using 8TB or lesser capacity drives. The proposed backup appliance must be sized for adequate capacity with 10% YoY data growth and 2% daily change rate for the contract period. Any additional software or backup storage capacity (in addition to minimum XX TB usable capacity) or any other component required as per sizing needs to be provided by the OEM & bidder during the time of bidding for entire warranty period of 5 years.			As per RFP

98	New Point to be added - Functional requirement of backup solution	New		The proposed Purpose-built backup appliance should support retention lock (WORM) feature which ensures that no user and administrator is allowed to data is deleted accidentally and support for point-in-time copies of a LUN or volumes with minimal performance impact. Even Administrator should not be able to delete the data deliberately or accidentally till the retention of the backup get expired. The offered backup appliance must have the ability of inbuilt target side data deduplication, WORM (Write Once Read Many), Replication and Encryption using AES 256 bit for data at-rest as well as in-flight while supporting VTL, CIFS, NFS and OST protocols over IP as well as FC.			As per RFP
99	New Point to be added - Functional requirement of backup solution	New		The offered backup solution must complete all backup within 8 hours backup window and the bidder must provide all the hardware and software to meet this requirement.			As per RFP
100	RAILTEL/TENDER/OT/CO /ITP/2020-21/ DC Solution /540	13	Veeam is the existing incumbent in the Backup Space. It would be recommended to have Backup Solution co-exist with incumbent solution and enhance the backup capacity. However bidder may propose any other backup solution which needs to be integrated with existing backup solution i.e. Veeam Backup Solution or propose entirely a new backup solution comprising existing and proposed solution capacity.		Two different backup software cannot be managed by single console and co-exist. Hence we request you to please remove Veeam reference from this RFP and ask the entire new backup solution and follow the standard terms of RFP.		As per RFP
101	CHAPTER-3-A	20	SOR-A-Storage – A-2 – Backup solution at DC & DR	The Specifications for Backup Solution are only for Software and Disk Based Storage, and no specifications for Tape. Request: Inclusion of D2D2T Solution with Specifications	Comprehensive data protection with D2D2T provides two-stages of protection at significantly less cost than many tape (D2T) or disk-only solutions (D2D). With LTO Tape we achieve longevity, scalability & Low Cost Per GB, and disk would get us quick file restoration.		As per RFP
102		New		Request for Specifications for Dedicated Tape Backup to be included as a Part of D2D2T Backup Strategy.	The purpose of an offline backup is to remain unaffected should any incident impact your Online environment. LTO Tape Automation would be ideal. With at least one backup offline at any given time, an incident cannot affect all of your backups simultaneously.		As per RFP
103		New		Tape Library (DC & DR): Technical Specifications	A). Minimum 80 Slots LTO Tape Automation. B) Minimum 8 x LTO8 FC Drives considering ~50% Backup Efficiency, should be able to Restore approx 50TB in 12 Hours Window. C)Minimum 50 x LTO8 Media		As per RFP
104	CHAPTER- 2 SCHEDULE OF REQUIREMENT	5	Backup Solution at DC and DR along with Tape/Disk Based storage as per specification given in Chapter-3A	Is the Backup Solution (Backup Software & Tape/Disk Hardware) is required each at DC & DR	UOM says Lot : 01.		Clarification: Backup software required each at DC & DR while 500TB Disk Storage required only at DC.

105	Preference: Make In India	68	21.3: Requirement of Purchase Preference	In procurement of goods in respect of which the Nodal Ministry has communicated that there is sufficient local capacity and local competition, and where the estimated value of procurement is Rs.50 Lakhs or less, only local suppliers shall be eligible. If the estimated value of procurement of such goods is more than Rs.50 Lakhs, the provisions of subparagraph b or c as the case may be, shall apply.	Will Railtel prefer Indian OEM/technology provider for SOR category mentioned in the Tender to encourage Indian OEM	This clause is to be enforced for each category of the SOR .	As per RFP
106	Authenticated for VPNs, firewall for access in MFA	New	Authenticated for VPNs, firewall for access in MFA	The MFA should be integrated with access integrator for users to access seamlessly	whether the proposed solution can be accessed any time anywhere and can scale up without change of hardware and scale up for VPN as well as VDI. Why Railtel should us multiple systems/device for MFA and VPN access. Reduction in TCO for life cycle management and maximise ROI on security	Proposed solution should be built with access integrator. In case vendor wants to deploy seamless access the same should be offered to see the users access eoffice seamlessly from home. Access and MFA on a single hardware will be preferred. The access solution to be integrated with MFA working on deployed eoffice solution should be provided	As per RFP
107	General Functionalities	46	MFA	The project is for DC Infra for eoffice. Whether the solution is deployed for prevalent eoffice application of NIC	Whether Railtel would like to accept the credibility of The proposed solution to be deployed on eoffice application to evaluate specific eligibility rather than General eligibility criteria	The MFA must have been deployed on eoffice application for at least 1000 users/licenses	As per RFP
108	MFA	47	The proposed solution should support soft token (TOTP) / Hardware Token / Push Notification (SMS) / Email / App Based etc..	The solution should support Biometric authentication solution that can work with 3rd party biometric solution. Biometric should also be considered as one of factor of authentication	Biometric is always an important factor of Multifactor authentication. The solution should support the facility. Biometric devices will be purchased as and when required	MFA must have the facility to support Biometric	Corrigendum-III
109	Scalability	New	MFA	Solution scalability and authentication	The solution should have in built Biometric authentication	The solution should come with built-in biometric authentication server (with additional licenses) in case customer want to use the solution from same OEM.	Clarification: The proposed solution must support Biometric device as and when procured by RailTel.
110	Scalability	New	MFA	Support for different Biometric device	Any MFA solution has Biometric as one of its factor of authentication. Biometric solution can be deployed on the same hardware/software. Solution should be open and should not be vendor lock in	The proposed solution must support Biometric device as and when procured by Railtel. The devices should be not vendor locking	Clarification: The proposed solution must support Biometric device as and when procured by RailTel.
111		New	MFA	Secure authentication	In Cyber Experts Pass words are generally weak and useful data can be leaked from Data Centre which can create damage to the organisation	The solution should allow password less authentication to ensure minimising the leakage, theft, and severity of loss of IT assets	As per RFP
112		New	MFA	Secure authentication	Futuristic MFA without cost impact to Railtel	The solution should support FIDO keys for authentication	As per RFP

113		New	MFA	LDAP Support		The solution should be supported on LDAP or local database	Clarification: "The solution should be supported on LDAP or local database."
114	The proposed solution should support soft token (TOTP) / Hardware Token / Push Notification (SMS) / Email / App Based etc..	47	MFA		The proposed solution should support soft token (TOTP) / Hardware Token / Push Notification (SMS) / Email / App Based etc..	The proposed solution should support soft token (TOTP)/Hardware Token/Push Notification /SMS /Email/ App based etc.	Corrigendum-III
115	Solution Access	New			No of Named user to use MFA	Kindly provide the no of Named users who will use MFA to access eoffice from anywhere/home	As per RFP
116	Preference: Make In India	67	21.3: Requirement of Purchase Preference	In procurement of goods in respect of which the Nodal Ministry has communicated that there is sufficient local capacity and local competition, and where the estimated value of procurement is Rs.50 Lakhs or less, only local suppliers shall be eligible. If the estimated value of procurement of such goods is more than Rs.50 Lakhs, the provisions of subparagraph b or c as the case may be, shall apply.	Will Railtel prefer Indian OEM/technology provider for SOR category metioned in the Tender to encourage Indian OEM	This clause is to be enforced for each category of the SOR .	As per RFP
117	General Functionalities	46	Authenticated for VPNs,firewall for access in MFA	The MFA should be integrated with access integrator for users to access seamlessly	whether the proposed solution can be accesed any time any where and can scale up without change of hardware and scale up for VPN as well as VDI.Why Railtel should us multiple systems/device for MFA and VPN access.Reduction in TCO for life cycle management and maximise ROI on security.	Proposed solution should be built with access integrator.In case vendor wants to deploy seamless access the same should be offered to see the users access eoffice seamlessly from home.Access and MFA on a single hardware will be preferred.The access solution to be integrated with MFA working on deployed eoffice solution should be provided	As per RFP
118	General Functionalities	46	MFA	The project is for DC Infra for eoffice .Whether the solution is deployed for prevalent eoffice application of NIC	Whether Railtel would like to accept the credibility of The proposed solution to be deployed on eoffice application to evaluate specific eligibility rather than General eligibility criteria	The MFA must have been deployed on eoffice application for at least 1000 users/licenses	As per RFP
119	MFA	47	The proposed solution should support soft token (TOTP) / Hardware Token / Push Notification (SMS) / Email / App Based etc..	he solution should support Biometric authentication solution that can work with 3rd party biometric solution.Biometric should also be considered as one of factor of authentication	Biometric is always an imortant factor of Multifactor authentication.The solution should support the facility.Biometric devices will be purchased as and when required	MFA must have the facility to support Biometric	Corrigendum-III
120	Scalability	New	MFA	Solution scalability and authentication	The solution should have in built Biometric authentication	The solution should come with built-in biometric authentication server (with additional licenses) in case customer want to use the solution from same OEM.	Clarification: The proposed solution must support Biometric device as and when procured by RailTel.

121	Scalability	New	MFA	Support for different Biometric device	Any MFA solution has Biometric as one of its factor of authentication.Biometric solution can be deployed on the same hardware/software.Solution should be open and should not be vendor lock in	The proposed solution must support Biometric device as and when procured by Railtel.The devices should be not vendor lockin	Clarification: The proposed solution must support Biometric device as and when procured by RailTel.
122		New	MFA	Secure uthentication	In Cyber Experts Pass words are generally weak and useful data can be leaked from Data Centerwhich can create damage to the organisation	The solution should allow password less authentication to ensure minimising the leakage,theft and severity of loss of IT assets	As per RFP
123		New	MFA	Secure authentication	Futuristic MFA without cost impact to Railtel	The solution should support FIDO keys for authentication	As per RFP
124		New	MFA	LDAP support		The solution should be supported on LDAP or local database	Clarification: "The solution should be supported on LDAP or local database."
125	The proposed solution should support soft token (TOTP) / Hardware Token / Push Notification (SMS) / Email / App Based etc..	47	MFA		The proposed solution should support soft token (TOTP) / Hardware Token / Push Notification (SMS) / Email / App Based etc..	The proposed solution should support soft token (TOTP)/Hardware Token/Push Notification /SMS /Email/ App based etc.	Corrigendum-III
126	Solution Access	New			No of Named user to use MFA	Kindly provide the no of Named users who will use MFA to access eoffice from anywhere/home	As per RFP
127	12.2.1	64,78	The tenderer should have executed Single order showcasing supply, installation, testing, commissioning, implementation and operations projects for Data Center solutions commercially costing not less than 35% of the tendered value during last preceding 3 financial years (i.e. current year and three previous financial years) from the date of opening of tender. The bidder shall also furnish Supply/ work completion certificate issued by customer/s for the Purchase Orders/ Work Orders. Copy of work orders supported with relevant documentary evidences for the same and the completion certificates issued by customer/s for the Purchase Orders/ Work Orders. Documentary evidence should clearly indicate the nature of systems implemented for each project.	We request to amend the clause as follows:- The tenderer should have executed Single order for IT/ITES/ICT/Telecom Sector/Data Centre Solutions/System Integration Services with one of the component as - supply, installation, testing, commissioning, implementation of Hardware & software equipments for Data Center solutions/Expansion of Data Centre / EMS / NMS/ Network Operation Centre / Command Control Centre. The total value of such project should not be less than 35% of the tendered value during last preceding 3 financial years (i.e. current year and three previous financial years) from the date of opening of tender. The bidder shall also furnish Supply/ work completion / phase completion certificate issued by customer/s for the Purchase Orders/ Work Orders.	Setting up NoC / EMS requires similar skill set and competency that requires for Data Center Solutions. This would increase the participation and competitiveness in the tender.		As per RFP

128	NIT	2	Earnest Money (EMD): Rs 35,68,500/- to be made in favor of RailTel online through IREPS Portal.	Two different amounts against EMD are mentioned in the tender document. We request you to confirm which one to be adhered.	Contradiction arised due to two different values.		Corrigendum-III
129	Clause 20	78	Earnest Money Deposit (EMD)/ Bid Security Rs. 36,06,000/- (Rs. Thirty Six Lakh Six Thousand only)				Corrigendum-III
130	44c)	76	Bidder of Indian origin shall submit the Integrity Pact (in 2 copies) on a non-judicial stamp paper of Rs. 100/- duly signed by the person signing the bid. If the bidder is a partnership or a consortium, the Integrity Pact shall be signed by all the partners or consortium members.	We understand that consortium is allowed in this tender and consorium bidder collectively need to comply the eligibility criteria. Please confirm.	Allowing consortium will increase bid participation and competitiveness.		As per RFP
131	Chapter 3A - 2 (vii)	12	Core router for DC & DR	Requirement of core router is given in Solution Building Block, however detailed techincal specifications is not given. Request to add the specification of core routers required in DC & DR.	Technical specification is must to offer a fully complied product		Corrigendum-III
132	SOR-B, B-3	5	Software defined Storage, Virtualization Virtual Cloud Foundation& Site Recovery License as per Technical Specification given in chapter-3A	Based on the requirement kindly amend this line for clarity as: "Software defined Storage, Cloud Management Platform, SDN & Site Recovery License as per Technical Specification given in chapter-3A"	Amendment required for more clarity and to avoid any ambiguity		As per RFP
133	SOR-B- Cloud Solution –B-3- Software defined Storage, Virtualization Virtual Cloud Foundation & Site Recovery License:	29	SOR-B- Cloud Solution –B-3- Software defined Storage, Virtualization Virtual Cloud Foundation & Site Recovery License:	Based on the requirement kindly amend this line for clarity as: "Software defined Storage, Cloud Management Platform, SDN & Site Recovery License as per Technical Specification given in chapter-3A"	Amendment required for more clarity and to avoid any ambiguity		As per RFP

134	4. Scope of Work-xiii	15	xiii. Bidder needs to integrate the cloud platform with existing LDAP solution in RailTel. xvi. Offered cloud solution version should be latest and bidder needs to perform the migration/upgradation activity of the existing cloud solution to maintain uniformity of entire cloud solution. iv. Integrate Virtualization Manager with Cloud Management Platform (CMP), Software Defined Network (SDN) & Software Defined Storage (SDS). vi. Create Virtual machines for Linux OS or Windows, Virtual machine templates, Virtual machine configured in High Availability mode in cluster, affinity group creation of virtual machines and virtual machine backup configuration (Snapshot and Clone).	Kindly add following clause "VMware cloud management paltform is already setup in existing private cloud at RailTel. For VMware solution, scope will be to 1. Prepare new servers being procured as part of this tender and add them as part of existing cloud setup for expansion . 2. Migrate existing NSX-V to NSX-T 3. Integration of cloud portal with Multi factor authentication solution being procured in this tender4. Implement SSO for cloud management software components for 15 to 20 administrators 5. Replicate cloud management components to DR site "	We understand that for VMware solution all this activities are not be applicable as VMware cloud management paltform is already setup and as part of scope new servers being procured as part of this tender needs to be prepared and added in existing cloud setup for expansion.		Clarification: Complete scope of work has been defined considering both scenarios that bidder may propose VMware CMP or may propose entirely new CMP platform . If bidder is proposing VMware CMP than high level SOW to be read as but not limited to " VMware cloud management paltform is already setup in existing private cloud at RailTel. For VMware solution, scope will be to 1. Prepare new servers being procured as part of this tender and add them as part of existing cloud setup for expansion . 2. Migrate existing NSX-V to NSX-T 3. Integration of cloud portal with Multi factor authentication solution being procured in this tender 4. Implement SSO for cloud management software components for 15 to 20 administrators. 5. Replicate cloud management components to DR site ". If Bidder propose new CMP platform , then bidder has to perform all the activities as defined in tender."
135	7-iv	17	iv. Integrate Virtualization Manager with Cloud Management Platform (CMP), Software Defined Network (SDN) & Software Defined Storage (SDS). vi. Create Virtual machines for Linux OS or Windows, Virtual machine templates, Virtual machine configured in High Availability mode in cluster, affinity group creation of virtual machines and virtual machine backup configuration (Snapshot and Clone). vii. Configure storage policies to automate provisioning and balancing of storage resources to ensure that each VM gets the specified storage resources and services. viii. Bidder shall perform integration of HCI with the supplied backup solution and should enable integration with VM to perform backup of VM data and configuration files.				

136	8	17	"i. Bidder should integrate the CMP fully with the supplied HCI solution i.e., integration with manager of the hypervisor, Software Defined Network, Software Defined Storage, etc." "ii. The bidder should create policy-based controls of cloud resources and should configure Rolebased policy management, administration and enforce role- based policies." "iii. The bidder should create workflow and blueprints for IaaS, PaaS as defined in Functional Requirements" Memory, Storage and Network) utilization and available resources." v. Bidder should configure auto-scaling of resource as per demand "vi. The bidder should configure CMP with, backup software to enable configuration of backup and restore through self- service Dashboard."				
137	SOR-B	29	The solution should have capability to automate the bring-up process of the entire software platform, including deployment of infrastructure VMs, creation of the management cluster, configuration of VLANs, virtual storage, virtual network, and cluster creation and provisioning.	We understand that VMware cloud management platform with management cluster is already setup in existing RailTel private cloud. So this clause is not applicable. Kindly confirm.	We understand that VMware cloud management platform with management cluster is already setup in existing RailTel private cloud. So this clause is not applicable. Kindly confirm.		Clarification: Specification given considering the scenario that bidder may propose the extension of VMware CMP or may propose the entire new CMP.
138	SOR-B	32	The solution should provide true multi tenancy, Each tenant needs to be able to create their own profiles/blueprints, share them to a public catalog, and not be able to see other tenant's build profiles, compute resources, or managed machines. At least 3 tenants will be required to be configured during the Cloud deployment.	Kindly amend this as "The solution should provide true multi tenancy, Each tenant needs to be able to create their own profiles/blueprints, share them to a public catalog, and not be able to see other tenant's build profiles, compute resources, or managed machines. At least 3 Business Groups will be required to be configured during the Cloud deployment."	As per our understanding in present setup different departments are onboarded with business groups. More business groups can be created as per requirement of this clause.		As per RFP
139	SOR-B	31	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.	Request to kindly remove this clause	This feature is not part of the components asked at section 4 page 15 point xvi. Also kindly note this feature is not a part of currently running stack in RailTel eoffice project.		As per RFP

140	SOR –D Licenses for OS, DB and NMS/EMS	41	EDB PostGre SQL support system for DB servers - 860 Nos.	Kindly make it open and amend as "EDB/ VMware PostGre SQL support system for DB servers - 860 cores"	Amendment required to make it open and for wider participation		Corrigendum-III
141	SOR –D Licenses for OS, DB and NMS/EMS	41	EDB PostGre SQL support system for DB servers - 860 Nos.	Kindly mention the segregation for cores for active, passive, DR, reporting instances	Clarification required		Corrigendum-III
142	4. Scope of Work-xvi.	15	VMware Site Recovery Manager Standard Latest edition (25 VM Pack) or equivalent -6 Nos.	Kindly amend as "VMware Site Recovery Manager Enterprise Latest edition (25 VM Pack) -6 Nos."	Existing setup has Site Recovery Manager Enterprise edition		Corrigendum-III
143	4. Scope of Work-xvi.	15	VMware vSAN 6 or latest Enterprise for 1 Processor or equivalent - 105 Nos.	Kindly amend as "VMware vSAN Advanced 6 or latest for 1 Processor or equivalent - 105 Nos."	Existing setup is with vSAN Advanced.		Corrigendum-III
144	SOR-B	32	The solution should provide automatic private cloud metering and consumption analysis. The Cloud portal will be configured with Multi factor authentication during the deployment.	VMware Cloud portal already setup for RailTel e-Office will be configured with Multi factor authentication solution being procured as part of this tender. Supported authentication types are listed on this link. Would request that the asked MFA solution should be compatible as per this list. https://docs.vmware.com/en/vRealize-Automation/7.6/com.vmware.vra.prepare.use.doc/GUID-D16CB962-78B9-4FAD-92D5-E16613A381FF.html?hWord=N4lghgNiBcIC4HcD2ACAZmAxnJAnFYArnABYcmAdnAJaZg1IUgC+QA			Clarification: The solution should support following protocols for integration including Radius, SAML, RestAPI, OIDC, Web SDK etc or equivalent for providing MFA services.
145	SOR-B	33	There should be single portal to manage all the Cloud based management software using single sign on functionality.	We understand that this functionality is required for RailTel administrators and there would be 15 to 20 such users. Kindly confirm if we can propose the solution for 20 users.			Corrigendum-III
146	12.1.1	64	12.1.1 The Equipment offered by the OEM or equipment of the same series/family from the same OEM should have been satisfactorily working in Government/PSUs/Telecom Service Providers network for at least 12 months as on date of opening of tender, in India or Abroad. The certificates from the actual users will have to be submitted along with bid.	Kindly amend "12.1.1 The Equipment offered by the OEM or equipment of the same series/family from the same OEM should have been satisfactorily working in Government/PSUs/Telecom Service Providers network for at least 12 months as on date of opening of tender, in India or Abroad. The certificates from the actual users or publically available references/ case studies will have to be submitted along with bid."	Kindly amend to accept the publically available customer references/ case studies		As per RFP

147	12.1.2	64	12.1.2 The OEM should have supplied at least 35% of the tendered value/SOR Value of the equipment offered or equipment of the same series/family during last preceding 3 financial years (i.e. current year and three previous financial years) as on opening of bid to Government/PSUs/Telecom Service Providers. OEM should submit self-certificate with proper contact detail of clients along with PO reference and amount supplied (Firm Name, Contact person, Designation, Telephone Number, Fax, Official mail id etc.). The same should be issued by authorized signatory.	We understand that Global Government/PSUs/Telecom Service Providers references will be acceptable. Kindly confirm			Corrigendum-III
148	SOR-C- Network –C-2 –End point protection for end user	41	27. The endpoint solution shall be able to pinpoint vulnerable versions of popular applications installed in Endpoints	The endpoint solution shall be able to protect vulnerable versions of popular applications installed in Endpoints with multi-layered prevention.	Protection is key for all applications and processes. By identifying attacker behaviour with Tactics, Techniques and Procedures organizations can stay ahead of vulnerabilities by having multi-layered prevention of these behaviours.		Corrigendum-III
149	SOR-C- Network –C-2 –End point protection for end user	41	22. The proposed solution shall have the capability to quarantine the malicious application/program/file automatically without quarantining the entire user machine from network which would affect business productivity of the user	The proposed solution shall have the capability to quarantine the malicious application/program/file automatically without quarantining the entire user machine from network which would affect business productivity of the user. The solution should also include the capability to isolate the host if required to protect from lateral movement.	Host Isolation provides an additional layer of security control where is a user or endpoint is remote, it enables the security team to quickly isolate the endpoint on incident detection (for critical incidents) until they inspect for forensics and next steps.		As per RFP
150	SOR-C- Network –C-2 –End point protection for end user	41	23. The proposed solution shall have the capability to work with Indicators of Compromise (IOC's)	The proposed solution shall have the capability to work with Indicators of Compromise (IOC's) and correlate MITRE ATT&CK Tactics Techniques & Procedures (TTPs)	IOC's are post-breach or reactive in nature. Tactics, Techniques and Procedures enable organizations to hunt proactively for attacker behavior and are now a widely adopted standard across all endpoint security solutions. Reference: attack.mitre.org		As per RFP
151	SOR-C- Network –C-2 –End point protection for end user	41	28. The proposed solution shall be able to identify the threat root cause of incidents, child processes of malwares and parent file disposition	The proposed solution shall be able to identify the threat root cause of incidents, child processes of malwares and parent file disposition, network connections, registry modifications, scripts executed and targets injected.	Metadata such as network connections, registry modifications, injections and script executions are crucial to uncovering all stages of the attack and artifacts from a single console.		As per RFP
152	SOR-C- Network –C-2 –End point protection for end user	41	32. Solution should allow Users to choose to preview the new Policy UI.	The solution should allow administrators to identify policy effects based on historical data before apply the Prevention policy.	It should enable administrators to intelligently push policies that work with minimal disruption to the end user by identifying possible conflicts or business application effects of enabling a specific feature Using the historical data that is gathered by the solution.		Corrigendum-III

153	SOR-C- Network –C-2 –End point protection for end user	New	Additional Clause	The proposed solution should include the capability for security admins to remotely connect to endpoint via secure shell for live forensics, data collection and remote remediation even when the endpoint is off the corporate network.	Remote shell capability will enable Railtel to remotely triage, investigate and gather forensics from endpoints not on the corporate network - such as a WFH scenario / on field scenario.		As per RFP
154	SOR-C- Network –C-2 –End point protection for end user	New	Additional Clause	The proposed solution should have the capability to perform threat hunting based on MITRE TIDs, Tactics, Techniques & Procedures and IOCs.	Hunting on TIDs / TTPs enables Railtel to hunt proactively in the environment for suspicious behaviors, while IOC hunting identifies breach artifacts. Both are essential in identifying todays modern attacks.		As per RFP
155	SOR-C- Network –C-2 –End point protection for end user	New	Additional Clause	The proposed solution should include actionable threat intelligence capabilities on the latest attack campaigns - including observed TTPs, policy recommendations, IOCs.	Actionable threat intelligence will enable Railtel team to stay ahead of emerging attacks and enrich existing security stack.		As per RFP
156	3.5	New	For AMC he will be paid @ 3.5% per annum only. If the Tenderer quotes a higher base rate for AMC, he will be paid at his quoted rate per annum and five-year differential cost shall be added to offered cost. AMC would have to be valid for minimum period of 5 years after the warranty.	1) Kindly remove this clause, as a Software OEM, we do not offer AMC for our Software licences at this rate per annum. This is not the Industry standard for AMC for Software. 2) Also please advise if the total Comprehensive Support period is 5 years (Warranty period to be taken as per Page 77, Clause 2)	In this clause it is mentioned 5 years after the warranty period.		As per RFP
157	1	19	The offered storage should be a true symmetric active-active storage	The offered storage should be a Dual active-active controller storage or higher. In case of any controller failure, the workload from failed controller should automatically failover/move to the active controller without any manual intervention.	Clarifying the functionality required from the active-active controller configuration		Clarification: Our requirement is to achieve enterprise class storage functionalities wherein host can access all the luns through all the controllers simultaneously. Asymmetric/ALUA, in case of failover might require more storage system resources and a longer response time per I/O.
158	2	19	The Storage Systems should be supplied with minimum 600TB Usable capacity using 500 capacity on SAS/NLSAS Drives on RAID6 and 100TB using SSD on RAID 6 and scalable up to 1PetaByte usable capacity using SAS/SSD.	The Storage Systems should be supplied with minimum 1100TB Usable capacity using 1000TB on SAS/NLSAS Drives on RAID6 and 100TB using SSD on RAID 5. The Storage should be scalable up to Double of usable capacity or higher.	* The rack server speciifications also asks for 480TB usable capacity to be added on the SAN Stroage. Hence the capacity needs to be changed to ~1100TB (600TB + 480TB). * Also request you to remove the 480TB Capacity requirement from the rack server specifications.		Corrigendum-III
159	4	19	The Storage should be scalable to at least 800 SFF/LFF disk drives on the same set of controllers.	The Storage should be scalable to at least 1500 SFF/LFF disk drives or higher.	The specifications asks for 1100TB of usable capacity on day one hence the storage should be power enough to support large number of disk drives to support scalability in future.		Clarification: As per RFP, However bidder may propose higher storage scalable capacity.

160	8	19	Storage should be equipped with 8*32 Gbps FC ports, 4*10Gbe port for host connectivity. Required SFPs/Optical Module to be populated from day one	Storage should be equipped with 8x32Gbps / 16 x 16 Gbps FC ports and 4 x 10Gbe SFP+ port for host connectivity. Required SFPs/Optical Module to be populated from day one The ports should support both Block (FC & iSCSI) and File (NFS & CIFS/SMB) protocols.	The RFP specification asks for a unified storage while the specifications does not mentions about NAS/File protocols. Hence request you to please add the same in this clause.		As per RFP
161	17	19	The proposed storage system should support at least 24000 LUNs or volumes	The proposed storage system should support at least 6000 LUNs/ volumes or higher	In the current project, the required usable capacity (expandable) is ~2000TB. If the average size of each volume is 20TB then the max. volumes/LUNs which can be created are 100. Even if we consider 5 times the number of volumes to be created then also the max. volumes required is 500. Hence we request you to please change the clause as requested to increase bidders participation.		Corrigendum-III
162	25.1	20	Proposed storage system should support third-party storage virtualization natively or using another headers in High availability from day1. Necessary licenses and hardware on High availability should be supplied from day1.	The solution should include data migration from old/existing storage to the new/proposed storage system without any data loss. The migration and data protection during migration responsibility lies completely with the bidder. RAILTEL will assist the migration team with support related to the existing infrastructure for the data migration purpose.	The primary purpose of this clause is to get the data migrated from the existing storage to the new storage without any data loss.		Corrigendum-III
163	8	23	12Gbps PCIe 3.0 with RAID 1, 5, 6,10, 50 with 2GB cache	Request to amend the clause as - “12Gbps PCIe 3.0 with RAID 1, 5, 6,10, 50 with 2GB cache OR 12Gbps PCIe 3.0 SAS HBA”	The vSAN certified ready servers come with 12Gbps SAS HBA for pass-through functionality as per vSAN deployment guidelines. vSAN solution deployment doesn’t require hardware RAID controller and needs only a pass-through SAS HBA as per vSAN architecture and compatibility.		Corrigendum-III
164	9	23	2 nos. of 960GB SATA M.2 in mirrored configuration for OS	Request to amend the clause as - “2 nos. of 480GB or higher SATA M.2 in mirrored configuration for OS”	960GB SATA M.2 Boot Flash disks are not available with all the leading OEMs. Moreover 480GB capacity is more than sufficient for vSphere hypervisor and OS installation.		Corrigendum-III
165	5	24	The switching OEM should be part of latest Gartner’s Leader Quadrant for Data Center networking.	The switching OEM should be part of latest Gartner’s Magic Quadrant for Data Center networking.	Most of the OEMs are in Latest Gartner report on Data Centre Networking, but may not in a leaders position, in order to have a healthy competition, we request to allow OEMs from Challengers/Visionaries quadrant as well.		Corrigendum-III
166	12	25	Switch should have a minimum 40MB buffer of more.	Switch should have a minimum 32 MB buffer of more.	Request for Change to 32 MB Buffer for us to participate		As per RFP
167	40	26	Switch should support MPLS segment routing and VRF route leaking functionality from day 1.	Switch should support VRF route leaking functionality from day 1.	MPLS is required on Wan Routers orSdwan CPE and not inside Data Centre fabric In Page 18 Tender RFP DC Network Connectivity diagram MPLS is terminated on DC router so MPLS is not required in Internal Data centre Fabric		As per RFP
168	5	35	The switching OEM should be part of latest Gartner’s Leader Quadrant for Data Center networking.	The switching OEM should be part of latest Gartner’s Magic Quadrant for Data Center networking	Most of the OEMs are in Latest Gartner report on Data Centre Networking, but may not in a leaders position, in order to have a healthy competition, we request to allow OEMs from Challengers/Visionaries quadrant as well.		Corrigendum-III
169	12	36	Switch should have a minimum 40MB buffer of more.	Switch should have a minimum 32 MB buffer of more.	Request for Change to 32 MB Buffer for us to Participate		As per RFP

170	40	37	Switch should support MPLS segment routing and VRF route leaking functionality from day 1.	Switch should support VRF route leaking functionality from day 1.	MPLS is required on Wan Routers or Sdwan CPE and not inside Data Centre fabric MPLS is terminated on DC router so MPLS is not required in Internal Data centre Fabric		As per RFP
171	4. Scope of Work-Point XII	15	Any Management switches required for the proposed solution will be provisioned by the bidder in redundant topology.	Please clarify if each rack will have dedicated Management switch (2 nos in HA) to connect to all out of band Management port of all servers and switches on Rack . This switch will then Uplink to Dual 24 port 10G Aggregation Switch on 10G multimode fiber .	Please specify the qty of Access Management switch 24 port Gigabit with 2x 10G uplink and 2 Nos 24 Port 10G Aggregation Switch . No of Access Management Switch= N (No if racks) in HA mode 2 nos required per Rack , 2 nos Aggregation Switch 24 x 10 G Please specify qty as it will be equivalent to all to Bidders . Also For full redundancy in Management network , dual Access Management Switches to be proposed per rack .		Clarification: Bidder needs to provide Minimum 2 numbers of management switch in DC and Two numbers in DR. 48 port 10/100/1000 BaseT with 4x10G uplink Switch with Redundant Power supply and stackable Switch. If in case bidder requires more ports as per the solution proposed , bidder to provision accordingly.
172	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 1	20	Backup software proposed should be in Gartner's leader quadrant of the latest Gartner Magic Quadrant report for Data Protection / Backup Software.	Backup software proposed should be in Gartner's leader quadrant of the latest Gartner Magic Quadrant report for Data Center Backup & Recovery Solution published in year 2019.	Request you to please modify considering the latest report from Gartner's.		Corrigendum-III
173	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 4	21	Backup software should be totally agentless but should support application aware backups for MS SQL, Oracle, SAP HANA, Exchange transaction logs with non-staged granular recovery of all these applications. It should support crash consistent VM level backup for all other workloads.	Backup software should be totally agentless with VM image level backup and should support application aware backups for MS SQL, Oracle, SAP HANA, Exchange transaction logs with non-staged granular recovery of all these applications. It should support crash consistent VM level backup as well.	Request you to please modify this clause being language used here is single OEM specific. Hence, we request you to please accept the changes suggested here.		Corrigendum-III
174	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 5	21	The Data protection services should be hosted on Scale out solution using software defined storage. The solution should be Multi-controller architecture to be quoted with 4 controllers/Nodes having 256GB Cache/Memory per Controller/Node.	The Data protection services should be hosted on Purpose built backup appliance (PBBA). The solution should be Multi-controller architecture to be quoted with 2 controllers having 768 GB RAM per Controller.	PBBA is widely accepted technology by world leading organizations in India as well as National Informatics Center using PBBA in multiple National Data Center's & Mini Cloud in many states in India.		Corrigendum-III
175	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 6	21	Backup solution should be provided for 500TB usable Disk based backup storage capacity (only at DC) leveraging 10TB NL-SAS drives on erasure coding or equivalent with protection of data against simultaneous 2 (Two) disk Failure with rack awareness and encryption functionality.	Backup solution should be provided for XX TB usable capacity purpose built backup appliance storage capacity (only at DC) leveraging 8TB NL-SAS drives with RAID 6 protection of data against simultaneous 2 (Two) disk Failure with one hot spare drive per disk shelf enclosure and encryption functionality.	PBBA is widely accepted technology. Hence we suggest here to include PBBA instead of commodity storage. Also request you to place front end data need to be backup here in place of XX.		Corrigendum-III
176	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 7	21	Backup solution shall be able to scale more than three times the current proposed usable capacity in a scale-out fashion.	Backup solution shall be able to scale more than Two times the current proposed usable capacity.	Scale out architecture is used in unstructured data storage and does not have any relevance to PBBA and backup solution. Hence we request you to please modify this clause to make leading backup solution OEM's to propose the backup solution.		As per RFP

177	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 8	21	The Software defined storage solution should provide multiprotocol support NFS, SMB & S3 and should have native protection from ransomware attacks or include third party antivirus scanning system using ICAP protocol any hardware required should be quoted from day 1	The proposed purpose built backup appliance should provide multiprotocol support CIFS, NFS, FC, VTL & OST and also provide methodology framework to safeguard backup data from ransomware/malware attacks.	SMB & S3 protocol is used in NAS or commodity storage. All leading backup solution OEM's provide PBBA with suggested protocols. OST & VTL protocol are standard protocols of backup solution.		Corrigendum-III
178	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 10	21	Backup software should provide best RTOs and RPOs through booting of Virtual Machines directly from the Backup to reduce the downtime.	Backup solution should provide 10 minutes RTOs and RPOs as per the last successful backup by booting of Virtual Machines directly from the Backup appliance to reduce the downtime. Purpose built backup appliance should be capable to boot minimum 30 VM's simultaneously.	Backup solution should have capability to provide enough random IOPs to support Business Continuity thru backup data. Hence, we request you to please accept the changes suggested here.		As per RFP
179	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 11	21	Backup software should have integrated data de-duplication engine with multi-vendor storage support to save space by storing de-duplicated copies of data. The deduplication engine should also facilitate IP base replication of de-dupe data. All necessary hardware and software required to support this functionality should be supplied along with other components	Backup solution should have integrated data de-duplication engine to save space by storing de-duplicated copies of data. The deduplication engine should also facilitate IP base replication of de-dupe data. All necessary hardware and software required to support this functionality should be supplied along with other components	Request you to please modify this clause being language used here is single OEM specific. Hence, we request you to please accept the changes suggested here.		Corrigendum-III
180	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 13	21	Backup software must have a feature of data validation, whereby a workload is powered-on in a sandbox environment and tested for its recoverability.	Backup solution must have inbuilt feature of data validation, where data validation is continuous process. This ensures backup data written on PBBA is can't modified and can be restored in the same state.	Request you to please modify this clause being language used here is single OEM specific. Hence, we request you to please accept the changes suggested here.		Corrigendum-III
181	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 14	21	Recovery verification should automatically boot the server from backup and verify the recoverability of VM image, Guest OS and Application Consistency.		Request you to delete this clause being the same requirement is mentioned in Point No. 13. Hence, we request you to please accept the changes suggested here.		As per RFP
182	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 15	21	The software should support varieties of backup mechanisms like Full, Incremental, and Differential etc. at different frequencies i.e. yearly, monthly, weekly, daily, hourly etc. as per defined policy. It should also have calendar-based backup scheduling. The restoration should also be supported accordingly.				As per RFP

183	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 16	21	Proposed backup Software shall support seamless integration with existing Backup solution for a wholistic view and better Management.	Proposed backup appliance shall support seamless integration with existing Backup solution for a wholistic view and better Management.	Two different backup cannot be managed by single console, however the purpose bult back appliance can integrate with multiple leading backup software OEM's. Like wise Dell Data Domain can integrate with Veeam, Networker, etc.		Clarification: Bidder is allowed to quote new Backup solution (Existing & New requirement) on a new platform to provide single Management console.
184	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 19	21	The proposed Backup software must allow to configure the maximum acceptable I/O latency level for production data stores to ensure backup and replication activities do not impact storage Availability to production workloads		Request you to delete this clause since it is forfeiting the backup perfomance and restore of backup data.		Corrigendum-III
185	New Point to be added - Functional requirement of backup solution	New		The offered Purpose-built backup appliance should be sized appropriately for backup of front-end data of XX TB (XX % File System and XX % DB) as per below mentioned backup policies: - oDaily Incremental Backup – retained for 28 Days in the backup appliance. - oWeekly Full Backup for all data types – retained for 4 Weeks in the backup appliance. - oMonthly Full Backups – Retained for 12 Months in the same backup appliance. - oYearly Full Backups - Retained for 5 years in the same backup appliance. The offered purpose-built backup appliance should be quoted with at least XX TB usable capacity post RAID 6 and hot-spare penalty using 8TB or lesser capacity drives. The proposed backup appliance must be sized for adequate capacity with 10% YoY data growth and 2% daily change rate for the contract period. Any additional software or backup storage capacity (in addition to minimum XX TB usable capacity) or any other component required as per sizing needs to be provided by the OEM & bidder during the time of bidding for entire warranty period of 5 years.			As per RFP

186	New Point to be added - Functional requirement of backup solution	New		The proposed Purpose-built backup appliance should support retention lock (WORM) feature which ensures that no user and administrator is allowed to data is deleted accidentally and support for point-in-time copies of a LUN or volumes with minimal performance impact. Even Administrator should not be able to delete the data deliberately or accidentally till the retention of the backup get expired. The offered backup appliance must have the ability of inbuilt target side data deduplication, WORM (Write Once Read Many), Replication and Encryption using AES 256 bit for data at-rest as well as in-flight while supporting VTL, CIFS, NFS and OST protocols over IP as well as FC.			As per RFP
187	New Point to be added - Functional requirement of backup solution	New		The offered backup solution must complete all backup within 8 hours backup window and the bidder must provide all the hardware and software to meet this requirement.			As per RFP
188	RAILTEL/TENDER/OT/CO /ITP/2020-21/ DC Solution /540	13	Veeam is the existing incumbent in the Backup Space. It would be recommended to have Backup Solution co-exist with incumbent solution and enhance the backup capacity. However bidder may propose any other backup solution which needs to be integrated with existing backup solution i.e. Veeam Backup Solution or propose entirely a new backup solution comprising existing and proposed solution capacity.		Two different backup software cannot be managed by single console and co-exist. Hence we request you to please remove Veeam reference from this RFP and ask the entire new backup solution and follow the standard terms of RFP.		As per RFP
189	SOR-B, B-3	5	Software defined Storage, Virtualization Virtual Cloud Foundation& Site Recovery License as per Technical Specification given in chapter-3A	Based on the requirement kindly amend this line for clarity as: "Software defined Storage, Cloud Management Platform, SDN & Site Recovery License as per Technical Specification given in chapter-3A"	Amendment required for more clarity and to avoid any ambiguity		As per RFP
190	SOR-B- Cloud Solution –B-3- Software defined Storage, Virtualization Virtual Cloud Foundation & Site Recovery License:	29	SOR-B- Cloud Solution –B-3- Software defined Storage, Virtualization Virtual Cloud Foundation & Site Recovery License:	Based on the requirement kindly amend this line for clarity as: "Software defined Storage, Cloud Management Platform, SDN & Site Recovery License as per Technical Specification given in chapter-3A"	Amendment required for more clarity and to avoid any ambiguity		As per RFP

191	4. Scope of Work-xiii	15	xiii. Bidder needs to integrate the cloud platform with existing LDAP solution in RailTel. xvi. Offered cloud solution version should be latest and bidder needs to perform the migration/upgradation activity of the existing cloud solution to maintain uniformity of entire cloud solution.	Kindly add following clause "VMware cloud management paltform is already setup in existing private cloud at RailTel. For VMware solution, scope will be to 1. Prepare new servers being procured as part of this tender and add them as part of existing cloud setup for expansion . 2. Migrate existing NSX-V to NSX-T 3. Integration of cloud portal with Multi factor authentication solution being procured in this tender	We understand that for VMware solution all this activities are not be applicable as VMware cloud management paltform is already setup and as part of scope new servers being procured as part of this tender neds to be prepared and added in existing cloud setup for expansion.		Clarification: Complete scope of work has been defined considering both scenarios that bidder may propose Vmware CMP or may propose entirely new CMP platform . If bidder is proposing Vmware CMP than high level SOW to be read as but not limited to " VMware cloud management paltform is already setup in existing private cloud at RailTel. For VMware solution, scope will be to 1. Prepare new servers being procured as part of this tender and add them as part of existing cloud setup for expansion . 2. Migrate existing NSX-V to NSX-T 3. Integration of cloud portal with Multi factor authentication solution being procured in this tender 4. Implement SSO for cloud management software components for 15 to 20 administrators. 5. Replicate cloud management components to DR site " If Bidder propose new CMP platform , then bidder has to perform all the activities as defined in tender."
192	7-iv	17	iv. Integrate Virtualization Manager with Cloud Management Platform (CMP), Software Defined Network (SDN) & Software Defined Storage (SDS). vi. Create Virtual machines for Linux OS or Windows, Virtual machine templates, Virtual machine configured in High Availability mode in cluster, affinity group creation of virtual machines and virtual machine backup configuration (Snapshot and Clone). vii. Configure storage policies to automate provisioning and balancing of storage resources to ensure that each VM gets the specified storage resources and services. viii. Bidder shall perform integration of HCI with the supplied backup solution and should enable integration with VM to perform backup of VM data and configuration files.	4. Implement SSO for cloud management software components for 15 to 20 administrators 5. Replicate cloud management components to DR site "			

193	8	17	"i. Bidder should integrate the CMP fully with the supplied HCI solution i.e., integration with manager of the hypervisor, Software Defined Network, Software Defined Storage, etc." "ii. The bidder should create policy-based controls of cloud resources and should configure Rolebased policy management, administration and enforce role- based policies." "iii. The bidder should create workflow and blueprints for IaaS, PaaS as defined in Functional Requirements" "iv. The bidder shall also create basic & necessary reports for the analysis of resources (CPU, Memory, Storage and Network) utilization and available resources." v. Bidder should configure auto-scaling of resource as per demand "vi. The bidder should configure CMP with, backup software to enable configuration of backup and restore through self- service Dashboard."				
194	SOR-B	29	The solution should have capability to automate the bring-up process of the entire software platform, including deployment of infrastructure VMs, creation of the management cluster, configuration of VLANs, virtual storage, virtual network, and cluster creation and provisioning.	We understand that VMware cloud management platform with management cluster is already setup in existing RailTel private cloud. So this clause is not applicable. Kindly confirm.	VMware cloud management platform along with management cluster is already setup in existing RailTel private cloud. So bring-up of software platform, management cluster, infrastructure VMs is not required		Clarification: Specification given considering the scenario that bidder may propose the extension of VMware CMP or may propose the entire new CMP.
195	SOR-B	32	The solution should provide true multi tenancy, Each tenant needs to be able to create their own profiles/blueprints, share them to a public catalog, and not be able to see other tenant's build profiles, compute resources, or managed machines. At least 3 tenants will be required to be configured during the Cloud deployment.	Kindly amend this as "The solution should provide true multi tenancy, Each tenant needs to be able to create their own profiles/blueprints, share them to a public catalog, and not be able to see other tenant's build profiles, compute resources, or managed machines. At least 3 Business Groups will be required to be configured during the Cloud deployment."	As per our understanding in present setup different departments are onboarded with business groups. More business groups can be created as per requirement of this clause.		As per RFP
196	SOR-B	31	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.	Request to kindly remove this clause	This feature is not part of the components asked at section 4 page 15 point xvi. Also kindly note this feature is not a part of currently running stack in RailTel eoffice project.		As per RFP

197	SOR –D Licenses for OS, DB and NMS/EMS	41	EDB PostGre SQL support system for DB servers - 860 Nos.	Kindly make it open and amend as "EDB/ VMware PostGre SQL support system for DB servers - 860 cores"	Amendment required to make it open and for wider participation		Corrigendum-III
198	SOR –D Licenses for OS, DB and NMS/EMS	41	EDB PostGre SQL support system for DB servers - 860 Nos.	Kindly mention the segregation for cores for active, passive, DR, reporting instances	Clarification required		Corrigendum-III
199	4. Scope of Work-xvi.	15	VMware Site Recovery Manager Standard Latest edition (25 VM Pack) or equivalent -6 Nos.	Kindly amend as "VMware Site Recovery Manager Enterprise Latest edition (25 VM Pack) -6 Nos."	Existing setup has Site Recovery Manager Enterprise edition		Corrigendum-III
200	4. Scope of Work-xvi.	15	VMware vSAN 6 or latest Enterprise for 1 Processor or equivalent - 105 Nos.	Kindly amend as "VMware vSAN Advanced 6 or latest for 1 Processor or equivalent - 105 Nos."	Existing setup is with vSAN Advanced.		Corrigendum-III
201	SOR-B	32	The solution should provide automatic private cloud metering and consumption analysis. The Cloud portal will be configured with Multi factor authentication during the deployment.	VMware Cloud portal already setup for RailTel e-Office will be configured with Multi factor authentication solution being procured as part of this tender. Supported authentication types are listed on this link. Would request that the asked MFA solution should be compatible as per this list. https://docs.vmware.com/en/vRealize-Automation/7.6/com.vmware.vra.prepare.use.doc/GUID-D16CB962-78B9-4FAD-92D5-E16613A381FF.html?hWord=N4lghgNiBcIC4HcD2ACAZmAxnJAnFYArnABYcmAdnAJaZg1IUgC+QA			Clarification: The solution should support following protocols for integration including Radius, SAML, RestAPI, OIDC, Web SDK etc or equivalent for providing MFA services.
202	SOR-B	33	There should be single portal to manage all the Cloud based management software using single sign on functionality.	We understand that this functionality is required for RailTel administrators and there would be 15 to 20 such users. Kindly confirm if we can propose the solution for 20 users.			Corrigendum-III
203	12.1.1	64	12.1.1 The Equipment offered by the OEM or equipment of the same series/family from the same OEM should have been satisfactorily working in Government/PSUs/Telecom Service Providers network for at least 12 months as on date of opening of tender, in India or Abroad. The certificates from the actual users will have to be submitted along with bid.	Kindly amend "12.1.1 The Equipment offered by the OEM or equipment of the same series/family from the same OEM should have been satisfactorily working in Government/PSUs/Telecom Service Providers network for at least 12 months as on date of opening of tender, in India or Abroad. The certificates from the actual users or publically available references/ case studies will have to be submitted along with bid."	Kindly amend to accept the publically available customer references/ case studies		As per RFP

204	12.1.2	64	12.1.2 The OEM should have supplied at least 35% of the tendered value/SOR Value of the equipment offered or equipment of the same series/family during last preceding 3 financial years (i.e. current year and three previous financial years) as on opening of bid to Government/PSUs/Telecom Service Providers. OEM should submit self-certificate with proper contact detail of clients along with PO reference and amount supplied (Firm Name, Contact person, Designation, Telephone Number, Fax, Official mail id etc.). The same should be issued by authorized signatory.	We understand that Global Government/PSUs/Telecom Service Providers references will be acceptable. Kindly confirm			As per RFP
205	SOR-C- Network –C-2 –End point protection for end user	41	27. The endpoint solution shall be able to pinpoint vulnerable versions of popular applications installed in Endpoints	The endpoint solution shall be able to protect vulnerable versions of popular applications installed in Endpoints with multi-layered prevention.	Protection is key for all applications and processes. By identifying attacker behaviour with Tactics, Techniques and Procedures organizations can stay ahead of vulnerabilities by having multi-layered prevention of these behaviours.		Corrigendum-III
206	SOR-C- Network –C-2 –End point protection for end user	41	22. The proposed solution shall have the capability to quarantine the malicious application/program/file automatically without quarantining the entire user machine from network which would affect business productivity of the user	The proposed solution shall have the capability to quarantine the malicious application/program/file automatically without quarantining the entire user machine from network which would affect business productivity of the user. The solution should also include the capability to isolate the host if required to protect from lateral movement.	Host Isolation provides an additional layer of security control where is a user or endpoint is remote, it enables the security team to quickly isolate the endpoint on incident detection (for critical incidents) until they inspect for forensics and next steps.		As per RFP
207	SOR-C- Network –C-2 –End point protection for end user	41	23. The proposed solution shall have the capability to work with Indicators of Compromise (IOC's)	The proposed solution shall have the capability to work with Indicators of Compromise (IOC's) and correlate MITRE ATT&CK Tactics Techniques & Procedures (TTPs)	IOC's are post-breach or reactive in nature. Tactics, Techniques and Procedures enable organizations to hunt proactively for attacker behavior and are now a widely adopted standard across all endpoint security solutions. Reference: attack.mitre.org		As per RFP
208	SOR-C- Network –C-2 –End point protection for end user	41	28. The proposed solution shall be able to identify the threat root cause of incidents, child processes of malwares and parent file disposition	The proposed solution shall be able to identify the threat root cause of incidents, child processes of malwares and parent file disposition, network connections, registry modifications, scripts executed and targets injected.	Metadata such as network connections, registry modifications, injections and script executions are crucial to uncovering all stages of the attack and artifacts from a single console.		As per RFP
209	SOR-C- Network –C-2 –End point protection for end user	41	32. Solution should allow Users to choose to preview the new Policy UI.	The solution should allow administrators to identify policy effects based on historical data before apply the Prevention policy.	It should enable administrators to intelligently push policies that work with minimal disruption to the end user by identifying possible conflicts or business application effects of enabling a specific feature Using the historical data that is gathered by the solution.		Corrigendum-III

210	SOR-C- Network –C-2 –End point protection for end user	New	Additional Clause	The proposed solution should include the capability for security admins to remotely connect to endpoint via secure shell for live forensics, data collection and remote remediation even when the endpoint is off the corporate network.	Remote shell capability will enable Railtel to remotely triage, investigate and gather forensics from endpoints not on the corporate network - such as a WFH scenario / on field scenario.		As per RFP
211	SOR-C- Network –C-2 –End point protection for end user	New	Additional Clause	The proposed solution should have the capability to perform threat hunting based on MITRE TIDs, Tactics, Techniques & Procedures and IOCs.	Hunting on TIDs / TTPs enables Railtel to hunt proactively in the environment for suspicious behaviors, while IOC hunting identifies breach artifacts. Both are essential in identifying todays modern attacks.		As per RFP
212	SOR-C- Network –C-2 –End point protection for end user	New	Additional Clause	The proposed solution should include actionable threat intelligence capabilities on the latest attack campaigns - including observed TTPs, policy recommendations, IOCs.	Actionable threat intelligence will enable Railtel team to stay ahead of emerging attacks and enrich existing security stack.		As per RFP
213	3.5	60	For AMC he will be paid @ 3.5% per annum only. If the Tenderer quotes a higher base rate for AMC, he will be paid at his quoted rate per annum and five-year differential cost shall be added to offered cost. AMC would have to be valid for minimum period of 5 years after the warranty.	1) Kindly remove this clause, as a Software OEM, we do not offer AMC for our Software licences at this rate per annum. This is not the Industry standard for AMC for Software. 2) Also please advise if the total Comprehensive Support period is 5 years (Warranty period to be taken as per Page 77, Clause 2)	In this clause it is mentioned 5 years after the warranty period.		As per RFP
214	5	6	The tenderer will be fully responsible Supply of Equipment/cards/interfaces and all related items for installation and commissioning of the network including the following: a) Integration with existing Network as required. b) Spares required for Commissioning, maintenance supervision & warranty period shall be maintained by the Contractor at his own cost. c) All necessary cables and connectors and other accessories required for installation.	Please share the list of components which needs to be spare and also share the list of necessary cables and connectors with it's types.			As per RFP
215	Scope of Work/V	14	Bidder has to ensure smooth migration from existing SAN switch to proposed SAN switch.	Please share the existing SAN switches details of make and model along with how many servers are configured into it.			Refer- Existing Inventory Sheet enclosed in "Annexure-A"
216	Scope of Work/XIII	15	Bidder needs to integrate the cloud platform with existing LDAP solution in RailTel.	Please share the detailed information of LDAP and share the version also.			Clarification: Open LDAP and Active Directory is used.

217	Scope of Work/XVI	15	In case bidder is offering VMware cloud solution, qty required for different lic. are mentioned below- VMware vCloud Suite Latest edition or equivalent -114 Nos. VMware NSX Data Center (NSX-T) Advanced per Processor or equivalent-114 Nos. VMware vSAN 6 or latest Enterprise for 1 Processor or equivalent - 105 Nos. VMware Site Recovery Manager Standard Latest edition (25 VM Pack) or equivalent -6 Nos	Please share the sizing of all required licenses of vmware for 60 servers and also share the deployment strategy of 60 servers for both the sites (will it be 30 each site)			As per RFP
218	Bidder shall perform following work for equipment installation implementation & integration with existing Infras/I	17	Bidder shall provision the necessary Structured LAN cabling components for physical network connectivity of the new infrastructure as well as integration of HCI based RailTel Cloud with existing RAILTEL gateway. The bidder shall prepare a detailed plan to perform these activities.Planned downtime of appropriate duration shall be allocated for these activities during off peak hours.	Please share the complete detail of required structured cabling for required solution.			As per RFP
219	SOR –D Licenses for OS, DB and NMS/EMS/II	41	Bidder will ensure that all costs with respect to upgrades/updates etc of all perpetual license software being procured in this tender are borne by the bidder.	Please clarify software assurance will be required for microsoft licenses			Corrigendum-III
220	Generic Query	New	Existing SDN	Please share the complete details of SDN setup in existing environment			Refer- Existing Inventory Sheet enclosed in "Annexure-A"
221	Generic Query	New	Migration Services	Please share the detailed information of any migration services will be required by bidder			As per RFP
No Data		New					N/A

222	SOR-C-Network-C2	40	End point protection for End User	As per the scope of the RFP, Railtel has planned for the purchase of End Point Protection which is the good approach towards security. It will help Railtel to block the attacks but the big question is why that attack is happening is because of some addressed Vulnerability in the asset or end point. Vulnerability can be in the form of missing patches, unused services or compliance issue. If the Vulnerability is addressed then the overall attack surface is reduced which will further result in the reduction of attacks. Most breaches were due to bad cyber hygiene where attackers are leveraging on unpatched vulnerabilities. As per Gartner, Zero days attack are only 0.04% of the overall attacks, most of the attacks are leveraging the common vulnerabilities only.	So Therefore, we recommend to include Vulnerability Management(VM) solution as part of this RFP which will complement EDR with the following benefits:- 1) VM complements EPP/EDR EPP/. EDR focus on protection, detection and response to know and unknow threats (exploits/malwares). However we should always shift left to identify/remediate vulnerability proactively than to reactively block every single exploits and malwares targeting on that vulnerability. 2)Client-side application vulnerabilities represent another set of CVEs actively being targeted by threat actors in the wild in a variety of attacks ranging from drive-by-exploitation, exploit-kit, phishing, ransomware and cryptojacking. i.e. Web Browsers, Java, Adobe PDF and flash player, MS office, SSL VPN, Slack, Zoom. 3) Focus on System Hygiene and not Zero-Days		As per RFP
223	SOR-B, B-3	5	Software defined Storage, Virtualization Virtual Cloud Foundation& Site Recovery License as per Technical Specification given in chapter-3A	Based on the requirement kindly amend this line for clarity as: "Software defined Storage, Cloud Management Platform, SDN & Site Recovery License as per Technical Specification given in chapter-3A"	Amendment required for more clarity and to avoid any ambiguity		As per RFP
224	4. Scope of Work-xvi.	15	VMware Site Recovery Manager Standard Latest edition (25 VM Pack) or equivalent -6 Nos.	Kindly amend as "VMware Site Recovery Manager Enterprise Latest edition (25 VM Pack) -6 Nos."	Existing setup has Site Recovery Manager Enterprise edition		Corrigendum-III
225	4. Scope of Work-xvi.	15	VMware vSAN 6 or latest Enterprise for 1 Processor or equivalent - 105 Nos.	Kindly amend as "VMware vSAN Advanced 6 or latest for 1 Processor or equivalent - 105 Nos."	Existing setup is with vSAN Advanced.		Corrigendum-III

226	4. Scope of Work-xiii	15	xiii. Bidder needs to integrate the cloud platform with existing LDAP solution in RailTel. xvi. Offered cloud solution version should be latest and bidder needs to perform the migration/upgradation activity of the existing cloud solution to maintain uniformity of entire cloud solution.	Kindly add following clause "VMware cloud management paltform is already setup in existing private cloud at RailTel. For VMware solution, scope will be to 1. Prepare new servers being procured as part of this tender and add them as part of existing cloud setup for expansion . 2. Migrate existing NSX-V to NSX-T 3. Integration of cloud portal with Multi factor authentication solution being procured in this tender 4. Implement SSO for cloud management software components for 15 to 20 administrators 5. Replicate cloud management components to DR site "	We understand that for VMware solution all this activities are not be applicable as VMware cloud management paltform is already setup and as part of scope new servers being procured as part of this tender needs to be prepared and added in existing cloud setup for expansion.		Clarification: Complete scope of work has been defined considering both scenarios that bidder may propose VMware CMP or may propose entirely new CMP platform . If bidder is proposing VMware CMP than high level SOW to be read as but not limited to " VMware cloud management paltform is already setup in existing private cloud at RailTel. For VMware solution, scope will be to 1. Prepare new servers being procured as part of this tender and add them as part of existing cloud setup for expansion . 2. Migrate existing NSX-V to NSX-T 3. Integration of cloud portal with Multi factor authentication solution being procured in this tender 4. Implement SSO for cloud management software components for 15 to 20 administrators. 5. Replicate cloud management components to DR site ". If Bidder propose new CMP platform , then bidder has to perform all the activities as defined in tender."
227	1	19	The offered storage should be a true symmetric active-active storage	The offered storage should be a Dual active-active controller storage or higher. In case of any controller failure, the workload from failed controller should automatically failover/move to the active controller without any manual intervention.	Clarifying the functionality required from the active-active controller configuration		Clarification: Our requirement is to achieve enterprise class storage functionalities wherein host can access all the luns through all the controllers simultaneously. Asymmetric/ALUA, in case of failover might require more storage system resources and a longer response time per I/O.
228	2	19	The Storage Systems should be supplied with minimum 600TB Usable capacity using 500 capacity on SAS/NLSAS Drives on RAID6 and 100TB using SSD on RAID 6 and scalable up to 1PetaByte usable capacity using SAS/SSD.	The Storage Systems should be supplied with minimum 1100TB Usable capacity using 1000TB on SAS/NLSAS Drives on RAID6 and 100TB using SSD on RAID 5. The Storage should be scalable up to Double of usable capacity or higher.	* The rack server specifiactions also asks for 480TB usable capacity to be added on the SAN Stroage. Hence the capacity needs to be changed to ~1100TB (600TB + 480TB). * Also request you to remove the 480TB Capacity requirement from the rack server specifications.		Corrigendum-III
229	4	19	The Storage should be scalable to at least 800 SFF/LFF disk drives on the same set of controllers.	The Storage should be scalable to at least 1500 SFF/LFF disk drives or higher.	The specifications asks for 1100TB of usable capacity on day one hence the storage should be power enough to support large number of disk drives to support scalability in future.		Clarification: As per RFP, However bidder may propose higher storage scalable capacity.

230	8	19	Storage should be equipped with 8*32 Gbps FC ports, 4*10Gbe port for host connectivity. Required SFPs/Optical Module to be populated from day one	Storage should be equipped with 8x32Gbps / 16 x 16 Gbps FC ports and 4 x 10Gbe SFP+ port for host connectivity. Required SFPs/Optical Module to be populated from day one The ports should support both Block (FC & iSCSI) and File (NFS & CIFS/SMB) protocols.	The RFP specification asks for a unified storage while the specifications does not mentions about NAS/File protocols. Hence request you to please add the same in this clause.		As per RFP
231	17	19	The proposed storage system should support at least 24000 LUNs or volumes	The proposed storage system should support at least 6000 LUNs/ volumes or higher	In the current project, the required usable capacity (expandable) is ~2000TB. If the average size of each volume is 20TB then the max. volumes/LUNs which can be created are 100. Even if we consider 5 times the number of volumes to be created then also the max. volumes required is 500. Hence we request you to please change the clause as requested to increase bidders participation.		Corrigendum-III
232	25.I	20	Proposed storage system should support third-party storage virtualization natively or using another headers in High availability from day1. Necessary licenses and hardware on High availability should be supplied from day1.	The solution should include data migration from old/existing storage to the new/proposed storage system without any data loss. The migration and data protection during migration responsibility lies completely with the bidder. RAILTEL will assist the migration team with support related to the existing infrastructure for the data migration purpose.	The primary purpose of this clause is to get the data migrated from the existing storage to the new storage without any data loss.		Corrigendum-III
233	4. Scope of Work-Point XII	15	Any Management switches required for the proposed solution will be provisioned by the bidder in redundant topology.	Please clarify if each rack will have dedicated Manangement switch (2 nos in HA)to connect to all out of band Manangement port of all servers and switches on Rack . This switch will then Uplink to Dual 24 port 10G Aggregation Switch on 10G multimode fiber .	Please specify the qty of Access Manangement switch 24 port Gigabit with 2x 10G uplink and 2 Nos 24 Port 10G Aggregation Switch . No of Access Manangement Switch= N (No if racks) in HA mode 2 nos required per Rack , 2 nos Aggegation Switch 24 x 10 G Please specify qty as it will be equivalent to all to Bidders . Also For fyull redundancy in Manangement network , dual Access Managemnet Switches to be proposed per rack .		Clarification: Bidder needs to provide Minimum 2 numbers of management switch in DC and Two numbers in DR. 48 port 10/100/1000 BaseT with 4x10G uplink Switch with Redundant Power supply and stackable Switch. If in case bidder requires more ports as per the solution proposed , bidder to provision accorddingly.
234	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 1	20	Backup software proposed should be in Gartner's leader quadrant of the latest gartner Magic Quadrant report for Data Protection / Backup Software.	Backup software proposed should be in Gartner's leader quadrant of the latest gartner Magic Quadrant report for Data Center Backup & Recovery Solution published in year 2019.	Request you to please modify considering the latest report from Gartners.		Corrigendum-III
235	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 4	21	Backup software should be totally agentless but should support application aware backups for MS SQL, Oracle, SAP HANA, Exchange transaction logs with non-staged granular recovery of all these applications. It should support crash consistent VM level backup for all other workloads.	Backup software should be totally agentless with VM image level backup and should support application aware backups for MS SQL, Oracle, SAP HANA, Exchange transaction logs with non-staged granular recovery of all these applications. It should support crash consistent VM level backup as well.	Request you to please modify this clause being language used here is single OEM specific. Hence, we request you to please accept the changes suggested here.		Corrigendum-III

236	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 5	21	The Data protection services should be hosted on Scale out solution using software defined storage. The solution should be Multi-controller architecture to be quoted with 4 controllers/Nodes having 256GB Cache/Memory per Controller/Node.	The Data protection services should be hosted on Purpose built backup appliance (PBBA). The solution should be Multi-controller architecture to be quoted with 2 controllers having 768 GB RAM per Controller.	PBBA is widely accepted technology by world leading organizations in India as well as National Informatics Center using PBBA in multiple National Data Center's & Mini Cloud in many states in India.		Corrigendum-III
237	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 6	21	Backup solution should be provided for 500TB usable Disk based backup storage capacity (only at DC) leveraging 10TB NL-SAS drives on erasure coding or equivalent with protection of data against simultaneous 2 (Two) disk Failure with rack awareness and encryption functionality.	Backup solution should be provided for XX TB usable capacity purpose built backup appliance storage capacity (only at DC) leveraging 8TB NL-SAS drives with RAID 6 protection of data against simultaneous 2 (Two) disk Failure with one hot spare drive per disk shelf enclosure and encryption functionality.	PBBA is widely accepted technology. Hence we suggest here to include PBBA instead of commodity storage. Also request you to place front end data need to be backup here in place of XX.		Corrigendum-III
238	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 7	21	Backup solution shall be able to scale more than three times the current proposed usable capacity in a scale-out fashion.	Backup solution shall be able to scale more than Two times the current proposed usable capacity.	Scale out architecture is used in unstructured data storage and does not have any relevance to PBBA and backup solution. Hence we request you to please modify this clause to make leading backup solution OEM's to propose the backup solution.		As per RFP
239	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 8	21	The Software defined storage solution should provide multiprotocol support NFS, SMB & S3 and should have native protection from ransomware attacks or include third party antivirus scanning system using ICAP protocol any hardware required should be quoted from day 1	The proposed purpose built backup appliance should provide multiprotocol support CIFS, NFS, FC, VTL & OST and also provide methodology framework to safeguard backup data from ransomware/malware attacks.	SMB & S3 protocol is used in NAS or commodity storage. All leading backup solution OEM's provide PBBA with suggested protocols. OST & VTL protocol are standard protocols of backup solution.		Corrigendum-III
240	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 10	21	Backup software should provide best RTOs and RPOs through booting of Virtual Machines directly from the Backup to reduce the downtime.	Backup solution should provide 10 minutes RTOs and RPOs as per the last successful backup by booting of Virtual Machines directly from the Backup appliance to reduce the downtime. Purpose built backup appliance should be capable to boot minimum 30 VM's simultaneously.	Backup solution should have capability to provide enough random IOPs to support Business Continuity thru backup data. Hence, we request you to please accept the changes suggested here.		As per RFP
241	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 11	21	Backup software should have integrated data de-duplication engine with multi-vendor storage support to save space by storing de-duplicated copies of data. The deduplication engine should also facilitate IP base replication of de-dupe data. All necessary hardware and software required to support this functionality should be supplied along with other components	Backup solution should have integrated data de-duplication engine to save space by storing de-duplicated copies of data. The deduplication engine should also facilitate IP base replication of de-dupe data. All necessary hardware and software required to support this functionality should be supplied along with other components	Request you to please modify this clause being language used here is single OEM specific. Hence, we request you to please accept the changes suggested here.		Corrigendum-III
242	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 13	21	Backup software must have a feature of data validation, whereby a workload is powered-on in a sandbox environment and tested for its recoverability.	Backup solution must have inbuilt feature of data validation, where data validation is continuous process. This ensures backup data written on PBBA is can't modified and can be restored in the same state.	Request you to please modify this clause being language used here is single OEM specific. Hence, we request you to please accept the changes suggested here.		Corrigendum-III

243	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 14	21	Recovery verification should automatically boot the server from backup and verify the recoverability of VM image, Guest OS and Application Consistency.		Request you to delete this clause being the same requirement is mentioned in Point No. 13. Hence, we request you to please accept the changes suggested here.		As per RFP
244	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 15	21	The software should support varieties of backup mechanisms like Full, Incremental, and Differential etc. at different frequencies i.e. yearly, monthly, weekly, daily, hourly etc. as per defined policy. It should also have calendar-based backup scheduling. The restoration should also be supported accordingly.				As per RFP
245	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 16	21	Proposed backup Software shall support seamless integration with existing Backup solution for a wholistic view and better Management.	Proposed backup appliance shall support seamless integration with existing Backup solution for a wholistic view and better Management.	Two different backup cannot be managed by single console, however the purpose bult back appliance can integrate with multiple leading backup software OEM's. Like wise Dell Data Domain can integrate with Veeam, Networker, etc.		Clarification: Bidder is allowed to quote new Backup solution (Existing & New requirement) on a new platform to provide single Management console.
246	Page No. 20 - SOR-A-Storage – A-2 – Backup solution at DC & DR: Point No. 19	21	The proposed Backup software must allow to configure the maximum acceptable I/O latency level for production data stores to ensure backup and replication activities do not impact storage Availability to production workloads		Request you to delete this clause since it is forfeiting the backup performance and restore of backup data.		Corrigendum-III
247	8	23	12Gbps PCIe 3.0 with RAID 1, 5, 6,10, 50 with 2GB cache	Request to amend the clause as - “12Gbps PCIe 3.0 with RAID 1, 5, 6,10, 50 with 2GB cache OR 12Gbps PCIe 3.0 SAS HBA”	The vSAN certified ready servers come with 12Gbps SAS HBA for pass-through functionality as per vSAN deployment guidelines. vSAN solution deployment doesn't require hardware RAID controller and needs only a pass-through SAS HBA as per vSAN architecture and compatibility.		Corrigendum-III
248	9	23	2 nos. of 960GB SATA M.2 in mirrored configuration for OS	Request to amend the clause as - “2 nos. of 480GB or higher SATA M.2 in mirrored configuration for OS”	960GB SATA M.2 Boot Flash disks are not available with all the leading OEMs. Moreover 480GB capacity is more than sufficient for vSphere hypervisor and OS installation.		Corrigendum-III
249	5	24	The switching OEM should be part of latest Gartner's Leader Quadrant for Data Center networking.	The switching OEM should be part of latest Gartner's Magic Quadrant for Data Center networking.	Most of the OEMs are in Latest Gartner report on Data Centre Networking, but may not in a leaders position, in order to have a healthy competition, we request to allow OEMs from Challengers/Visionaries quadrant as well.		Corrigendum-III
250	12	25	Switch should have a minimum 40MB buffer of more.	Switch should have a minimum 32 MB buffer of more.	Request for Change to 32 MB Buffer for us to participate		As per RFP
251	40	26	Switch should support MPLS segment routing and VRF route leaking functionality from day 1.	Switch should support VRF route leaking functionality from day 1.	MPLS is required on Wan Routers orSdwan CPE and not inside Data Centre fabric In Page 18 Tender RFP DC Network Connectivity diagram MPLS is terminated on DC router so MPLS is not required in Internal Data centre Fabric		As per RFP

252	SOR-B	29	The solution should have capability to automate the bring-up process of the entire software platform, including deployment of infrastructure VMs, creation of the management cluster, configuration of VLANs, virtual storage, virtual network, and cluster creation and provisioning.	We understand that VMware cloud management platform with management cluster is already setup in existing RailTel private cloud. So this clause is not applicable. Kindly confirm.	VMware cloud management platform along with management cluster is already setup in existing RailTel private cloud. So bring-up of software platform, management cluster, infrastructure VMs is not required		Clarification: Specification given considering the scenario that bidder may propose the extension of VMware CMP or may propose the entire new CMP.
253	SOR-B	29	The solution should provide true multi tenancy, Each tenant needs to be able to create their own profiles/blueprints, share them to a public catalog, and not be able to see other tenant's build profiles, compute resources, or managed machines. At least 3 tenants will be required to be configured during the Cloud deployment.	Kindly amend this as "The solution should provide true multi tenancy, Each tenant needs to be able to create their own profiles/blueprints, share them to a public catalog, and not be able to see other tenant's build profiles, compute resources, or managed machines. At least 3 Business Groups will be required to be configured during the Cloud deployment."	As per our understanding in present setup different departments are onboarded with business groups. More business groups can be created as per requirement of this clause.		As per RFP
254	SOR-B	31	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.	Request to kindly remove this clause	This feature is not part of the components asked at section 4 page 15 point xvi. Also kindly note this feature is not a part of currently running stack in RailTel eoffice project.		As per RFP
255	5	35	The switching OEM should be part of latest Gartner's Leader Quadrant for Data Center networking.	The switching OEM should be part of latest Gartner's Magic Quadrant for Data Center networking	Most of the OEMs are in Latest Gartner report on Data Centre Networking, but may not in a leaders position, in order to have a healthy competition, we request to allow OEMs from Challengers/Visionaries quadrant as well.		Corrigendum-III
256	12	36	Switch should have a minimum 40MB buffer of more.	Switch should have a minimum 32 MB buffer of more.	Request for Change to 32 MB Buffer for us to Participate		As per RFP
257	40	37	Switch should support MPLS segment routing and VRF route leaking functionality from day 1.	Switch should support VRF route leaking functionality from day 1.	MPLS is required on Wan Routers or SD-WAN CPE and not inside Data Centre fabric MPLS is terminated on DC router so MPLS is not required in Internal Data centre Fabric		As per RFP
258	SOR –D Licenses for OS, DB and NMS/EMS	41	EDB PostGre SQL support system for DB servers - 860 Nos.	Kindly make it open and amend as "EDB/ VMware PostGre SQL support system for DB servers - 860 cores"	Amendment required to make it open and for wider participation		Corrigendum-III
259	SOR –D Licenses for OS, DB and NMS/EMS	41	EDB PostGre SQL support system for DB servers - 860 Nos.	Kindly mention the segregation for cores for active, passive, DR, reporting instances	Clarification required		Corrigendum-III

260	12.1.1	64	12.1.1 The Equipment offered by the OEM or equipment of the same series/family from the same OEM should have been satisfactorily working in Government/PSUs/Telecom Service Providers network for at least 12 months as on date of opening of tender, in India or Abroad. The certificates from the actual users will have to be submitted along with bid.	Kindly amend "12.1.1 The Equipment offered by the OEM or equipment of the same series/family from the same OEM should have been satisfactorily working in Government/PSUs/Telecom Service Providers network for at least 12 months as on date of opening of tender, in India or Abroad. The certificates from the actual users or publically available references/ case studies will have to be submitted along with bid."	Kindly amend to accept the publically available customer references/ case studies		As per RFP
261	12.1.2	64	12.1.2 The OEM should have supplied at least 35% of the tendered value/SOR Value of the equipment offered or equipment of the same series/family during last preceding 3 financial years (i.e. current year and three previous financial years) as on opening of bid to Government/PSUs/Telecom Service Providers. OEM should submit self-certificate with proper contact detail of clients along with PO reference and amount supplied (Firm Name, Contact person, Designation, Telephone Number, Fax, Official mail id etc.). The same should be issued by authorized signatory.	We understand that Global Government/PSUs/Telecom Service Providers references will be acceptable. Kindly confirm			As per RFP
262	SOR-C- Network –C-2 –End point protection for end user	41	27. The endpoint solution shall be able to pinpoint vulnerable versions of popular applications installed in Endpoints	The endpoint solution shall be able to protect vulnerable versions of popular applications installed in Endpoints with multi-layered prevention.	Protection is key for all applications and processes. By identifying attacker behaviour with Tactics, Techniques and Procedures organizations can stay ahead of vulnerabilities by having multi-layered prevention of these behaviours.		Corrigendum-III
263	SOR-C- Network –C-2 –End point protection for end user	41	22. The proposed solution shall have the capability to quarantine the malicious application/program/file automatically without quarantining the entire user machine from network which would affect business productivity of the user	The proposed solution shall have the capability to quarantine the malicious application/program/file automatically without quarantining the entire user machine from network which would affect business productivity of the user. The solution should also include the capability to isolate the host if required to protect from lateral movement.	Host Isolation provides an additional layer of security control where is a user or endpoint is remote, it enables the security team to quickly isolate the endpoint on incident detection (for critical incidents) until they inspect for forensics and next steps.		As per RFP
264	SOR-C- Network –C-2 –End point protection for end user	41	23. The proposed solution shall have the capability to work with Indicators of Compromise (IOC's)	The proposed solution shall have the capability to work with Indicators of Compromise (IOC's) and correlate MITRE ATT&CK Tactics Techniques & Procedures (TTPs)	IOC's are post-breach or reactive in nature. Tactics, Techniques and Procedures enable organizations to hunt proactively for attacker behavior and are now a widely adopted standard across all endpoint security solutions. Reference: attack.mitre.org		As per RFP

265	SOR-C- Network –C-2 –End point protection for end user	41	28. The proposed solution shall be able to identify the threat root cause of incidents, child processes of malwares and parent file disposition	The proposed solution shall be able to identify the threat root cause of incidents, child processes of malwares and parent file disposition, network connections, registry modifications, scripts executed and targets injected.	Metadata such as network connections, registry modifications, injections and script executions are crucial to uncovering all stages of the attack and artifacts from a single console.		As per RFP
266	SOR-C- Network –C-2 –End point protection for end user	41	32. Solution should allow Users to choose to preview the new Policy UI.	The solution should allow administrators to identify policy effects based on historical data before apply the Prevention policy.	It should enable administrators to intelligently push policies that work with minimal disruption to the end user by identifying possible conflicts or business application effects of enabling a specific feature Using the historical data that is gathered by the solution.		Corrigendum-III
267	SOR-C- Network –C-2 –End point protection for end user	New	Additional Clause	The proposed solution should include the capability for security admins to remotely connect to endpoint via secure shell for live forensics, data collection and remote remediation even when the endpoint is off the corporate network.	Remote shell capability will enable Railtel to remotely triage, investigate and gather forensics from endpoints not on the corporate network - such as a WFH scenario / on field scenario.		As per RFP
268	SOR-C- Network –C-2 –End point protection for end user	New	Additional Clause	The proposed solution should have the capability to perform threat hunting based on MITRE TIDs, Tactics, Techniques & Procedures and IOCs.	Hunting on TIDs / TTPs enables Railtel to hunt proactively in the environment for suspicious behaviors, while IOC hunting identifies breach artifacts. Both are essential in identifying todays modern attacks.		As per RFP
269	SOR-C- Network –C-2 –End point protection for end user	New	Additional Clause	The proposed solution should include actionable threat intelligence capabilities on the latest attack campaigns - including observed TTPs, policy recommendations, IOCs.	Actionable threat intelligence will enable Railtel team to stay ahead of emerging attacks and enrich existing security stack.		As per RFP
270	3.5	60	For AMC he will be paid @ 3.5% per annum only. If the Tenderer quotes a higher base rate for AMC, he will be paid at his quoted rate per annum and five-year differential cost shall be added to offered cost. AMC would have to be valid for minimum period of 5 years after the warranty.	1) Kindly remove this clause, as a Software OEM, we do not offer AMC for our Software licences at this rate per annum. This is not the Industry standard for AMC for Software. 2) Also please advise if the total Comprehensive Support period is 5 years (Warranty period to be taken as per Page 77, Clause 2)	In this clause it is mentioned 5 years after the warranty period.		As per RFP
271		New					N/A
272							N/A
273							N/A
274	SCHEDULE OF REQUIREMENT	5	Backup Solution at DC and DR along with Tape/Disk Based storage as per specification given in Chapter-3A	Kindly update this point to " Backup Solution at DC and DR along with Virutal Tape Library /Disk Based storage as per specification given in Chapter-3A"	There is no technology comparison between Tape and Disk based Backup solution since there is a huge gap in terms of performance and commercials between Tape and Disk based storage. Request to update this to Modify to Virtual Tape library (VTL) since VTL is based on Disk based technology.		Corrigendum-III

275	3. Design Considerations	13	Veeam is the existing incumbent in the Backup Space. It would be recommended to have Backup Solution co-exist with incumbent solution and enhance the backup capacity. However bidder may propose any other backup solution which needs to be integrated with existing backup solution i.e. Veeam Backup Solution or propose entirely a new backup solution comprising existing and proposed solution capacity.	Request to kindly share the details of existing Backup solution.	Since bidder is allowed to quote entirely new Backup solution if incumbent backup vendor is not quoted. Request to share details like: Total existing VM's, Host Servers, backed up storage, type of storage media etc.		Refer- Existing Inventory Sheet enclosed in "Annexure-A"
276	3. Design Considerations	13	Total 50 nodes each at DC & DR have been envisaged for connectivity with proposed SAN Switch.	We understand a total of 60 servers are required as per New requirement across DC & DR. In the above specifications it's mentioned that SAN connectivity for existing Servers is separate and under Railtel scope. Request to clarify on Nodes count and their connectivity.	Clarification requested on the port distribution of SAN switch with total server		Clarification: Existing Nodes may also be connected with SAN switch which bidder has to implement, however any additional hardware requirement in existing server shall be arranged by RailTel.
277	SOR-A-Storage – A-3 – SAN Switch:	22	Proposed switch should be NVMe ready to allow seamless transition to related workloads without any SAN switch upgrade.	Request to remove this point	Not all SAN switches support NVMe support capability. Request to remove this point for wider participation.		Corrigendum-III
278	SOR-A-Storage – A-4 – HBA Card	22	Should have compatibility with existing servers of RailTel	We understand Railtel currently has mix of Server vendors in their Datacenter. Request to kindly confirm if additional HBA cards asked in SOR are to be provided for new quoted servers or for existing servers. If these cards are required for existing servers, request to confirm Server Make & Model since we understand Railtel currently has mix of server OEM's.	Clarification requested on HBA cards asked in SOR		Refer- Existing Inventory Sheet enclosed in "Annexure-A", HBA Card provided must be fully populated from Day-1.
279	SOR-B- Cloud Solution –B-1- Rack Servers:	23	Server Vendor should be under Gartner leaders Magic quadrant in last available report.	Kindly update this point to " Server Vendor should be under Gartner leaders Magic quadrant in 2016 report".	Gartner has last published Server report in 2016. Is this report still valid for Railtel Requirement. Request to kindly confirm.		Clarification: Yes, in case Gartner latest reports are not available for any required Hardware & Software, its last available report to be considered.
280	SOR-B- Cloud Solution –B-1- Rack Servers:	23	The management tool should be able to provide global resource pooling and policy management to enable policy based automation.	Kindly update this point to "The management tool should be able to provide Global resource pooling/Management and policy management to enable policy based automation."	We understand by pooling it is not that server resources to be pooled centrally both at DC & DR, we understand that proposed servers should be able for central Management & Monitoring. Request to confirm our understanding.		As per RFP

281	SOR-B- Cloud Solution –B-1- Rack Servers:	24	For server data storage 16x60= 960TB. Additional storage capacity of each server (80-64=16) TB should be arranged in SAN storage for the proposed solution. Each data center needs to be provisioned with 480TB usable capacity using 6TB or less NL-SAS drives on RAID6 in offered storage solution.	Specs for central storage asks for 600TB storage capacity . Request to kindly confirm if Railtel is asking bidders to include additional 480TB storage capacity in the Storage array both at DC & DR on NL-SAS drives.	Clarification requested for Storage		Corrigendum-III
282	Monitoring and Management of DC/HCI Infrastructure:	45	The analytics platform should be able to capture and analyze flow and process telemetry from all workloads across all DC's and Cloud environments in near real time	Request to confirm if Railtel wishes to seamlessly integrate new VM's with existing Application visibility solution or entire new solution is required for existing & new Infrastructure. If yes, request to kindly share the virtual machine & Host counts w.r.t existing Setup both at DC and DR.	Clarification requested		Clarification: Bidder may propose the extension to existing Solution to leveraged or propose the entirely a new solution . Bidder needs to provide the solution which must provide single console for its Management.For the solution design kindly refer the existing inventory details.
283	General Requirement in Multifactor Authentication	46	The proposed solution should be able to provide multifactor authentication for Windows, Mac, Linux Operating systems & Database etc.	Kindly share more information on what type of Database application are being considered and whether do they support RADIUS or SAML 2.0?	Clarification requested		Clarification: Applications supports Radius and SAML.
284	General Requirement in Multifactor Authentication	46	The proposed solution be able to provide multifactor authentication for VPNs, Firewall, Network Switch's, Router, Wireless controllers and web proxy	Kindly share details on type of WLC & Web Proxy solution is being used	Clarification requested		Clarification: WLC is Cisco and Rackus.
285	General Requirement in Multifactor Authentication	46	The proposed solution should provide multifactor authentication for in-house developed application	Kindly share Details on application languages which needs to be integrated and what is the supported authentication protocol is it Radius or Saml 2.0?	Clarification requested		Clarification: Applications supports Radius and SAML.
286	General Requirement in Multifactor Authentication	47	The proposed solution should provide multifactor authentication for virtualization platform (HCI)	Kindly share details on what is the functionality needed here?	As MFA typically integrated with VDI and offers MFA for user login. Need more details on functional ask here.		Clarification: MFA solution should be able to integrate with applications VMware Horizon/View, MS Server, ADFS etc.
287	General Requirement in Multifactor Authentication	47	The proposed solution should be able to be deployed in virtual environments such as VMware, LPAR or Hyper-V	Please relax this point by replacing 'Any component of the proposed solution should be deployed on an Windows or Linux VM running on VMWare, Hyper-V or LPAR hypervisor'	As not all OEMs have components that get deployed on bare metal virtual machines.		Corrigendum-III

288	General Requirement in Multifactor Authentication	48	The Authentication Mechanism should provide capabilities to prevent Brute Force Attacks and should be able to send alerts to the Admin/Helpdesk in case of a brute force attack on a user account.	Please remove this point. As primary credentials are not stored in MFA solution and Brute Force attack usually happens on user's primary authentication. So not a valid ask.	As in the RFP the ask is to not store the user credentials thus there is no chance that Brute Force Attack can be done as this happens on the primary credential source.		Corrigendum-III
289	Integration in Multifactor Authentication	48	Integration with PIM (Privilege identity management) solution	Kindly provide clarification on which PIM solution needs to be integrated	Clarification requested		Clarification: Solution should provide an interface or method to integrate over Radius, SAML or API.
290	Clause 10, SOR-C_Network-C-2-End Point Protection for End User	40	Endpoint software should be easy to deploy and support (not limited to) deployment through 3rd party systems management tools	Please change as "Endpoint software should be easy to deploy and support (not limited to) deployment through 3rd party systems management tools or by publishing the URL	This is to ensure that multiple deployment options are available for agent roll out		As per RFP
291	Clause 26 SOR-C_Network-C-2-End Point Protection for End User	41	The solution shall be capable of working in Windows, Windows Server & Linux operating systems	The solution shall be capable of working in Windows, Windows Server, MacOS, Linux operating systems	As Mac is also widely used in todays network. Having a MAC support will ensure that a solution supports a larger end user operating environment.		Corrigendum-III
292	Clause 2, solution building block	12	vii Core router for DC & DR	This item mentioned in this clause is not found SOR line item. Kindly clarify whether any such requirement is there for Router at DC & DR and what is the quantity	Clarification requested		Corrigendum-III
293	Clause 3: Solution Building Block	12	vi. Total 200 no. of VMs across DC & DR have been envisaged for overall solution consideration	Kindly clarify that the requirement of VM to be captured are 100 VM in DC and 100 VM in DR	Clarification requested		Clarification: Total 200 No. of VM including both DC and DR is required, Distribution details will be shared with successful bidder.
294	Clause 6 a: Leaf Switch	25,35	48 x 1G/10G/25G Multi Mode Fiber Interface populated with 48*10G multi mode interfaces.	Kindly clarify port speed requirement is 1/10/25 Gbps and port to be populated with 10G Multimode SFP	Clarification requested		Clarification: Yes all 48 ports to be equipped with 10G short reach multimode SFP+
295	Clause 28: Leaf Switch	26,37	Spanning Tree Protocol (IEEE 801.D, 802.1W, 802.1S)	Software defin networking is done by creating VxLAN Fabric with Layer 3 protocols. Kindly clarify "Spanning tree protocol" speccified here are related to connecting Layer 2 switches running Spanning tree protocol.	Clarification requested		As per RFP
296	Clause 56: Leaf Switch	27,38	Switch should support to prevent edge devices in the network not administrator's controlled from becoming Spanning Tree Protocol root nodes	Software defin networking is done by creating VxLAN Fabric with Layer 3 protocols. Kindly clarify "Spanning tree protocol" speccified here are related to connecting Layer 2 switches running Spanning tree protocol.	Clarification requested		As per RFP
297	License	46	All licenses should be quoted for total 200 Virtual Machines/ Instances across DC & DR.	Kindly clarify that the requirement of VM to be captured are 100 VM in DC and 100 VM in DR	Clarification requested		Clarification: Distribution details will be shared with successful bidder.

298	point 7 , Scope of Work	14	vii.RailTel is already using the SDN architecture in its DC and DR , bidder has to ensure that If any integration issue of the proposed Leaf switches with the existing controller and Spine - Leaf architecture, bidder to propose Spine switches and SDN controller separately to make the solution up and running without any additional cost to RailTel.	Required detail of existing SDN infra	For Existing infra integration		Clarification: The existing SDN infrastructure comprises 64x100G port Spine Switch (12 Tbps throughput) (Spine switch - two in DC & two in DR making HA mode) and N+1 SDN controller in DC and DR. Bidder may propose equivalent or higher capacity. Existing inventory sheet is enclosed in "Annexure-A".
299	point 12, Scope of Work	15	Any Management switches required for the proposed solution will be provisioned by the bidder in redundant topology.	hardware redundancy or Vlan topology	need clarity for ILO / iDRAC / UCS port		Clarification: Bidder needs to provide Minimum 2 numbers of management switch in DC and Two numbers in DR. 48 port 10/100/1000 BaseT with 4x10G uplink Switch with Redundant Power supply and stackable Switch. If in case bidder requires more ports as per the solution proposed , bidder to provision accordingly.
300	Point 9,3.Design Considerations	13	Veeam is the existing incumbent in the Backup Space. It would be recommended to have Backup Solution co-exist with incumbent solution and enhance the backup capacity. However bidder may propose any other backup solution which needs to be integrated with existing backup solution i.e. Veeam Backup Solution or propose entirely a new backup solution comprising existing and proposed solution capacity.	Need more clarity about currently deployed backup software and backup storage ,please explain about the expectation about integration			As per RFP
301	Point 10, 3.Design Considerations	13	x.This RFP is extension of e-office phase-I, under which VMware vCloud suite is already deployed at Gurgaon DC and Secunderabad DC. Any proposed cloud solution in the RFP should be integrable with existing cloud system to work as a single cluster. Bidder should propose the solution considering the existing infrastructure and software (Licenses).	Please share current deployment architecture			As per RFP

302	Scope of Work	13	The primary objective of this RFP is to select a bidder who shall supply, install, test and commission IT infrastructure and software for e-Office	Please explain more about bidder's & OEMs scope in relation to e-office deployment			As per RFP
303	Scope of Work Point No.5	14	v.Bidder has to ensure smooth migration from existing SAN switch to proposed SAN switch	Please provide existing san switch make and model details and port information. Also confirm no of server which are connected with these switches. Any activity and downtime required at server end to be taken care by Railtel.	Firmware of SFP connectors could have compatibility issue with the new proposed switch.		Refer- Existing Inventory Sheet enclosed in "Annexure-A"
304	Scope of Work Point No.13	15	xiii.Bidder needs to integrate the cloud platform with existing LDAP solution in RailTel.	Please describe about existing LDAP deployment			Clarification: Open LDAP and Active Directory is used.
305	Data Center Service Requirements	16	i. Supply, Installation, Configuration, performance Tuning & Integration, Performance Testing , Acceptance Testing, Commissioning and Training of the supplied hardware, Software, network equipment and network software as per Schedule of Requirements.	We are assuming RailTel already having performance tool			As per RFP
306	7.B idder shall perform following work for equipment installation implementation & integration with existing Infrastructure: Point No :	17	viii.Bidder shall perform integration of HCI with the supplied backup solution and should enable integration with VM to perform backup of VM data and configuration files.	Please provide high level architecture os the current deployed solution. Also suggest in detail scope for fresh deployment in DC & DR.			As per RFP
307	SOR-A: Storage – A-1 - Unified Storage system of 600 TB: Point no 5	19	The Storage Systems should be supplied with minimum 600TB Usable capacity using 500 capacity on SAS/NLSAS Drives on RAID6 and 100TB using SSD on RAID 6 and scalable up to 1PetaByte usable capacity using SAS/SSD.	Typo error -it should be as 500TB capacity on SAS/NLSAS			Corrigendum-III
308	SOR –D Licenses for OS, DB and NMS/EMS:	41	Multi domain SSL certificates – 4 Nos.	No. of SAN entries not mentioned			As per RFP
309	SOW - xvi	15	VMware vCloud Suite Latest edition or equivalent -114 Nos. VMware NSX Data Center (NSX-T) Advanced per Processor or equivalent-114 Nos. VMware vSAN 6 or latest Enterprise for 1 Processor or equivalent - 105 Nos. VMware Site Recovery Manager Standard Latest edition (25 VM Pack) or equivalent -6 Nos.	Please suggest if the defined count is correct.			As per RFP

310	SOR –D	41	Licenses for OS, DB and NMS/EMS:	We understand from other sections that RailTel requires 24x7 support for all systems. Please confirm same is also applicable for licenses listed under SOR-D	This clarification would help SI/OEM to propose the right product SKU		As per RFP
311	SOR-B, B-3	5	Software defined Storage, Virtualization Virtual Cloud Foundation& Site Recovery License as per Technical Specification given in chapter-3A	Based on the requirement kindly amend this line for clarity as: "Software defined Storage, Cloud Management Platform, SDN & Site Recovery License as per Technical Specification given in chapter-3A"	Amendment required for more clarity and to avoid any ambiguity		As per RFP
312	SOR-B- Cloud Solution –B-3- Software defined Storage, Virtualization Virtual Cloud Foundation & Site Recovery License:	29	SOR-B- Cloud Solution –B-3- Software defined Storage, Virtualization Virtual Cloud Foundation & Site Recovery License:	Based on the requirement kindly amend this line for clarity as: "Software defined Storage, Cloud Management Platform, SDN & Site Recovery License as per Technical Specification given in chapter-3A"	Amendment required for more clarity and to avoid any ambiguity		As per RFP
313	4. Scope of Work-xiii	15	xiii. Bidder needs to integrate the cloud platform with existing LDAP solution in RailTel. xvi. Offered cloud solution version should be latest and bidder needs to perform the migration/upgradation activity of the existing cloud solution to maintain uniformity of entire cloud solution.	Kindly add following clause "VMware cloud management paltform is already setup in existing private cloud at RailTel. For VMware solution, scope will be to 1. Prepare new servers being procured as part of this tender and add them as part of existing cloud setup for expansion . 2. Migrate existing NSX-V to NSX-T 3. Integration of cloud portal with Multi factor authentication solution being procured in this tender	We understand that for VMware solution all this activities are not be applicable as VMware cloud management paltform is already setup and as part of scope new servers being procured as part of this tender needs to be prepared and added in existing cloud setup for expansion.		Clarification: Complete scope of work has been defined considering both scenarios that bidder may propose VMware CMP or may propose entirely new CMP platform . If bidder is proposing VMware CMP than high level SOW to be read as but not limited to " VMware cloud management paltform is already setup in existing private cloud at RailTel. For VMware solution, scope will be to 1. Prepare new servers being procured as part of this tender and add them as part of existing cloud setup for expansion . 2. Migrate existing NSX-V to NSX-T 3. Integration of cloud portal with Multi factor authentication solution being procured in this tender 4. Implement SSO for cloud management software components for 15 to 20 administrators. 5. Replicate cloud management components to DR site ". If Bidder propose new CMP platform , then bidder has to perform all the activities as defined in tender."
314	7-iv	17	iv. Integrate Virtualization Manager with Cloud Management Platform (CMP), Software Defined Network (SDN) & Software Defined Storage (SDS). vi. Create Virtual machines for Linux OS or Windows, Virtual machine templates, Virtual machine configured in High Availability mode in cluster, affinity group creation of virtual machines and virtual machine backup configuration (Snapshot and Clone). vii. Configure storage policies to automate provisioning and balancing of storage resources to ensure that each VM gets the specified storage resources and services. viii. Bidder shall perform integration of HCI with the supplied backup solution and should enable integration with VM to perform backup of VM data and configuration files.	4. Implement SSO for cloud management software components for 15 to 20 administrators 5. Replicate cloud management components to DR site "			

315	8	17	"i. Bidder should integrate the CMP fully with the supplied HCI solution i.e., integration with manager of the hypervisor, Software Defined Network, Software Defined Storage, etc." "ii. The bidder should create policy-based controls of cloud resources and should configure Rolebased policy management, administration and enforce role- based policies." "iii. The bidder should create workflow and blueprints for IaaS, PaaS as defined in Functional Requirements" "iv. The bidder shall also create basic & necessary reports for the analysis of resources (CPU, Memory, Storage and Network) utilization and available resources." v. Bidder should configure auto-scaling of resource as per demand "vi. The bidder should configure CMP with, backup software to enable configuration of backup and restore through self- service Dashboard."				Clarification: Complete scope of work has been defined considering both scenarios that bidder may propose VMware CMP or may propose entirely new CMP platform . If bidder is proposing VMware CMP than high level SOW to be read as but not limited to " VMware cloud management platform is already setup in existing private cloud at RailTel. For VMware solution, scope will be to 1. Prepare new servers being procured as part of this tender and add them as part of existing cloud setup for expansion . 2. Migrate existing NSX-V to NSX-T 3. Integration of cloud portal with Multi factor authentication solution being procured in this tender 4. Implement SSO for cloud management software components for 15 to 20 administrators. 5. Replicate cloud management components to DR site ". If Bidder propose new CMP platform , then bidder has to perform all the activities as defined in tender."
316	SOR-B	29	The solution should have capability to automate the bring-up process of the entire software platform, including deployment of infrastructure VMs, creation of the management cluster, configuration of VLANs, virtual storage, virtual network, and cluster creation and provisioning.	We understand that VMware cloud management platform with management cluster is already setup in existing RailTel private cloud. So this clause is not applicable. Kindly confirm.	VMware cloud management platform along with management cluster is already setup in existing RailTel private cloud. So bring-up of software platform, management cluster, infrastructure VMs is not required		Clarification: Specification given considering the scenario that bidder may propose the extension of VMware CMP or may propose the entire new CMP.
317	SOR-B	29	The solution should provide true multi tenancy, Each tenant needs to be able to create their own profiles/blueprints, share them to a public catalog, and not be able to see other tenant's build profiles, compute resources, or managed machines. At least 3 tenants will be required to be configured during the Cloud deployment.	Kindly amend this as "The solution should provide true multi tenancy, Each tenant needs to be able to create their own profiles/blueprints, share them to a public catalog, and not be able to see other tenant's build profiles, compute resources, or managed machines. At least 3 Business Groups will be required to be configured during the Cloud deployment."	As per our understanding in present setup different departments are onboarded with business groups. More business groups can be created as per requirement of this clause.		As per RFP
318	SOR-B	31	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.	Request to kindly remove this clause	This feature is not part of the components asked at section 4 page 15 point xvi. Also kindly note this feature is not a part of currently running stack in RailTel eoffice project.		As per RFP

319	4. Scope of Work-xvi.	15	VMware Site Recovery Manager Standard Latest edition (25 VM Pack) or equivalent -6 Nos.	Kindly amend as "VMware Site Recovery Manager Enterprise Latest edition (25 VM Pack) -6 Nos."	Existing setup has Site Recovery Manager Enterprise edition		Corrigendum-III
320	4. Scope of Work-xvi.	15	VMware vSAN 6 or latest Enterprise for 1 Processor or equivalent - 105 Nos.	Kindly amend as "VMware vSAN Advanced 6 or latest for 1 Processor or equivalent - 105 Nos."	Existing setup is with vSAN Advanced.		Corrigendum-III
321	SOR-B	32	The solution should provide automatic private cloud metering and consumption analysis. The Cloud portal will be configured with Multi factor authentication during the deployment.	VMware Cloud portal already setup for RailTel e-Office will be configured with Multi factor authentication solution being procured as part of this tender. Supported authentication types are listed on this link. Would request that the asked MFA solution should be compatible as per this list. https://docs.vmware.com/en/vRealize-Automation/7.6/com.vmware.vra.prepare.use.doc/GUID-D16CB962-78B9-4FAD-92D5-E16613A381FF.html?hWord=N4lghgNiBclC4HcD2ACAZmAxnJAnFYArnABYcmAdnAJaZg1IUgC+QA			Clarification: The solution should support following protocols for integration including Radius, SAML, RestAPI, OIDC, Web SDK etc or equivalent for providing MFA services.
322	SOR-B	33	There should be single portal to manage all the Cloud based management software using single sign on functionality.	We understand that this functionality is required for RailTel administrators and there would be 15 to 20 such users. Kindly confirm if we can propose the solution for 20 users.			Corrigendum-III
323	12.1.1	64	12.1.1 The Equipment offered by the OEM or equipment of the same series/family from the same OEM should have been satisfactorily working in Government/PSUs/Telecom Service Providers network for at least 12 months as on date of opening of tender, in India or Abroad. The certificates from the actual users will have to be submitted along with bid.	Kindly amend "12.1.1 The Equipment offered by the OEM or equipment of the same series/family from the same OEM should have been satisfactorily working in Government/PSUs/Telecom Service Providers network for at least 12 months as on date of opening of tender, in India or Abroad. The certificates from the actual users or publically available references/ case studies will have to be submitted along with bid."	Kindly amend to accept the publically available customer references/ case studies		As per RFP

324	12.1.2	64	12.1.2 The OEM should have supplied at least 35% of the tendered value/SOR Value of the equipment offered or equipment of the same series/family during last preceding 3 financial years (i.e. current year and three previous financial years) as on opening of bid to Government/PSUs/Telecom Service Providers. OEM should submit self-certificate with proper contact detail of clients along with PO reference and amount supplied (Firm Name, Contact person, Designation, Telephone Number, Fax, Official mail id etc.). The same should be issued by authorized signatory.	We understand that Global Government/PSUs/Telecom Service Providers references will be acceptable. Kindly confirm			As per RFP
325	3.5	60	For AMC he will be paid @ 3.5% per annum only. If the Tenderer quotes a higher base rate for AMC, he will be paid at his quoted rate per annum and five-year differential cost shall be added to offered cost. AMC would have to be valid for minimum period of 5 years after the warranty.	1) Kindly remove this clause, as a Software OEM, we do not offer AMC for our Software licences at this rate per annum. This is not the Industry standard for AMC for Software. 2) Also please advise if the total Comprehensive Support period is 5 years (Warranty period to be taken as per Page 77, Clause 2)	In this clause it is mentioned 5 years after the warranty period.		As per RFP
326	Additional	New	Backup	Will RAILTEL be interested in automated failover and orchestration of DR, along with failover plans and DR readiness checks, between DC and DR site using backup copies as well as production VM replication, where hypervisor level DR is not already established? How many critical VMs would you like to have as part of this automated DR functionality.			As per RFP
327	SOR-A: Storage – A-1 - Unified Storage system of 600 TB	19	The Storage Systems should be supplied with minimum 600TB Usable capacity using 500 capacity on SAS/NLSAS Drives on RAID 6 and 100TB using SSD on RAID 6 and scalable up to 1PetaByte usable capacity using SAS/SSD.	Please define capacity of 500 qty of which type of drive, NL-SAS or SAS?			Corrigendum-III

328			The storage should support and be configured with automated data tiering between different drive types namely SSD, SAS, and NL-SAS within the same storage array. The storage should be capable of moving data blocks between these drive types (up and down the tier) depending on the access patterns to ensure optimum storage performance.	Request you to amend as below, "The storage should support and be configured with automated data tiering between different drive types namely SSD & SAS or SSD & NL-SAS within the same storage array. The storage should be capable of moving data blocks between these drive types (up to down the tier) depending on the access patterns to ensure optimum storage performance."			As per RFP
329			The Storage should be scalable to at least 800 SFF/LFF disk drives on the same set of controllers.	Request you to amend as below, "The Storage should be scalable to at least 1400 SFF/LFF disk drives on the same set of controllers."			Clarification: As per RFP, However bidder may propose higher storage scalable capacity.
330			The Storage should support minimum RAID 5, RAID 6 and RAID10 as different applications requires different performance levels	Request you to amend as below, "The Storage should support minimum RAID 6 or equivalent".			As per RFP
331			Storage should be equipped with 8*32 Gbps FC ports, 4*10Gbe port for host connectivity. Required SFPs/Optical Module to be populated from day one	Request you to amend as below, "Storage should be equipped with 8*32 Gbps FC ports, 4*40G Ports and 4*10Gbe port for host connectivity. Required SFPs/Optical Module to be populated from day one"			As per RFP
332			The storage system should have minimum 512GB global cache on the same set of proposed controllers for both reads & writes. Cache memory should be delivered on DRAM, any other device or HDD should not be considered as cache. Cache shall be completely dynamic for read and write operations.	Request you to amend as below. "The storage system should have minimum 512GB DRAM cache across the same set of proposed controllers for both reads & writes. Cache memory should be delivered on DRAM, any other device or HDD should not be considered as cache. Cache shall be completely dynamic for read and write operations."			As per RFP
333			The proposed storage system should support at least 24000 LUNs or volumes	Request you to amend as below, " The proposed storage system should support at least 5000 LUNs or Volumes"			Corrigendum-III
334	Solution Requirement: Monitoring/point 42	44	Provide online and offline reports that allow the user to view the present usage of their devices. Reports generates should be exportable in the format of HTML, PDF, Excel and CSV	Online reports can be fetched directly from the reporting engine, Offline reports can be exported into various supported format. PDF, CSV etc.			Clarification: Reports should be genrated in different format like PDF, Excel, HTML.
335	Solution Requirement: Monitoring/point 57	44	System licensing should be based only on Physical Hosts and not charge separately for individual guest VMs running on VM Hosts	License have to factor Virtual OS instance too.			As per RFP
336	Solution Requirement: Monitoring/point 62	45	Provide XML, Corba, REST API, SOAP based system to communicate with external software	Provide any of the XML, Corba, REST API, SOAP based system to communicate with external software			Clarification: Software should support all kind of API integration if required in future.

337	SOR-A-Storage – A-2 – Backup solution at DC & DR Point - 6		Additional Clause	Will there not be Backup Storage requirement at DR, in case 1) if production is running DR. 2) How backup of local VMs would happen at DR.			As per RFP
338	SOR-C- Network –C-2 –End point protection for end user		27. The endpoint solution shall be able to pinpoint vulnerable versions of popular applications installed in Endpoints	The endpoint solution shall be able to protect vulnerable versions of popular applications installed in Endpoints with multi-layered prevention.	Protection is key for all applications and processes. By identifying attacker behaviour with Tactics, Techniques and Procedures organizations can stay ahead of vulnerabilities by having multi-layered prevention of these behaviours.		Corrigendum-III
339	SOR-C- Network –C-2 –End point protection for end user		22. The proposed solution shall have the capability to quarantine the malicious application/program/file automatically without quarantining the entire user machine from network which would affect business productivity of the user	The proposed solution shall have the capability to quarantine the malicious application/program/file automatically without quarantining the entire user machine from network which would affect business productivity of the user. The solution should also include the capability to isolate the host if required to protect from lateral movement.	Host Isolation provides an additional layer of security control where is a user or endpoint is remote, it enables the security team to quickly isolate the endpoint on incident detection (for critical incidents) until they inspect for forensics and next steps.		As per RFP
340	SOR-C- Network –C-2 –End point protection for end user		23. The proposed solution shall have the capability to work with Indicators of Compromise (IOC's)	The proposed solution shall have the capability to work with Indicators of Compromise (IOC's) and correlate MITRE ATT&CK Tactics Techniques & Procedures (TTPs)	IOC's are post-breach or reactive in nature. Tactics, Techniques and Procedures enable organizations to hunt proactively for attacker behavior and are now a widely adopted standard across all endpoint security solutions. Reference: attack.mitre.org		As per RFP
341	SOR-C- Network –C-2 –End point protection for end user		28. The proposed solution shall be able to identify the threat root cause of incidents, child processes of malwares and parent file disposition	The proposed solution shall be able to identify the threat root cause of incidents, child processes of malwares and parent file disposition, network connections, registry modifications, scripts executed and targets injected.	Metadata such as network connections, registry modifications, injections and script executions are crucial to uncovering all stages of the attack and artifacts from a single console.		As per RFP
342	SOR-C- Network –C-2 –End point protection for end user		32. Solution should allow Users to choose to preview the new Policy UI.	The solution should allow administrators to identify policy effects based on historical data before apply the Prevention policy.	It should enable administrators to intelligently push policies that work with minimal disruption to the end user by identifying possible conflicts or business application effects of enabling a specific feature Using the historical data that is gathered by the solution.		Corrigendum-III
343	SOR-C- Network –C-2 –End point protection for end user		Additional Clause	The proposed solution should include the capability for security admins to remotely connect to endpoint via secure shell for live forensics, data collection and remote remediation even when the endpoint is off the corporate network.	Remote shell capability will enable Railtel to remotely triage, investigate and gather forensics from endpoints not on the corporate network - such as a WFH scenario / on field scenario.		As per RFP
344	SOR-C- Network –C-2 –End point protection for end user		Additional Clause	The proposed solution should have the capability to perform threat hunting based on MITRE TIDs, Tactics, Techniques & Procedures and IOCs.	Hunting on TIDs / TTPs enables Railtel to hunt proactively in the environment for suspicious behaviors, while IOC hunting identifies breach artifacts. Both are essential in identifying todays modern attacks.		As per RFP
345	SOR-C- Network –C-2 –End point protection for end user		Additional Clause	The proposed solution should include actionable threat intelligence capabilities on the latest attack campaigns - including observed TTPs, policy recommendations, IOCs.	Actionable threat intelligence will enable Railtel team to stay ahead of emerging attacks and enrich existing security stack.		As per RFP

346	SOR-C- Network –C-2 –End point protection for end user		Additional Clause	The majority of today's cyberattacks feature advanced tactics such as lateral movement and island hopping that target legitimate tools to inflict damage. These sophisticated hacking methods pose a tremendous risk to Railtel protecting high-value assets, including money, intellectual property and state secrets.			As per RFP
347				Only by applying the unlimited processing power and scale of the cloud to the endpoint security problem can we keep up with — and even predict — these advanced threats. The cloud can monitor an endpoint's behavior, looking at both normal and abnormal activity, and compare that activity to vast stores of data from other endpoints. By analyzing these event streams across all endpoints under management through a process known as streaming analytics, the cloud creates a global threat monitoring system, allowing it to detect and predict attacks — even if they've never been seen before.			As per RFP
348				The cloud also enables simplified operations – No premise management equipment or servers, no multiple agents for specific tasks – leverage a single agent that enables all capabilities and ensures users are protected no matter where they are.			As per RFP
349				We therefore suggest Railtel to consider and allow Cloud based NGAV+EDR solutions that will enable Railtel to better secure their endpoints and servers.			As per RFP
350	SOR-C- Network –C-2 –End point protection for end user, Point no. 1	40	The bidder shall propose dedicated end point based solution to protect systems Advanced Targeted Attacks and APT's	As per specification you have asked for protection from Advanced Targeted Attacks/APT's and to achieve holistic protection from known and unknown threats a sandbox solution will be required.	EPP solution does not have compute where they can simulate endpoint environments to detonate objects carrying malicious codes. Hence a sandbox technology will be required which is specifically meant to cater unknown/Zero day attacks by simulating your endpoint environment i.e. OS, browser, MS office versions etc. Hence its a humble submission to incorporate sandbox solution with proposed solution to cater APT attacks. Clause should read as : The bidder shall propose dedicated end point based solution to protect systems from Advanced Targeted Attacks and APT's by integrating with sandbox solution supporting customised images having 60 virtual analyzers.		As per RFP

351	SOR-C- Network –C-2 –End point protection for end user, Point no. 2	40	The proposed solution shall work on a signature-less mechanism to stop threats without relying on a database to be present at the endpoint	Considering current threat landscape which is changing very rapidly and dynamically just relying on single technique is not adequate and will work as a single point of failure	As you have already considered the importance of Gartner in this RFP which itself said in his report that merely relying on single technique can not give you required protection also this is completely violating MoUD, NCIIPC, NIST and Cert-In guidelines. Hence considering defense in depth strategy a proposed endpoint solution should consist combination of both detection as well as prevention techniques to avoid single point of failure. Hence it is requested to incorporate prevention techniques as well instead of merely relying on detection techniques. Clause should read as : The proposed solution shall work on machine learning\signature-less mechanism\Behavior monitoring also use Firewall, Device control, Variant protection, Census check, crypto malware, fileless malware, Portable Executable files control, CVE number visibility, Application/Process control, Virtual patching and Data Exfiltration capability in a single unified agent to stop threats holistically.		As per RFP
352	SOR-C- Network –C-2 –End point protection for end user, Point no. 5	40	The proposed solution shall utilize layered and defense in depth approach, wherein the solution cannot be of the same make as existing endpoint AV	The proposed solution should co-exist with existing AV that is something you have already required as per point no. 4 of specification, now specifically mention that existing AV vendor can not participate by just giving justification of defense in depth approach is not logical	This point is restrictive in nature and not allowing our participation as EPP does consists multiple features and modules those do not have any dependency on each other and completely adhere defense in depth approach. Hence its a humble submission to dilute this clause to allow our participation also to achieve threat protection holistically. Clause should read as : The proposed solution shall utilize layered and defense in depth approach by incorporating multiple security layers i.e Application/Process control, Virtual patching and Data Exfiltration, Machine learning and Behavior Monitoring capability in a single unified agent avoiding single point of failure.		Corrigendum-III

353	SOR-C- Network –C-2 –End point protection for end user, Point no. 8	40	Security vendor should have a dedicated research organisation that is focus on vulnerability research and should actively contribute to discoveries of new vulnerabilities exploited in the wild.	As you have understand the criticality and importance of contribution towards undisclosed vulnerabilities those are not even discovered by other infrastructure/security vendors. Public discloser is important to see how much contribution vendor has done in terms of vulnerability discloser also it should be acknowledge by microsoft and Adobe those are being widely used in industry and vendor should be recognised by pioneer threat research institution.	Vendor's contribution towards discloser of undisclosed vulnerability lie in commercially available application/OS is need of the hour and this capability give you proactive shield from sophisticated attacks which can use these open vulnerabilities not discovered by even vendors i.e. Microsoft, Adobe, etc. but how much contribution these vendors are making is something very crucial. Hence its a humble submission that vendor should publish these statistics of thier vulnerability disclosers and same should be acknowledge by other vendors i.e. Microsoft, Adobe, etc. also vendor should got recognised by Forrester who is leader in vulnerability research. Clause should read as : Security vendor should have a dedicated research organisation/vertical that is focus on vulnerability research and should actively contribute to discover undisclosed vulnerabilities and vendor should be in leader quadrant as per Forrester Wave Endpoint Security 2019 report.		As per RFP
354	SOR-C- Network –C-2 –End point protection for end user, Point no. 9	40	Software footprint should be small <50MB and should support interactive and/or silent install. Total of 39000 Licenses should be factored for this End Points from Day- 1. Proposed solution should support 100,000 concurrent end points from day-1 by purchasing additional Lic in future.	Defining any limit on endpoint footprint will going to restrict participation as every OEM is having its own architecture to deliver higher performance with security effectiveness	This point is restrictive in nature and not allowing our participation as every OEM is having its own architecture and methodology to deliver required security effectiveness along with higher performance without impacting user experience. Hence instead of defining limit on endpoint footprint specification should be focus on bringing required security effectiveness with higher performance. Hence its a humble submission to dilute this to allow our participation. Clause should read as : Software footprint should be small and support interactive and/or silent install. Total of 39000 Licenses should be factored for this End Points from Day- 1. Proposed solution should support 100,000 concurrent end points from day-1 by purchasing additional Lic in future.		Corrigendum-III
355	SOR-C- Network –C-2 –End point protection for end user, Point no. 26	41	The solution shall be capable of working in Windows, Windows Server & Linux operating systems	Are you using Linux OS at your endpoint (Laptop/Desktop) machines ? as EDR capability at endpoints running on Linux platform will provide very limited feature which will completely not going to server the purpose.	This point is restrictive in nature and not allowing our participation. Hence its a humble submission to dilute this to allow our participation. Clause should read as : The solution shall be capable of working in Windows, Windows Server & Mac systems		Corrigendum-III

356	SOR-C- Network –C-2 –End point protection for end user, Point no. 27	41	The endpoint solution shall be able to pinpoint vulnerable versions of popular applications installed in Endpoints	A proposed solution should have capability to prevent installation of any malicious application/process in your endpoint environment and by merely "pinpoint" vulnerable application will not going to server the purpose.	Proposed solution should be capable to blocking any malicious application initiating any illegitimate process which can work as a platform to host and perform malicious activities in network. Hence its a humble submission to dilute this clause and consider our recommendations. Clause should read as : The endpoint solution shall be able to block malicious applications/process to installed in Endpoints		Corrigendum-III
357	SOR-C- Network –C-2 –End point protection for end user, Point no. 29	41	The proposed solution should not be dependent on a network sandbox for its detection as it takes up bandwidth and affects productivity and shall provide the option of choosing which files to be submitted for sandboxing, to administrator	Most of the APT vendors are using Sandbox solution in offline mode which will not impose any latency on user experience and complete process is automate in nature. As you have already asked for mitigating Advanced Targeted Attacks and APT's based attack a sandbox solution is required.	APT solution placement is crucial for delivering security effectiveness along with higher performance without impacting user experience and it also depend on the vendor's approach and architecture as well. Most APT vendor sit in offline mode and inspect malicious object passively to give their verdict of unknow threat which do not impact network performance.Hence its a humble submission to incorporate sandbox solution which should tightly integrate with proposed solution and sit in offline mode. Clause should read as : The proposed solution should have network sandbox solution having 60 customised sandbox images simulating endpoint environment for its detection of Advanced Targeted Attacks and should natively integrate with proposed solution with complete automation of file sharing.		Clarification: Proposed EDR solution should have its own Sandboxing feature and should not be dependent on any Network level Sandbox.
358	SOR-C- Network –C-2 –End point protection for end user, Point no. 32	41	Solution should allow Users to choose to preview the new Policy UI.	This clause is restrictive and not allowing our participation and moreover why user interaction is required ?	This clause is restrictive and not allowing our participation as favoring particular OEM.Hence its a humble submission to delete this clause. Clause should read as : Solution should have both web based as well local management console for administrator policy and investigation purpose.		Corrigendum-III
359	SOR-C- Network –C-2 –End point protection for end user, Point no. 32	41	Suggestion	Suggestion	As you have already considered the importance and recognition of Gartner for other components in this RFP. Hence it's a humble request you to consider Gartner recognition for proposed Endpoint protection solution as well which will allow participation of best in the breed solution providers and bring required security effectiveness. Clause should read as : The proposed solution should be positioned in the leader quadrant from last three published Gartner Magic quadrant report for Endpoint Protection		As per RFP
360	SOR –D Licenses for OS, DB and NMS/EMS	41	EDB PostGre SQL support system for DB servers - 860 Nos.	Kindly make it open and amend as "EDB/ VMware PostGre SQL support system for DB servers - 860 cores"	Amendment required to make it open and for wider participation		Corrigendum-III

361	SOR –D Licenses for OS, DB and NMS/EMS	41	EDB PostGre SQL support system for DB servers - 860 Nos.	Kindly mention the segregation for cores for active, passive, DR, reporting instances	Clarification required		Corrigendum-III
362	SOR-C- Network –C-2 –End point protection for end user	41	27. The endpoint solution shall be able to pinpoint vulnerable versions of popular applications installed in Endpoints	The endpoint solution shall be able to protect vulnerable versions of popular applications installed in Endpoints with multi-layered prevention.	Protection is key for all applications and processes. By identifying attacker behaviour with Tactics, Techniques and Procedures organizations can stay ahead of vulnerabilities by having multi-layered prevention of these behaviours.		Corrigendum-III
363	SOR-C- Network –C-2 –End point protection for end user	41	22. The proposed solution shall have the capability to quarantine the malicious application/program/file automatically without quarantining the entire user machine from network which would affect business productivity of the user	The proposed solution shall have the capability to quarantine the malicious application/program/file automatically without quarantining the entire user machine from network which would affect business productivity of the user. The solution should also include the capability to isolate the host if required to protect from lateral movement.	Host Isolation provides an additional layer of security control where is a user or endpoint is remote, it enables the security team to quickly isolate the endpoint on incident detection (for critical incidents) until they inspect for forensics and next steps.		As per RFP
364	SOR-C- Network –C-2 –End point protection for end user	41	23. The proposed solution shall have the capability to work with Indicators of Compromise (IOC's)	The proposed solution shall have the capability to work with Indicators of Compromise (IOC's) and correlate MITRE ATT&CK Tactics Techniques & Procedures (TTPs)	IOC's are post-breach or reactive in nature. Tactics, Techniques and Procedures enable organizations to hunt proactively for attacker behavior and are now a widely adopted standard across all endpoint security solutions. Reference: attack.mitre.org		As per RFP
365	SOR-C- Network –C-2 –End point protection for end user	41	28. The proposed solution shall be able to identify the threat root cause of incidents, child processes of malwares and parent file disposition	The proposed solution shall be able to identify the threat root cause of incidents, child processes of malwares and parent file disposition, network connections, registry modifications, scripts executed and targets injected.	Metadata such as network connections, registry modifications, injections and script executions are crucial to uncovering all stages of the attack and artifacts from a single console.		As per RFP
366	SOR-C- Network –C-2 –End point protection for end user	41	32. Solution should allow Users to choose to preview the new Policy UI.	The solution should allow administrators to identify policy effects based on historical data before apply the Prevention policy.	It should enable administrators to intelligently push policies that work with minimal disruption to the end user by identifying possible conflicts or business application effects of enabling a specific feature Using the historical data that is gathered by the solution.		Corrigendum-III
367	SOR-C- Network –C-2 –End point protection for end user	New	Additional Clause	The proposed solution should include the capability for security admins to remotely connect to endpoint via secure shell for live forensics, data collection and remote remediation even when the endpoint is off the corporate network.	Remote shell capability will enable Railtel to remotely triage, investigate and gather forensics from endpoints not on the corporate network - such as a WFH scenario / on field scenario.		As per RFP
368	SOR-C- Network –C-2 –End point protection for end user	New	Additional Clause	The proposed solution should have the capability to perform threat hunting based on MITRE TIDs, Tactics, Techniques & Procedures and IOCs.	Hunting on TIDs / TTPs enables Railtel to hunt proactively in the environment for suspicious behaviors, while IOC hunting identifies breach artifacts. Both are essential in identifying todays modern attacks.		As per RFP
369	SOR-C- Network –C-2 –End point protection for end user	New	Additional Clause	The proposed solution should include actionable threat intelligence capabilities on the latest attack campaigns - including observed TTPs, policy recommendations, IOCs.	Actionable threat intelligence will enable Railtel team to stay ahead of emerging attacks and enrich existing security stack.		As per RFP

370	12.2.1	64	The tenderer should have executed Single order showcasing supply, installation, testing, commissioning, implementation and operations projects for Data Center solutions commercially costing not less than 35% of the tendered value during last preceding 3 financial years (i.e. current year and three previous financial years) from the date of opening of tender. The bidder shall also furnish Supply/ work completion certificate issued by customer/s for the Purchase Orders/ Work Orders Copy of work orders supported with relevant documentary evidences for the same and the completion certificates issued by customer/s for the Purchase Orders/ Work Orders. Documentary evidence should clearly indicate the nature of systems implemented for each project.	We request you to please provide some relaxation on PQ criteria and change the clause as below:- The tenderer should have executed Single order showcasing supply, installation, testing, commissioning, implementation and operations projects for Data Center solutions commercially costing not less than 25% of the tendered value during last preceding 3 financial years (i.e. current year and three previous financial years) from the date of opening of tender. The bidder shall also furnish Supply/ work completion certificate issued by customer/s for the Purchase Orders/ Work Orders	Relaxation of this PQ clause will give access to more bidders for participation so as to enable healthy competition.		As per RFP
371	Point e) Earnest Money (EMD) at page No. 2 and Clause 20 at page No. 78	2,78	at Page NO. 2 s 35,68,500/- to be made in favor of RailTel online through IREPS Portal. At page No. 78 Earnest Money Deposit (EMD)/ Bid Security Rs. 36,06,000/- (Rs. Thirty Six Lakh Six Thousand only)	There is conflict between EMD amount mentioned at page no. 2 and page no. 78. please clarify the same.			Corrigendum-III
372	Point e) Earnest Money (EMD) at page No. 2 and Clause 20 at page No. 78	2,78	at Page NO. 2 s 35,68,500/- to be made in favor of RailTel online through IREPS Portal.	Bidders are allowed to submit EMD amount through online payment mode only using IREPS Portal. WE request you to please relax this clause and allow bidders with an option to pay EMD amount online or submit Bank Guarantee of equal value.	Online payment of Big amount transaction is a challenge for bidders . Even bidders will face challenge to make such a big amount payment online using internet banking due to banking rules and regulations for such big amount. Submission of BG will also enable more competitive bidding procedure and allow maximum participation.		As per RFP

373	5. Payment Terms	60	5.1 Payment shall be made in Indian Currency (Rs) 75% payment of the value of the supply items would be made on receipt of material by the consignee (at site / the stores) duly inspected and on submission of the following documents subject to any deductions or recovery which RailTel may be entitled to make under the contract: 5.2 15% payment of the value of Supply items of the PO shall be made by RailTel on successfully Installation & Commissioning at site, 5% payment of value of Supply items of the PO on issue of Provisional Acceptance Certificate (PAC) and the last 5% payment of the value of Supply items of the PO shall be made by RailTel on issue of Final Acceptance Certificate (FAC) which will be issued by GM/ITP.	5.1 Payment shall be made in Indian Currency (Rs) 85% payment of the value of the supply items would be made on receipt of material by the consignee (at site / the stores) duly inspected and on submission of the following documents subject to any deductions or recovery which RailTel may be entitled to make under the contract: 5.2 5% payment of the value of Supply items of the PO shall be made by RailTel on successfully Installation & Commissioning at site, 5% payment of value of Supply items of the PO on issue of Provisional Acceptance Certificate (PAC) and the last 5% payment of the value of Supply items of the PO shall be made by RailTel on issue of Final Acceptance Certificate (FAC) which will be issued by GM/ITP.	In such kind bid projects, heavy amount of bidder are engaged in procurement of hardware and software and they need to pay this amount to respective OEMs upfront. If railtel releases maximum amount at the time of delivery, it will encourage bidders for healthy participation.		As per RFP
374	Preference: Make In India	68	21.3: Requirement of Purchase Preference	In procurement of goods in respect of which the Nodal Ministry has communicated that there is sufficient local capacity and local competition, and where the estimated value of procurement is Rs.50 Lakhs or less, only local suppliers shall be eligible. If the estimated value of procurement of such goods is more than Rs.50 Lakhs, the provisions of subparagraph b or c as the case may be, shall apply.	Will Railtel prefer Indian OEM/technology provider for SOR category mentioned in the Tender to encourage Indian OEM	This clause is to be enforced for each category of the SOR .	As per RFP
375	General Functionalities	New	Authenticated for VPNs, firewall for access in MFA	The MFA should be integrated with access integrator for users to access seamlessly. Firewall has VPN connectivity but does not have secure access like restricting the end device for access	Whether the proposed solution can be accessed any time anywhere and can scale up without change of hardware and scale up for VPN as well as VDI. Why Railtel should us multiple systems/device for MFA and VPN access. Reduction in TCO for life cycle management and maximise ROI on security	Proposed solution should be built with access integrator. In case vendor wants to deploy seamless access the same should be offered to see the users access eoffice seamlessly from	As per RFP
376	General Functionalities	New	MFA	The project is for DC Infra for eoffice. Whether the solution is deployed for prevalent eoffice application of NIC	Whether Railtel would like to accept the credibility of The proposed solution to be deployed on eoffice application to evaluate specific eligibility rather than General eligibility criteria	The MFA must have been deployed on eoffice application for at least 1000 users/licenses	As per RFP
377	MFA	47	The proposed solution should support soft token (TOTP) / Hardware Token / Push Notification (SMS) / Email / App Based etc..	he solution should support Biometric authentication solution that can work with 3rd party biometric solution. Biometric should also be considered as one of factor of authentication	Biometric is always an important factor of Multifactor authentication. The solution should support the facility. Biometric devices will be purchased as and when required	MFA must have the facility to support Biometric	Corrigendum-III

378	Scalability	New	MFA	Solution scalability and authentication	The solution should have in built Biometric authentication	The solution should come with built-in biometric authentication server (with additional licenses) in case customer want to use the solution from same OEM.	Clarification: The proposed solution must support Biometric device as and when procured by RailTel.
379	Scalability	New	MFA	Support for different Biometric device	Any MFA solution has Biometric as one of its factor of authentication. Biometric solution can be deployed on the same hardware/software. Solution should be open and should not be vendor lock in	The proposed solution must support Biometric device as and when procured by Railtel. The devices should be not vendor locking	Clarification: The proposed solution must support Biometric device as and when procured by RailTel.
380		New	MFA	Secure authentication	In Cyber Experts Pass words are generally weak and useful data can be leaked from Data Centre which can create damage to the organisation	The solution should allow password less authentication to ensure minimising the leakage, theft, and severity of loss of IT assets	Clarification: "The solution should allow password less authentication to ensure minimising the leakage, theft, and severity of loss of IT assets"
381		New	MFA	Secure authentication	Futuristic MFA without cost impact to Railtel	The solution should support FIDO keys for authentication	As per RFP
382		New	MFA	LDAP support		The solution should be supported on LDAP or local database	Clarification: "The solution should be supported on LDAP or local database."
383	The proposed solution should support soft token (TOTP) / Hardware Token / Push Notification (SMS) / Email / App Based etc..	47	MFA		The proposed solution should support soft token (TOTP) / Hardware Token / Push Notification (SMS) / Email / App Based etc..	The proposed solution should support soft token (TOTP)/Hardware Token/Push Notification /SMS /Email/ App based etc.	Corrigendum-III
384	Solution Access	47			No of Named user to use MFA	Kindly provide the no of Named users who will use MFA to access eoffice from anywhere/home	As per RFP
385	12.2.1	64	The tenderer should have executed Single order showcasing supply, installation, testing, commissioning, implementation and operations projects for Data Center Solutions commercially costing not less than 35% of the tendered value during last proceeding 3 financial years (i.e. current year and three previous financial years) from the date of opening of tender. The bidder shall also furnish Supply / Work completion certificate issued by customer/s for the Purchase Orders/Work Orders.	Please add the below clause: "For MSME / Startup bidders: The tenderer should have executed cumulative orders showcasing supply, installation, testing, commissioning, implementation and operations projects for Data Center Solutions commercially costing not less than 35% of the tendered value during last proceeding 3 financial years (i.e. current year and three previous financial years) from the date of opening of tender. The bidder shall also furnish Supply / Work completion certificate issued by customer/s for the Purchase Orders/ Work Orders.	We request to kindly allow relaxation to Startup & MSME Bidders in Eligibility Criteria for past experience subject to meeting of quality & technical specifications in order to participate in this Tender.		As per RFP
386	Clause 4	77	Delivery and supervision of installation and commissioning within 120 of issue of LOA/PO.	Please add the below clause: Delivery and supervision of installation and commissioning within 150 of issue of LOA/PO.	Please extend the delivery & installation period due to the current unforeseen & unprecedented circumstances (COVID-19).		PQ

387	EMD	2	EMD - 35,68,500/- thru IREPS Portal	We also request you to accept the EMD thru BG / DD as well			Corrigendum-III
388	SOR-B, B-3	5	Software defined Storage, Virtualization Virtual Cloud Foundation& Site Recovery License as per Technical Specification given in chapter-3A	Based on the requirement kindly amend this line for clarity as: "Software defined Storage, Cloud Management Platform, SDN & Site Recovery License as per Technical Specification given in chapter-3A"	Amendment required for more clarity and to avoid any ambiguity		As per RFP
389	Design Considerations	12	Total 200 no. of VMs across DC & DR have been envisaged for overall solution consideration.	Would you run your VMs across both sites – will they be active on both sites, to clarify if we should quote for 200 instances or 400 instances?			Clarification: Total 200 No. of VM including both DC and DR is required, Distribution details will be shared with successful bidder.
390	Scope of Work	14	xi. Bidder needs to provide the network assurance functionality for the existing network environment	We request you to share us the existing network make & models that installed.	This info will give more clarity to propose correct make and model		Refer- Existing Inventory Sheet enclosed in "Annexure-A"
391	4. Scope of Work-xvi.	15	VMware Site Recovery Manager Standard Latest edition (25 VM Pack) or equivalent -6 Nos.	Kindly amend as "VMware Site Recovery Manager Enterprise Latest edition (25 VM Pack) -6 Nos."	Existing setup has Site Recovery Manager Enterprise edition		Corrigendum-III
392	4. Scope of Work-xvi.	15	VMware vSAN 6 or latest Enterprise for 1 Processor or equivalent - 105 Nos.	Kindly amend as "VMware vSAN Advanced 6 or latest for 1 Processor or equivalent - 105 Nos."	Existing setup is with vSAN Advanced.		Corrigendum-III
393	4. Scope of Work-xiii	15	xiii. Bidder needs to integrate the cloud platform with existing LDAP solution in RailTel. xvi. Offered cloud solution version should be latest and bidder needs to perform the migration/upgradation activity of the existing cloud solution to maintain uniformity of entire cloud solution.	Kindly add following clause "VMware cloud management platform is already setup in existing private cloud at RailTel. For VMware solution, scope will be to 1. Prepare new servers being procured as part of this tender and add them as part of existing cloud setup for expansion . 2. Migrate existing NSX-V to NSX-T 3. Integration of cloud portal with Multi factor authentication solution being procured in this tender 4. Implement SSO for cloud management software components for 15 to 20 administrators 5. Replicate cloud management components to DR site "	We understand that for VMware solution all this activities are not be applicable as VMware cloud management platform is already setup and as part of scope new servers being procured as part of this tender needs to be prepared and added in existing cloud setup for expansion.		Clarification: Complete scope of work has been defined considering both scenarios that bidder may propose VMware CMP or may propose entirely new CMP platform . If bidder is proposing VMware CMP than high level SOW to be read as but not limited to " VMware cloud management platform is already setup in existing private cloud at RailTel. For VMware solution, scope will be to 1. Prepare new servers being procured as part of this tender and add them as part of existing cloud setup for expansion . 2. Migrate existing NSX-V to NSX-T 3. Integration of cloud portal with Multi factor authentication solution being procured in this tender 4. Implement SSO for cloud management software components for 15 to 20 administrators. 5. Replicate cloud management components to DR site ". If Bidder propose new CMP platform , then bidder has to perform all the activities as defined in tender."

394	7-iv	17	iv. Integrate Virtualization Manager with Cloud Management Platform (CMP), Software Defined Network (SDN) & Software Defined Storage (SDS). vi. Create Virtual machines for Linux OS or Windows, Virtual machine templates, Virtual machine configured in High Availability mode in cluster, affinity group creation of virtual machines and virtual machine backup configuration (Snapshot and Clone). vii. Configure storage policies to automate provisioning and balancing of storage resources to ensure that each VM gets the specified storage resources and services. viii. Bidder shall perform integration of HCI with the supplied backup solution and should enable integration with VM to perform backup of VM data and configuration files.			Clarification: Complete scope of work has been defined considering both scenarios that bidder may propose VMware CMP or may propose entirely new CMP platform . If bidder is proposing VMware CMP than high level SOW to be read as but not limited to " VMware cloud management platform is already setup in existing private cloud at RailTel. For VMware solution, scope will be to 1. Prepare new servers being procured as part of this tender and add them as part of existing cloud setup for expansion . 2. Migrate existing NSX-V to NSX-T 3. Integration of cloud portal with Multi factor authentication solution being procured in this tender 4. Implement SSO for cloud management software components for 15 to 20 administrators. 5. Replicate cloud management components to DR site ". If Bidder propose new CMP platform , then bidder has to perform all the activities as defined in tender."
395	8	17	"i. Bidder should integrate the CMP fully with the supplied HCI solution i.e., integration with manager of the hypervisor, Software Defined Network, Software Defined Storage, etc." "ii. The bidder should create policy-based controls of cloud resources and should configure Rolebased policy management, administration and enforce role- based policies." "iii. The bidder should create workflow and blueprints for IaaS, PaaS as defined in Functional Requirements" "iv. The bidder shall also create basic & necessary reports for the analysis of resources (CPU, Memory, Storage and Network) utilization and available resources." v. Bidder should configure auto-scaling of resource as per demand "vi. The bidder should configure CMP with, backup software to enable configuration of backup and restore through self- service Dashboard."			Clarification: Complete scope of work has been defined considering both scenarios that bidder may propose VMware CMP or may propose entirely new CMP platform . If bidder is proposing VMware CMP than high level SOW to be read as but not limited to " VMware cloud management platform is already setup in existing private cloud at RailTel. For VMware solution, scope will be to 1. Prepare new servers being procured as part of this tender and add them as part of existing cloud setup for expansion . 2. Migrate existing NSX-V to NSX-T 3. Integration of cloud portal with Multi factor authentication solution being procured in this tender 4. Implement SSO for cloud management software components for 15 to 20 administrators. 5. Replicate cloud management components to DR site ". If Bidder propose new CMP platform , then bidder has to perform all the activities as defined in tender."

396	1 OF SOR-A: Storage – A-1 - Unified Storage system of 600 TB	19	The offered storage should be a true symmetric active-active storage	Request to change this clause as " Offered Storage array should be a active-active dual controllers. Controllers / Engines / VSD should be scalable in nature within the same storage upto minimum 4 without using any technologies like federation, external storage virtualization, external switch connectivity."	As RAILTEL is expanding its cloud solution, and scalability is one of the main tenant of Cloud Architecture, hence Storage infrastruce must have Option of Controller Scalability which will also provide investment protection for RAILTEL in future.		Clarification: Our requirement is to achieve enterprise class storage functionalities wherein host can access all the luns through all the controllers simultaneously. Asymmetric/ALUA, in case of failover might require more storage system resources and a longer response time per I/O.
397	4 OF SOR-A: Storage – A-1 - Unified Storage system of 600 TB	19	The Storage should be scalable to at least 800 SFF/LFF disk drives on the same set of controllers.	Request the clause to be changed to "The Storage should be scalable to at least 1PB usable capacity on the same set of controllers."	We understand scalability is prime importance for RAILTEL and as asked in the RFP Pt. No 2 of SOR A: A-1, we request Railtel to ask for scalability of 1 PB usable capacity within the same set of controllers		Clarification: As per RFP, However bidder may propose higher storage scalable capacity.
398	8 OF SOR-A: Storage – A-1 - Unified Storage system of 600 TB	19	Storage should be equipped with 8*32 Gbps FC ports, 4*10Gbe port for host connectivity. Required SFPs/Optical Module to be populated from day one	No Mention of Backend Bandwidth. Request to change the clause as "Storage should be equipped with 8*32 Gbps FC ports, 4*10Gbe port for host connectivity and equivalent of aggregated backend bandwidth. Required SFPs/Optical Module to be populated from day one"	We understand backend bandwidth must be atleast the same as the frontend bandwidth for a non-blocking architecture. Storage should also be supplied with equivalent of aggregate backend bandwidth so that the ports must work on line speed		As per RFP
399	9 OF SOR-A: Storage – A-1 - Unified Storage system of 600 TB	19	The storage system should have minimum 512GB global cache on the same set of proposed controllers for both reads & writes. Cache memory should be delivered on DRAM, any other device or HDD should not be considered as cache. Cache shall be completely dynamic for read and write operations.	Request to change the clause as "The storage system should have minimum 512GB global cache on the same set of proposed controllers for both reads & writes. The Global Cache should be scalable to 1TB. Cache memory should be delivered on DRAM, any other device or HDD should not be considered as cache. Cache shall be completely dynamic for read and write operations."	We understand scalability is prime importance for RAILTEL, we request Railtel to ask for scalability of 1 TB Global Cache		As per RFP
400	12 OF SOR-A: Storage – A-1 - Unified Storage system of 600 TB	19	Proposed storage system should be supplied with controller based encryption	Request to change the clause as "Proposed storage system should be supplied with Hardware/controller based encryption with FIPS 140-2 Level-2 Compliance."	We understand Data Security is prime for RAILTEL and Data at Rest Encryption is one of the method to secure the data and FIPS-140-2-Level 2 standard ensures this protection without any overhead. To ensure more participation from leading storage OEM's we request RAILTEL to consider this change.		As per RFP
401	17 OF SOR-A: Storage – A-1 - Unified Storage system of 600 TB	19	The proposed storage system should support at least 24000 LUNs or volumes	Request to change the clause as "The proposed storage system should support at least 16000 LUNs or volumes"	Request to reduce the no. of LUN's or volumes. To ensure more participation from leading storage OEM's we request RAILTEL to consider this change.		Corrigendum-III
402	23 OF SOR-A: Storage – A-1 - Unified Storage system of 600 TB	20	Storage should support VMware vStorage API for Array Integration including but not limited to VAAI, VVOL, VASA etc.	We understand VMware integration is important for RAILTEL, hence request you to modify the clause as "Storage should support VMware vStorage API for Array Integration including but not limited to VAAI, VVOL, VASA etc. Storage array VASA provider should be certified by VMware for VVOL - Storage based replication."	RAILTEL is augmenting Cloud Infrastructure and require VMWare VVOL, VASA and VAAI support, hence we request VVOL replication must also be asked for better integration today and into the future.		As per RFP

403	25-I OF SOR-A: Storage – A-1 - Unified Storage system of 600 TB	20	Proposed storage system should support third-party storage virtualization natively or using another headers in High availability from day1. Necessary licenses and hardware on High availability should be supplied from day1.	Request to remove this clause.	This clause is restrictive and will prevent leading storage OEM's to participate in this RFP.		Corrigendum-III
404	26-A OF SOR-A: Storage – A-1 - Unified Storage system of 600 TB	20	The storage should support both Synchronous and Asynchronous Data Replication to remote site and licenses should be supplied from day1.	To make it inline with clause 13, 24 and 25-H, we request you to change the clause as "The storage should support both Synchronous and Asynchronous Data Replication to remote site and licenses should be supplied from day1 for unlimited capacity."	As RAILTEL has asked all Licenses for Entire Capacity, similarly RAILTEL must ask for unlimited capacity license for replication.		As per RFP
405	6 OF SOR-A: Storage – A-1 - Unified Storage system of 600 TB	19	The Storage should support minimum RAID 5, RAID 6 and RAID10 as different applications requires different performance levels	The Storage should support minimum Dual Disk Failure Protection	With advant of SSD's which provide very high performs (IOPS), RAID 10 is not used any more because of Capacity panelty. RAID 5 is also not used as often because Drive Capacities have grown very large and it take time for Drive rebuilds. So RAID 5 with 1 Drive protection may not be good enough. Capacity Panelties on RAID 10 and Risk of Loosing Data on RAID 5 has made OEM's and customer (RAILTEL RFP also asks for the same) to Look at minimun Dual Disk Protection in order to achieve Best Performing and Protective RAID Level.		As per RFP
406	3 OF SOR-A: Storage – A-1 - Unified Storage system of 600 TB	19	The storage should support and be configured with automated data tiering between different drive types namely SSD, SAS, and NL-SAS within the same storage array. The storage should be capable of moving data blocks between these drive types (up and down the tier) depending on the access patterns to ensure optimum storage performance.	Request to remove this point	As the current requirement is for cloud setup where the SLO is managed by the orchestration layer(vMware in this case), the auto-tiering feature when enabled adds an overhead to the solution & may also result in the breach of SLO's.		As per RFP

407	SOR-A: Storage – A-1 - Unified Storage system of 600 TB	New	New Clause SOR-A: Storage – A-1 - Unified Storage system of 600 TB	We request Railtel to consider below clause 1. Offered storage array shall support quality of service for critical applications so that appropriate and required response time can be defined for application logical units at storage. It shall be possible to define different service / response time for different application logical units. 2. Quality of service engine shall allow to define minimum and maximum cap for required IOPS / bandwidth for a given logical units of application running at storage array. 3. It shall be possible to change the quality of service Response time (In both milliseconds as well as Sub-milliseconds), IOPS, bandwidth specification at real time.	As stated in our query mentioned above SLA's & SLO's are most critical requirement in any cloud architecture & hence we request Railtel to consider features like QoS, which will enable Railtel to deliver desired performance levels for various applications & tenants		As per RFP
408	SOR-A: Storage – A-1 - Unified Storage system of 600 TB	New	New Clause SOR-A: Storage – A-1 - Unified Storage system of 600 TB	Offered storage array shall be true multi-tenant and shall support more than 512 Tenant per storage array. Every tenant shall be treated as a separate logical storage array with its own user control access.	Multi-tenancy is basic aspect of any cloud architecure to mainatain data sovereignty & the storage should support the same.		As per RFP
409	1 OF SOR-A-Storage – A-3 – SAN Switch:	22	SAN switch should be supplied with minimum 96 * 32Gbps FC ports and all ports should be active with required license and fully populated modules from day one.	We understand Scalability is prime importance for RAILTEL. So Request that Scalability be asked to atleast 128 Ports	As RAILTEL is expanding its cloud solution, and scalability is one of the main tenant of Cloud Architecture, Hence this Option of Port Scalability must be included which will provide investment protection for RAILTEL in the future.		As per RFP
410	15 OF SOR-A-Storage – A-3 – SAN Switch:	22	Switch should support secure boot to allow only OEM's Genuine software to be loaded on switches.	Request to remove this clause as this language is proprietary to one OEM.	There are only two mainstream SAN Fabric Switch OEM's in the industry. We request to remove this clause, in interest of getting participation from both SAN Switch OEMs.		Corrigendum-III
411	SOR-B- Cloud Solution –B-1- Rack Servers:	23	SAP Certification: Server should be SAP HANA certified	Pls do remove this Clause	As we understand application to be deployed is e-office with Vmware. Hence SAP HANA certification for the server is not applicable in current scenario. We would request railtel to remove this clause to maximise solution from leading OEM offerings		As per RFP
412	SOR-B- Cloud Solution –B-1- Rack Servers:	New	Disk Configuration: 2 nos. of 960GB SATA M.2 in mirrored configuration for OS	Request to change this clause as "2 nos. of Hot swap 960GB SSD SATA M.2/SFF/LFF in mirrored configuration for OS"	M.2 Drives are not Hot Swap and require Downtime for replacement, also only limited Vendor supports Mirrored configuration that too with certain limitations in M.2 drives, So to make it generic, kindly allow M.2/ SFF/LFF drives, M.2 is only the form factor, drive type is SSD only and will not impact any performance to Railtel. Also request to ask Hot swap functionality to avoid any downtime due to drive failure.		Corrigendum-III
413	SOR-B- Cloud Solution –B-1- Rack Servers:	New	Configuration and Management: Zero-touch repository manager and self-updating firmware system using AI/ML.	Request to change this clause as "Configuration and Management: Firmware and driver repository manager and self-updating firmware system using AI/ML."	Please remove OEM specfic term like zero touch.		As per RFP

414	SOR-B- Cloud Solution –B-1- Rack Servers:	24	For server data storage 16x60= 960TB. Additional storage capacity of each server (80-64=16) TB should be arranged in SAN storage for the proposed solution. Each data center needs to be provisioned with 480TB usable capacity using 6TB or less NL-SAS drives on RAID6 in offered storage solution.	Request to remove from Server Configuration and add in the SAN storage, if required.	We could not relate this clause with the offered server configuration. In case this clause required for SAN storage capacity, request to please move to relevant section		Corrigendum-III
415	SOR-B- Cloud Solution –B-1- Rack Servers:	24	New Clause SOR-B- Cloud Solution –B-1- Rack Servers:	To enhance security of Railtel infrastructure, request to add following clause - "1. For firmware security, system should support remote management chip creating a fingerprint/digital signature in the silicon/hardware, preventing servers from booting up unless the firmware matches the fingerprint/digital signature. This feature should be immutable. 2. Server should maintain repository for firmware and should be able to rollback, if required. "	In today's IT era security is utmost priority for every organisation and at the same time organisation wants to have provision for quick recovery if anything goes wrong. It becomes more important for cloud environment where services would be exposed to internet.		As per RFP
416	SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity - 5	24	The switching OEM should be part of latest Gartner's Leader Quadrant for Data Center networking.	Request you to kindly modify the clause as "The switching OEM should be part of latest Gartner's Leader Quadrant for Data Center networking or Wired and wireless network"	We represent a leading company for networking and leader in Gartner Magic Quadrant for wired and wireless network since last 4-5 years. We manufacturers Datacenter Switches as well. Request you to kindly modify so that leading OEM can participate.		Corrigendum-III
417	SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity- 6 (c)	25	Similar no. of 100G SR transceivers should be additional supplied for fabric controller/spine switch for uplink connectivity termination.	Request you to kindly remove this clause.	As this is proprietry requirement, request Railtel to remove this from this tender, and may cause warranty violation in case third party SFP's are installed.		As per RFP
418	SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity- 12	25	Switch should have a minimum 40MB buffer of more.	The switch must have minimum 32MB buffer or more.	Technology and architecture differs from OEM to OEMs. 32 MB Packet buffers size is standard for best practice and sufficient for leaf switch and most of the OEMs supports the same. Request you to kindly modify so that leading OEM can participate.		As per RFP
419	SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity- 13	25	Switch should have smart buffering mechanism to classify long lived versus short lived flows and must have capability to dynamically prioritize short lived flows during congestion to avoid packet drop of mission critical traffic.	Request you to kindly remove this clause.	This clause is OEM specific. Only one OEM can comply to this, hence request you to remove the clause to maximize the participation of all leading OEMs.		Clarification: This is required. Bidder can propose more than 2GB Buffer in a switch alternatively, if this feature is not supported in switch.

420	SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity- 17	25	Switch should support for different logical interface types like loopback, VLAN, SVI/RVI, Port Channel, multi chassis port channel/LAG etc.	Switch should support for different logical interface types like loopback, VLAN, SVI/RVI or equivalent, Port Channel, multi chassis port channel/LAG etc.	Terminology differs from OEM to OEM. RVI is OEM specific and SVI is equivalent to VLAN Interface. Request you to kindly modify so that leading OEM can participate.		As per RFP
421	SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity - 27	26	Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically.	The product to support open standard environment and uplink to the existing leaf & spine architecture over industry standard L2/L3 protocols.	These clauses restrict to other leading OEMs. Our product support openflow open standard protocol which can be integrate and uplink with existing SDN controller and spine switch-leaf architecture over industry standard L2/L3 protocols.		As per RFP
422			Switch should integrate and would be part of Existing Fabric (as a Leaf), so that the Data Center Existing Networking environment can be used seamlessly with following Benefits:				As per RFP
423			policy-driven automation through an integrated underlay and overlay, is hypervisor agnostic, and extends policy automation to any workload — including virtual machines, physical bare-metal servers, and containers.				As per RFP
424			If any integration issue of the Leaf switches in the existing controller and Spine -Leaf architecture, bidder to propose separate Spine switches and SDN controller separately.				Clarification: Complete scope of work has been defined considering both scenarios that bidder may propose VMware CMP or may propose entirely new CMP platform . If bidder is proposing VMware CMP than high level SOW to be read as but not limited to " VMware cloud management platform is already setup in existing private cloud at RailTel. For VMware solution, scope will be to 1. Prepare new servers being procured as part of this tender and add them as part of existing cloud setup for expansion . 2. Migrate existing NSX-V to NSX-T 3. Integration of cloud portal with Multi factor authentication solution being procured in this tender 4. Implement SSO for cloud management software components for 15 to 20 administrators. 5. Replicate cloud management components to DR site ". If Bidder propose new CMP platform , then bidder has to perform all the activities as defined in tender."

425			The proposed solution must be able to analyze real time data about the network which includes any metadata, configurations, policies, device states or protocol states and then run automated checks to identify potential errors, misconfigurations and network misbehaviours.				Clarification: Complete scope of work has been defined considering both scenarios that bidder may propose VMware CMP or may propose entirely new CMP platform . If bidder is proposing VMware CMP than high level SOW to be read as but not limited to " VMware cloud management platform is already setup in existing private cloud at RailTel. For VMware solution, scope will be to 1. Prepare new servers being procured as part of this tender and add them as part of existing cloud setup for expansion . 2. Migrate existing NSX-V to NSX-T 3. Integration of cloud portal with Multi factor authentication solution being procured in this tender 4. Implement SSO for cloud management software components for 15 to 20 administrators. 5. Replicate cloud management components to DR site ". If Bidder propose new CMP platform , then bidder has to perform all the activities as defined in tender."
426			The proposed solution must be able to verify configurations before been committed to be adherent to configuration best practices and if any check/ verification failure occurs then system must notify it to the admin via a suitable mechanism				Clarification: Complete scope of work has been defined considering both scenarios that bidder may propose VMware CMP or may propose entirely new CMP platform . If bidder is proposing VMware CMP than high level SOW to be read as but not limited to " VMware cloud management platform is already setup in existing private cloud at RailTel. For VMware solution, scope will be to 1. Prepare new servers being procured as part of this tender and add them as part of existing cloud setup for expansion . 2. Migrate existing NSX-V to NSX-T 3. Integration of cloud portal with Multi factor authentication solution being procured in this tender 4. Implement SSO for cloud management software components for 15 to 20 administrators. 5. Replicate cloud management components to DR site ". If Bidder propose new CMP platform , then bidder has to perform all the activities as defined in tender."
427	SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity - 32	26	Switch should support 8 Nos. of link or more per Port channel (using LACP) and support 48 port channels or more per switch.	Switch should support 8 Nos. of link or more per Port channel (using LACP) and support 32 port channels or more per switch.	The current clause in the specifications restrict leading OEM's to participate. Hence request you to change the same		As per RFP

428	SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity - 44	27	Switch should support for BFD For Fast Failure Detection as per RFC 5880	Switch should support for BFD For Fast Failure Detection	Our switches supports BFD for Fast Failure Detection, but		Corrigendum-III
429	SOR-B- Cloud Solution –B-3- Software defined Storage, Virtualization Virtual Cloud Foundation & Site Recovery License:	29	SOR-B- Cloud Solution –B-3- Software defined Storage, Virtualization Virtual Cloudm Foundation & Site Recovery License:	Based on the requirement kindly amend this line for clarity as: "Software defined Storage, Cloud Management Platform, SDN & Site Recovery License as per Technical Specification given in chapter-3A"	Amendment required for more clarity and to avoid any ambiguity		As per RFP
430	SOR-B	29	The solution should have capability to automate the bring-up process of the entire software platform, including deployment of infrastructure VMs, creation of the management cluster, configuration of VLANs, virtual storage, virtual network, and cluster creation and provisioning.	We understand that VMware cloud management platform with management cluster is already setup in existing RailTel private cloud. So this clause is not applicable. Kindly confirm.	VMware cloud management platform along with management cluster is already setup in existing RailTel private cloud. So bring-up of software platform, management clstuter, infrastructure VMs is not required		Clarification: Specification given considering the scenario that bidder may propose the extension of VMware CMP or may propose the entire new CMP.
431	SOR-B	29	The solution should provide true multi tenancy, Each tenant needs to be able to create their own profiles/blueprints, share them to a public catalog, and not be able to see other tenant's build profiles, compute resources, or managed machines. At least 3 tenants will be required to be configured during the Cloud deployment.	Kindly amend this as "The solution should provide true multi tenancy, Each tenant needs to be able to create their own profiles/blueprints, share them to a public catalog, and not be able to see other tenant's build profiles, compute resources, or managed machines. At least 3 Business Groups will be required to be configured during the Cloud deployment."	As per our understanding in present setup different departments are onboarded with business groups. More business groups can be created as per requirement of this clause.		As per RFP
432	SOR-B	31	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.	Request to kindly remove this clause	This feature is not part of the components asked at section 4 page 15 point xvi. Also kindly note this feature is not a part of currently running stack in RailTel eoffice project.		As per RFP
433	SOR-B	32	The solution should provide automatic private cloud metering and consumption analysis. The Cloud portal will be configured with Multi factor authentication during the deployment.	VMware Cloud portal already setup for RailTel e-Office will be configured with Multi factor authentication solution being procured as part of this tender. Supported authentication types are listed on this link. Would request that the asked MFA solution should be compatible as per this list. https://docs.vmware.com/en/vRealize-Automation/7.6/com.vmware.vra.prepare.use.doc/GUID-D16CB962-78B9-4FAD-92D5-E16613A381FF.html?hWord=N4lghgNiBcIC4HcD2ACAZmAxnJAnFYArnABYcmAdnAJaZg1IUgC+QA			As per RFP

434	SOR-B	33	There should be single portal to manage all the Cloud based management software using single sign on functionality.	We understand that this functionality is required for RailTel administrators and there would be 15 to 20 such users. Kindly confirm if we can propose the solution for 20 users.			Corrigendum-III
435	SOR-C- Network –C-1 – Leaf Switch - 5	35	The switching OEM should be part of latest Gartner's Leader Quadrant for Data Center networking.	Request you to kindly modify the clause as "The switching OEM should be part of latest Gartner's Leader Quadrant for Data Center networking or Wired and wireless network"	We represent a leading company for networking and leader in Gartner Magic Quadrant for wired and wireless network since last 4-5 years. We manufacturers Datacenter Switches as well. Request you to kindly modify so that leading OEM can participate.		Corrigendum-III
436	SOR-C- Network –C-1 – Leaf Switch- 12	36	Switch should have a minimum 40MB buffer of more.	The switch must have minimum 32MB buffer or more.	Technology and architecture differs from OEM to OEMs. 32 MB Packet buffers size is standard for best practice and sufficient for leaf switch and most of the OEMs are supported. Request you to kindly modify so that leading OEM can participate.		As per RFP
437	SOR-C- Network –C-1 – Leaf Switch- 13	36	Switch should have smart buffering mechanism to classify long lived versus short lived flows and must have capability to dynamically prioritize short lived flows during congestion to avoid packet drop of mission critical traffic.	Request you to kindly remove this clause.	This clause is OEM specific. Only one OEM can comply, request you to kindly remove so that all leading OEM can comply.		Clarification: This is required. Bidder can propose more than 2GB Buffer in a switch alternatively, if this feature is not supported in switch.
438	SOR-C- Network –C-1 – Leaf Switch- 17	36	Switch should support for different logical interface types like loopback, VLAN, SVI/RVI, Port Channel, multi chassis port channel/LAG etc.	Switch should support for different logical interface types like loopback, VLAN, SVI/RVI or equivalent, Port Channel, multi chassis port channel/LAG etc.	Terminology differs from OEM to OEM. RVI is OEM specific and SVI is equivalent to VLAN Interface. Request you to kindly modify so that leading OEM can participate.		As per RFP
439	SOR-C- Network –C-1 – Leaf Switch- 27	36,37	Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically.	The product to support openstandard environment and uplink to the existing leaf & spine architecture over industry standard L2/L3 protocols.	These clauses restrict to other leading OEMs. Our product support openflow open standard protocol which can be integrate and uplink with existing SDN controller and spine switch-leaf architecture over industry standard L2/L3 protocols.		As per RFP
440			Switch should integrate and would be part of Existing Fabric (as a Leaf), so that the Data Center Existing Networking environment can be used seamlessly with following Benefits:				As per RFP
441			policy-driven automation through an integrated underlay and overlay, is hypervisor agnostic, and extends policy automation to any workload — including virtual machines, physical bare-metal servers, and containers.				As per RFP

442			If any integration issue of the Leaf switches in the existing controller and Spine -Leaf architecture, bidder to propose separate Spine switches and SDN controller separately.			Clarification: Complete scope of work has been defined considering both scenarios that bidder may propose VMware CMP or may propose entirely new CMP platform . If bidder is proposing VMware CMP than high level SOW to be read as but not limited to " VMware cloud management platform is already setup in existing private cloud at RailTel. For VMware solution, scope will be to 1. Prepare new servers being procured as part of this tender and add them as part of existing cloud setup for expansion . 2. Migrate existing NSX-V to NSX-T 3. Integration of cloud portal with Multi factor authentication solution being procured in this tender 4. Implement SSO for cloud management software components for 15 to 20 administrators. 5. Replicate cloud management components to DR site ". If Bidder propose new CMP platform , then bidder has to perform all the activities as defined in tender."
443			The proposed solution must be able to analyze real time data about the network which includes any metadata, configurations, policies, device states or protocol states and then run automated checks to identify potential errors, misconfigurations and network misbehaviours.			Clarification: Complete scope of work has been defined considering both scenarios that bidder may propose VMware CMP or may propose entirely new CMP platform . If bidder is proposing VMware CMP than high level SOW to be read as but not limited to " VMware cloud management platform is already setup in existing private cloud at RailTel. For VMware solution, scope will be to 1. Prepare new servers being procured as part of this tender and add them as part of existing cloud setup for expansion . 2. Migrate existing NSX-V to NSX-T 3. Integration of cloud portal with Multi factor authentication solution being procured in this tender 4. Implement SSO for cloud management software components for 15 to 20 administrators. 5. Replicate cloud management components to DR site ". If Bidder propose new CMP platform , then bidder has to perform all the activities as defined in tender."

444			The proposed solution must be able to verify configurations before been committed to be adherent to configuration best practices and if any check/ verification failure occurs then system must notify it to the admin via a suitable mechanism				Clarification: Complete scope of work has been defined considering both scenarios that bidder may propose Vmware CMP or may propose entirely new CMP platform . If bidder is proposing Vmware CMP than high level SOW to be read as but not limited to " VMware cloud management paltform is already setup in existing private cloud at RailTel. For VMware solution, scope will be to 1. Prepare new servers being procured as part of this tender and add them as part of existing cloud setup for expansion . 2. Migrate existing NSX-V to NSX-T 3. Integration of cloud portal with Multi factor authentication solution being procured in this tender 4. Implement SSO for cloud management software components for 15 to 20 administrators. 5. Replicate cloud management components to DR site ". If Bidder propose new CMP platform , then bidder has to perform all the activities as defined in tender."
445	SOR-C- Network –C-1 – Leaf Switch- 32	37	Switch should support 8 Nos. of link or more per Port channel (using LACP) and support 48 port channels or more per switch.	Switch should support 8 Nos. of link or more per Port channel (using LACP) and support 32 port channels or more per switch.	Sizing is specific. Maximum 2 or 4 ports uplink using between spine and leaf. 48 nos is oversizing. 32 ports channel is standard for all leading OEM. Request you to kindly modify so that leading OEM can participate.		As per RFP
446	SOR-C- Network –C-2 –End point protection for end user, Point no. 1	40	The bidder shall propose dedicated end point based solution to protect systems Advanced Targeted Attacks and APT's	As per specification you have asked for protection from Advanced Targeted Attacks/APT's and to achieve holistic protection from known and unknown threats a sandbox solution will be required.	EPP solution does not have compute where they can simulate endpoint environments to detonate objects carrying malicious codes. Hence a sandbox technology will be required which is specifically meant to cater unknown/Zero day attacks by simulating your endpoint environment i.e. OS, browser, MS office versions etc. Hence its a humble submission to incorporate sandbox solution with proposed solution to cater APT attacks. Clause should read as : The bidder shall propose dedicated end point based solution to protect systems from Advanced Targeted Attacks and APT's by integrating with sandbox solution supporting customised images having 60 virtual analyzers.		As per RFP

447	SOR-C- Network –C-2 –End point protection for end user, Point no. 2	40	The proposed solution shall work on a signature-less mechanism to stop threats without relying on a database to be present at the endpoint	Considering current threat landscape which is changing very rapidly and dynamically just relying on single technique is not adequate and will work as a single point of failure	As you have already considered the importance of Gartner in this RFP which itself said in his report that merely relying on single technique can not give you required protection also this is completely violating MoUD, NCIIPC, NIST and Cert-In guidelines. Hence considering defense in depth strategy a proposed endpoint solution should consist combination of both detection as well as prevention techniques to avoid single point of failure. Hence it is requested to incorporate prevention techniques as well instead of merely relying on detection techniques. Clause should read as : The proposed solution shall work on machine learning\signature-less mechanism\Behavior monitoring also use Firewall, Device control, Variant protection, Census check, crypto malware, fileless malware, Portable Executable files control, CVE number visibility, Application/Process control, Virtual patching and Data Exfiltration and MDR capability in a single unified agent to stop threats holistically.		As per RFP
448	SOR-C- Network –C-2 –End point protection for end user, Point no. 5	40	The proposed solution shall utilize layered and defense in depth approach, wherein the solution cannot be of the same make as existing endpoint AV	The proposed solution should co-exist with existing AV that is something you have already required as per point no. 4 of specification, now specifically mention that existing AV vendor can not participate by just giving justification of defense in depth approach is not logical	This point is restrictive in nature and not allowing our participation as EPP does consists multiple features and modules those do not have any dependency on each other and completely adhere defense in depth approach. Hence its a humble submission to dilute this clause to allow our participation also to achieve threat protection holistically. Clause should read as : The proposed solution shall utilize layered and defense in depth approach by incorporating multiple security layers i.e Application/Process control, Virtual patching and Data Exfiltration, Machine learning and Behavior Monitoring and MDR capability in a single unified agent avoiding sinlge point of failure.		Corrigendum-III

449	SOR-C- Network –C-2 –End point protection for end user, Point no. 8	40	Security vendor should have a dedicated research organisation that is focus on vulnerability research and should actively contribute to discoveries of new vulnerabilities exploited in the wild.	As you have understand the criticality and importance of contribution towards undisclosed vulnerabilities those are not even discovered by other infrastructure/security vendors. Public discloser is important to see how much contribution vendor has done in terms of vulnerability discloser also it should be acknowledge by microsoft and Adobe those are being widely used in industry and vendor should be recognised by pioneer threat research institution.	Vendor's contribution towards discloser of undisclosed vulnerability lie in commercially available application/OS is need of the hour and this capability give you proactive shield from sophisticated attacks which can use these open vulnerabilities not discovered by even vendors i.e. Microsoft, Adobe, etc. but how much contribution these vendors are making is something very crucial. Hence its a humble submission that vendor should publish these statistics of thier vulnerability disclosers and same should be acknowledge by other vendors i.e. Microsoft, Adobe, etc. also vendor should got recognised by Forrester who is leader in vulnerability research. Clause should read as : Security vendor should have a dedicated research organisation/vertical that is focus on vulnerability research and should actively contribute to discover undisclosed vulnerabilities and vendor should be in leader quadrant as per Forrester Wave Endpoint Security 2019 report.		As per RFP
450	SOR-C- Network –C-2 –End point protection for end user, Point no. 9	40	Software footprint should be small <50MB and should support interactive and/or silent install. Total of 39000 Licenses should be factored for this End Points from Day- 1. Proposed solution should support 100,000 concurrent end points from day-1 by purchasing additional Lic in future.	Defining any limit on endpoint footprint will going to restrict participation as every OEM is having its own architecture to deliver higher performance with security effectiveness	This point is restrictive in nature and not allowing our participation as every OEM is having its own architecture and methodology to deliver required security effectiveness along with higher performance without impacting user experience. Hence instead of defining limit on endpoint footprint specification should be focus on bringing required security effectiveness with higher performance. Hence its a humble submission to dilute this to allow our participation. Clause should read as : Software footprint should be small and support interactive and/or silent install. Total of 39000 Licenses should be factored for this End Points from Day- 1. Proposed solution should support 100,000 concurrent end points from day-1 by purchasing additional Lic in future.		Corrigendum-III
451	SOR-C- Network –C-2 –End point protection for end user, Point no. 26	41	The solution shall be capable of working in Windows, Windows Server & Linux operating systems	Are you using Linux OS at your endpoint (Laptop/Desktop) machines ? as EDR capability at endpoints running on Linux platform will provide very limited feature which will completely not going to server the purpose.	This point is restrictive in nature and not allowing our participation. Hence its a humble submission to dilute this to allow our participation. Clause should read as : The solution shall be capable of working in Windows, Windows Server & Mac systems		Corrigendum-III

452	SOR-C- Network –C-2 –End point protection for end user, Point no. 27	41	The endpoint solution shall be able to pinpoint vulnerable versions of popular applications installed in Endpoints	A proposed solution should have capability to prevent installation of any malicious application/process in your endpoint environment and by merely "pinpoint" vulnerable application will not going to server the purpose.	Proposed solution should be capable to blocking any malicious application initiating any illegitimate process which can work as a platform to host and perform malicious activities in network. Hence its a humble submission to dilute this clause and consider our recommendations. Clause should read as : The endpoint solution shall be able to block malicious applications/process to installed in Endpoints		Corrigendum-III
453	SOR-C- Network –C-2 –End point protection for end user, Point no. 29	41	The proposed solution should not be dependent on a network sandbox for its detection as it takes up bandwidth and affects productivity and shall provide the option of choosing which files to be submitted for sandboxing, to administrator	Most of the APT vendors are using Sandbox solution in offline mode which will not impose any latency on user experience and complete process is automate in nature. As you have already asked for mitigating Advanced Targeted Attacks and APT's based attack a sandbox solution is required.	APT solution placement is crucial for delivering security effectiveness along with higher performance without impacting user experience and it also depend on the vendor's approach and architecture as well. Most APT vendor sit in offline mode and inspect malicious object passively to give their verdict of unknow threat which do not impact network performance.Hence its a humble submission to incorporate sandbox solution which should tightly integrate with proposed solution and sit in offline mode. Clause should read as : The proposed solution should have network sandbox solution having 60 customised sandbox images (Windows XP, Win7, Win8/8.1, Win 10, Windows Server 2003, 2008, 2012) simulating endpoint environment for its detection of Advanced Targeted Attacks and should natively integrate with proposed solution with complete automation of file sharing.		Clarification: Proposed EDR solution should have its own Sandboxing feature and should not be dependent on any Network level Sandbox.
454	SOR-C- Network –C-2 –End point protection for end user, Point no. 32	41	Solution should allow Users to choose to preview the new Policy UI.	This clause is restrictive and not allowing our participation and moreove why user interaction is required ?	This clause is restrictive and not allowing our participation as favoring particular OEM.Hence its a humble submission to delete this clause. Clause should read as : Solution should have both web based as well local management console for administrator policy and investigation purpose.		Corrigendum-III
455	SOR-C- Network –C-2 –End point protection for end user, Point no. 32	New	Suggestion	Suggestion	As you have already considered the importance and recognition of Gartner for other components in this RFP. Hence it's a humble request you to consider Gartner recognition for proposed Endpoint protection solution as well which will allow participation of best in the breed solution providers and bring required security effectiveness. Clause should read as : The proposed solution should be positioned in the leader quadrant from last three published Gartner Magic quadrant report for Endpoint Protection		As per RFP

456	SOR - D	41	SOR –D Licenses for OS, DB and NMS/EMS:	All the Software needs to be Perpetual	The Global Policy of EDB is to provide support to PostgreSQL through support subscriptions, which essentially means a period during which the user can avail Technical Support and use EDB developed Tools during the period after paying the fees.. EDB does not sell or charge any license fee for Postgers Licenses instead EDB sells support subscriptions .		Corrigendum-III
457		New		EDB PostGre SQL support system for DB servers - 860 Nos	The Unit of Measure (UOM) for EDB to provide support subscriptions is on the Number of Cores that resides in Database server. Please treat 860 Nos as 860 No of Cores		Corrigendum-III
458		New		Request to add this point : The support (AMC) after 3 years of initial buy of support subscription of 3 years will be at a minimum of 100% fees charged towards the initial buy and needs to be discussed at the Renewal time (after first 3 years of support)			As per RFP
459	Solution Requirement: Monitoring : 29	43	All thresholds should have set point, reset point, polarity, set point message and reset point message for ease of use.	Removal of the clause	Pls give the use case of each type of threshold, which will be applicable in Railtel landscape.		Clarification: System should have multiple customised thresholds configuration as per user requirement.
460	Solution Requirement: Monitoring : 46	44	Provide correlation report between all major network devices to determine if there is any degradation in these devices	Pls rephrase as: "Provide correlation views between all major network devices to determine if there is any degradation in these devices "	The infrastructure correlation depends on inbuilt product algorithm & displayed for real-time views and analysis. The reports are based on the histoical data of the SLA parameters, which helps to ensure the uptime of the DC components, hence please modify the clause.		As per RFP
461	Solution Requirement: Monitoring : 52	44	Show the status of the connections based on the dependent connections and the utilization of the links by displaying connection with different width	Pls rephrase as: "Show the status of the connections based on the dependent connections and the utilization of the links by displaying connection with different color/width "	The product interface display of the software differs from OEM to OEM and relies on the product architecture & the various utilities. Thus, the clause to restrict the software to display in a certain fashion must be replaced.		As per RFP
462	Solution Requirement: Monitoring : 55	44	Collect & display syslog's from network devices & servers and Group syslog's based on severity (Critical, Emergency, Major)	Pls rephrase as: "Collect & monitor syslog's from network devices and Group syslog's based on severity (Critical, Emergency, Major) "	Syslog is a way for network devices to send event messages to a logging server – i.e Syslog server. The Syslog protocol is supported by a wide range of devices, hence this protocol will help to configure devices for real-time change detection via syslog .		Clarification: Syslog server should be integrated in the offered EMS solution.
463	Solution Requirement: Monitoring : 57	44	System licensing should be based only on Physical Hosts and not charge separately for individual guest VMs running on VM Hosts	Removal of the clause	The licensing of the software differs from OEM to OEM and relies on the product architecture & nomenclature. Thus, the clause to fix on the system licensing must be removed and the software must be sized based on the solution envisaged by the bidder for the project tenure.		As per RFP
464		New		EMS/NMS OEM must be an industry standard, enterprise grade solution and shall be in the present in Gartner's Magic Quadrant reports for Network Performance & Monitoring Diagnostics (NPMD) for last two years (2018 & 2019). Pls confirm if the understanding is correct.	Solution having been analysed & recognized by leading analysts ensures that an industry standard solution is being proposed. This is important because as NMS/EMS is the only solution that gives visibility into the project and is responsible for SLA measurements and audits, and therefore all the stakeholders must agree to the reports been generated from NMS/EMS. This warrants an industry-standard solution.		As per RFP

465		New		The propose solution should have diagnostic analytics capability that able to visually correlate performance and configuration changes of all network issues. Pls confirm if the understanding is correct.	The operators will be able to quickly recognize network configuration changes that negatively impact performance and can open a pop-up window to view the differences in the impacting configuration change directly on the change-correlated performance views.		As per RFP
466		New		The proposed NMS should provide out of the box Risk Visibility Dashboards of network infrastructure. Pls confirm if the understanding is correct.	With this risk visibility dashboard, we see the most offending devices in the group along with the the percentage of non-compliant devices.		As per RFP
467	12.2.2	64	The tenderer should have executed Single order showcasing supply, installation, testing, commissioning, implementation and operations projects for Data Center solutions commercially costing not less than 35% of the tendered value during last preceding 3 financial years (i.e. current year and three previous financial years) from the date of opening of tender. The bidder shall also furnish Supply/ work completion certificate issued by customer/s for the Purchase Orders/ Work Orders	we request to amend as : The tenderer should have executed showcasing supply, installation, testing, commissioning, implementation and operations projects for Data Center solutions commercially costing not less than 35% (in Single or in two orders) of the tendered value during last preceding 3 financial years (i.e. current year and three previous financial years) from the date of opening of tender. The bidder shall also furnish Supply/ work completion certificate issued by customer/s for the Purchase Orders/ Work Orders Copy of work orders supported with relevant documentary evidences for the same and the completion certificates issued by customer/s for the Purchase Orders/ Work Orders. Documentary evidence should clearly indicate the nature of systems implemented for each project. or reduce the previous order value from 35% to 25%.	The Amendment will help more no of Partipation and Railtel will get more no of Bids and Railtel would have the commercial benfit by having more no of participations.		As per RFP
468	Preference: Make In India	68	21.3: Requirement of Purchase Preference	In procurement of goods in respect of which the Nodal Ministry has communicated that there is sufficient local capacity and local competition, and where the estimated value of procurement is Rs.50 Lakhs or less, only local suppliers shall be eligible. If the estimated value of procurement of such goods is more than Rs.50 Lakhs, the provisions of subparagraph b or c as the case may be, shall apply.	Will Railtel prefer Indian OEM/technology provider for SOR category mentioned in the Tender to encourage Indian OEM	This clause is to be enforced for each category of the SOR .	As per RFP

469	General Functionalities	New	Authenticated for VPNs, firewall for access in MFA	The MFA should be integrated with access integrator for users to access seamlessly. Firewall has VPN connectivity but does not have secure access like restricting the end device for access	whether the proposed solution can be accessed any time anywhere and can scale up without change of hardware and scale up for VPN as well as VDI. Why Railtel should us multiple systems/device for MFA and VPN access. Reduction in TCO for life cycle management and maximise ROI on security	Proposed solution should be built with access integrator. In case vendor wants to deploy seamless access the same should be offered to see the users access eoffice seamlessly from home. Access and MFA on a single hardware will be preferred. The access solution to be integrated with MFA working on deployed eoffice solution should be provided	As per RFP
470	General Functionalities	New	MFA	The project is for DC Infra for eoffice. Whether the solution is deployed for prevalent eoffice application of NIC	Whether Railtel would like to accept the credibility of The proposed solution to be deployed on eoffice application to evaluate specific eligibility rather than General eligibility criteria	The MFA must have been deployed on eoffice application for at least 1000 users/licenses	As per RFP
471	MFA	47	The proposed solution should support soft token (TOTP) / Hardware Token / Push Notification (SMS) / Email / App Based etc..	he solution should support Biometric authentication solution that can work with 3rd party biometric solution. Biometric should also be considered as one of factor of authentication	Biometric is always an important factor of Multifactor authentication. The solution should support the facility. Biometric devices will be purchased as and when required	MFA must have the facility to support Biometric	Corrigendum-III
472	Scalability	New	MFA	Solution scalability and authentication	The solution should have in built Biometric authentication	The solution should come with built-in biometric authentication server (with additional licenses) in case customer want to use the solution from same OEM.	Clarification: The proposed solution must support Biometric device as and when procured by RailTel.
473	Scalability	New	MFA	Support for different Biometric device	Any MFA solution has Biometric as one of its factor of authentication. Biometric solution can be deployed on the same hardware/software. Solution should be open and should not be vendor lock in	The proposed solution must support Biometric device as and when procured by Railtel. The devices should be not vendor locking	Clarification: The proposed solution must support Biometric device as and when procured by RailTel.
474		New	MFA	Secure authentication	In Cyber Experts Pass words are generally weak and useful data can be leaked from Data Centre which can create damage to the organisation	The solution should allow password less authentication to ensure minimising the leakage, theft, and severity of loss of IT assets	Clarification: "The solution should allow password less authentication to ensure minimising the leakage, theft, and severity of loss of IT assets"
475		New	MFA	Secure authentication	Futuristic MFA without cost impact to Railtel	The solution should support FIDO keys for authentication	As per RFP
476		New	MFA	LDAP support		The solution should be supported on LDAP or local database	Clarification: "The solution should be supported on LDAP or local database."
477	The proposed solution should support soft token (TOTP) / Hardware Token / Push Notification (SMS) / Email / App Based etc..	47	MFA		The proposed solution should support soft token (TOTP) / Hardware Token / Push Notification (SMS) / Email / App Based etc..	The proposed solution should support soft token (TOTP)/Hardware Token/Push Notification /SMS /Email/ App based etc.	Corrigendum-III

478	Solution Access	New			No of Named user to use MFA	Kindly provide the no of Named users who will use MFA to access eoffice from anywhere/home	As per RFP
479	SCHEDULE OF REQUIREMENT	5	Backup Solution at DC and DR along with Tape/Disk Based storage as per specification given in Chapter-3A	Kindly update this point to " Backup Solution at DC and DR along with Virutal Tape Library /Disk Based storage as per specification given in Chapter-3A"	There is no technology comparison between Tape and Disk based Backup solution since there is a huge gap in terms of performance and commericals between Tape and Disk based storage. Request to update this to Modify to Virtual Tape library (VTL) since VTL is based on Disk based technology.		Corrigendum-III
480	3. Design Considerations	13	Veeam is the existing incumbent in the Backup Space. It would be recommended to have Backup Solution co-exist with incumbent solution and enhance the backup capacity. However bidder may propose any other backup solution which needs to be integrated with existing backup solution i.e. Veeam Backup Solution or propose entirely a new backup solution comprising existing and proposed solution capacity.	Request to kindly share the details of existing Backup solution.	Since bidder is allowed to quote entirely new Backup solution if incumbent backup vendor is not quoted. Request to share details liks: Total existing VM's, Host Servers, backed up storage, type of storage media etc.		As per RFP
481	3. Design Considerations	13	Total 50 nodes each at DC & DR have been envisaged for connectivity with proposed SAN Switch.	We understand a total of 60 servers are required as per New requirement across DC & DR. In the above specifications it's mentioned that SAN connectivity for existing Servers is separate and under Railtel scope. Request to clarify on Nodes count and their connectivity.	Clarification requested on the port distribution of SAN switch with total server		Clarification: Existing Nodes may also be connected with SAN switch which bidder has to implement, however any additional hardware requirement in existing server shall be arranged by RailTel.
482	SOR-A-Storage – A-3 – SAN Switch:	22	Proposed switch should be NVMe ready to allow seamless transition to related workloads without any SAN switch upgrade.	Request to remove this point	Not all SAN switches support NVMe support capability. Request to remove this point for wider participation.		Corrigendum-III
483	SOR-A-Storage – A-4 – HBA Card	22	Should have compatibility with existing servers of RailTel	We understand Railtel currently has mix of Server vendors in their Datacenter. Request to kindly confirm if additional HBA cards asked in SOR are to be provided for new quoted servers or for existing servers. If these cards are required for existing servers, request to confirm Server Make & Model since we understand Railtel currently has mix of server OEM's.	Clarification requested on HBA cards asked in SOR		Refer- Existing Inventory Sheet enclosed in "Annexure-A", HBA Card provided must be fully populated from Day-1.
484	SOR-B- Cloud Solution –B-1- Rack Servers:	23	Server Vendor should be under Gartner leaders Magic quadrant in last available report.	Kindly update this point to " Server Vendor should be under Gartner leaders Magic quadrant in 2016 report".	Gartner has last published Server report in 2016. Is this report still valid for Railtel Requirement. Request to kindly confirm.		Clarification: Yes, in case Gartner latest reports are not available for any requiried Hardware & Software, its last available report to be considered.

485	SOR-B- Cloud Solution –B-1- Rack Servers:	23	The management tool should be able to provide global resource pooling and policy management to enable policy based automation.	Kindly update this point to "The management tool should be able to provide Global resource pooling/Management and policy management to enable policy based automation."	We understand by pooling it is not that server resources to be pooled centrally both at DC & DR, we understand that proposed servers should be able for central Management & Monitoring. Request to confirm our understanding.		As per RFP
486	SOR-B- Cloud Solution –B-1- Rack Servers:	24	For server data storage 16x60= 960TB. Additional storage capacity of each server (80-64=16) TB should be arranged in SAN storage for the proposed solution. Each data center needs to be provisioned with 480TB usable capacity using 6TB or less NL-SAS drives on RAID6 in offered storage solution.	Specs for central storage asks for 600TB storage capacity . Request to kindly confirm if Railtel is asking bidders to include additional 480TB storage capacity in the Storage array both at DC & DR on NL-SAS drives.	Clarification requested for Storage		Corrigendum-III
487	Monitoring and Management of DC/HCI Infrastructure:	45	The analytics platform should be able to capture and analyze flow and process telemetry from all workloads across all DC's and Cloud environments in near real time	Request to confirm if Railtel wishes to seamlessly integrate new VM's with existing Application visibility solution or entire new solution is required for existing & new Infrastructure. If yes, request to kindly share the virtual machine & Host counts w.r.t existing Setup both at DC and DR.	Clarification requested		Clarification: Bidder may propose the extension to existing Solution to leveraged or propose the entirely a new solution . Bidder needs to provide the solution which must provide single console for its Management.For the solution design kindly refer the existing inventory details.
488	General Requirement in Multifactor Authentication	46	The proposed solution should be able to provide multifactor authentication for Windows, Mac, Linux Operating systems & Database etc.	Kindly share more information on what type of Database application are being considered and whether do they support RADIUS or SAML 2.0?	Clarification requested		Clarification: Applications supports Radius and SAML.
489	General Requirement in Multifactor Authentication	46	The proposed solution be able to provide multifactor authentication for VPNs, Firewall, Network Switch's, Router, Wireless controllers and web proxy	Kindly share details on type of WLC & Web Proxy solution is being used	Clarification requested		Clarification: WLC is Cisco and Rackus.
490	General Requirement in Multifactor Authentication	47	The proposed solution should provide multifactor authentication for in-house developed application	Kindly share Details on application languages which needs to be integrated and what is the supported authentication protocol is it Radius or Saml 2.0?	Clarification requested		Clarification: Applications supports Radius and SAML.
491	General Requirement in Multifactor Authentication	47	The proposed solution should provide multifactor authentication for virtualization platform (HCI)	Kindly share details on what is the functionality needed here?	As MFA typically integrated with VDI and offers MFA for user login. Need more details on functional ask here.		Clarification: MFA solution should be able to integrate with applications VMware Horizon/View, MS Server, ADFS etc.
492	General Requirement in Multifactor Authentication	47	The proposed solution should be able to be deployed in virtual environments such as VMware, LPAR or Hyper-V	Please relax this point by replacing 'Any component of the proposed solution should be deployed on an Windows or Linux VM running on VMWare, Hyper-V or LPAR hypervisor'	As not all OEMs have components that get deployed on bare metal virtual machines.		Corrigendum-III

493	General Requirement in Multifactor Authentication	48	The Authentication Mechanism should provide capabilities to prevent Brute Force Attacks and should be able to send alerts to the Admin/Helpdesk in case of a brute force attack on a user account.	Please remove this point. As primary credentials are not stored in MFA solution and Brute Force attack usually happens on user's primary authentication. So not a valid ask.	As in the RFP the ask is to not store the user credentials thus there is no chance that Brute Force Attack can be done as this happens on the primary credential source.		Corrigendum-III
494	Integration in Multifactor Authentication	48	Integration with PIM (Privilege identity management) solution	Kindly provide clarification on which PIM solution needs to be integrated	Clarification requested		Clarification: Solution should provide an interface or method to integrate over Radius, SAML or API.
495	Clause 10, SOR-C_Network-C-2-End Point Protection for End User	40	Endpoint software should be easy to deploy and support (not limited to) deployment through 3rd party systems management tools	Please change as "Endpoint software should be easy to deploy and support (not limited to) deployment through 3rd party systems management tools or by publishing the URL	This is to ensure that multiple deployment options are available for agent roll out		As per RFP
496	Clause 26 SOR-C_Network-C-2-End Point Protection for End User	41	The solution shall be capable of working in Windows, Windows Server & Linux operating systems	The solution shall be capable of working in Windows, Windows Server, MacOS, Linux operating systems	As Mac is also widely used in todays network. Having a MAC support will ensure that a solution supports a larger end user operating environment.		Corrigendum-III
497	Clause 2, solution building block	12	vii Core router for DC & DR	This item mentioned in this clause is not found SOR line item. Kindly clarify whether any such requirement is there for Router at DC & DR and what is the quantity	Clarification requested		Corrigendum-III
498	Clause 3: Solution Building Block	12	vi. Total 200 no. of VMs across DC & DR have been envisaged for overall solution consideration	Kindly clarify that the requirement of VM to be captured are 100 VM in DC and 100 VM in DR	Clarification requested		Clarification: Total 200 No. of VM including both DC and DR is required, Distribution details will be shared with successful bidder.
499	Clause 6 a: Leaf Switch	25,35	48 x 1G/10G/25G Multi Mode Fiber Interface populated with 48*10G multi mode interfaces.	Kindly clarify port speed requirement is 1/10/25 Gbps and port to be populated with 10G Multimode SFP	Clarification requested		Clarification: Yes all 48 ports to be equipped with 10G short reach multimode SFP+
500	Clause 28: Leaf Switch	26,37	Spanning Tree Protocol (IEEE 801.D, 802.1W, 802.1S)	Software defin networking is done by creating VxLAN Fabric with Layer 3 protocols. Kindly clarify "Spanning tree protocol" speccified here are related to connecting Layer 2 switches running Spanning tree protocol.	Clarification requested		As per RFP
501	Clause 56: Leaf Switch	27,38	Switch should support to prevent edge devices in the network not administrator's controlled from becoming Spanning Tree Protocol root nodes	Software defin networking is done by creating VxLAN Fabric with Layer 3 protocols. Kindly clarify "Spanning tree protocol" speccified here are related to connecting Layer 2 switches running Spanning tree protocol.	Clarification requested		As per RFP
502	License	46	All licenses should be quoted for total 200 Virtual Machines/ Instances across DC & DR.	Kindly clarify that the requirement of VM to be captured are 100 VM in DC and 100 VM in DR	Clarification requested		Clarification: Distribution details will be shared with successful bidder.
503	SOR-B, B-3	5	Software defined Storage, Virtualization Virtual Cloud Foundation& Site Recovery License as per Technical Specification given in chapter-3A	Based on the requirement kindly amend this line for clarity as: "Software defined Storage, Cloud Management Platform, SDN & Site Recovery License as per Technical Specification given in chapter-3A"	Amendment required for more clarity and to avoid any ambiguity		As per RFP

504	SOR-B- Cloud Solution –B-3- Software defined Storage, Virtualization Virtual Cloud Foundation & Site Recovery License:	29	SOR-B- Cloud Solution –B-3- Software defined Storage, Virtualization Virtual Cloud Foundation & Site Recovery License:	Based on the requirement kindly amend this line for clarity as: "Software defined Storage, Cloud Management Platform, SDN & Site Recovery License as per Technical Specification given in chapter-3A"	Amendment required for more clarity and to avoid any ambiguity		As per RFP
505	4. Scope of Work-xiii	15	xiii. Bidder needs to integrate the cloud platform with existing LDAP solution in RailTel. xvi. Offered cloud solution version should be latest and bidder needs to perform the migration/upgradation activity of the existing cloud solution to maintain uniformity of entire cloud solution.	Kindly add following clause "VMware cloud management paltform is already setup in existing private cloud at RailTel. For VMware solution, scope will be to 1. Prepare new servers being procured as part of this tender and add them as part of existing cloud setup for expansion . 2. Migrate existing NSX-V to NSX-T 3. Integration of cloud portal with Multi factor authentication solution being procured in this tender 4. Implement SSO for cloud management software components for 15 to 20 administrators 5. Replicate cloud management components to DR site "	We understand that for VMware solution all this activities are not be applicable as VMware cloud management paltform is already setup and as part of scope new servers being procured as part of this tender needs to be prepared and added in existing cloud setup for expansion.		Clarification: Complete scope of work has been defined considering both scenarios that bidder may propose VMware CMP or may propose entirely new CMP platform . If bidder is proposing VMware CMP than high level SOW to be read as but not limited to " VMware cloud management paltform is already setup in existing private cloud at RailTel. For VMware solution, scope will be to 1. Prepare new servers being procured as part of this tender and add them as part of existing cloud setup for expansion . 2. Migrate existing NSX-V to NSX-T 3. Integration of cloud portal with Multi factor authentication solution being procured in this tender 4. Implement SSO for cloud management software components for 15 to 20 administrators. 5. Replicate cloud management components to DR site ". If Bidder propose new CMP platform , then bidder has to perform all the activities as defined in tender."
506	7-iv	17	iv. Integrate Virtualization Manager with Cloud Management Platform (CMP), Software Defined Network (SDN) & Software Defined Storage (SDS). vi. Create Virtual machines for Linux OS or Windows, Virtual machine templates, Virtual machine configured in High Availability mode in cluster, affinity group creation of virtual machines and virtual machine backup configuration (Snapshot and Clone). vii. Configure storage policies to automate provisioning and balancing of storage resources to ensure that each VM gets the specified storage resources and services. viii. Bidder shall perform integration of HCI with the supplied backup solution and should enable integration with VM to perform backup of VM data and configuration files.				

507	8	17	"i. Bidder should integrate the CMP fully with the supplied HCI solution i.e., integration with manager of the hypervisor, Software Defined Network, Software Defined Storage, etc." "ii. The bidder should create policy-based controls of cloud resources and should configure Rolebased policy management, administration and enforce role- based policies." "iii. The bidder should create workflow and blueprints for IaaS, PaaS as defined in Functional Requirements" "iv. The bidder shall also create basic & necessary reports for the analysis of resources (CPU, Memory, Storage and Network) utilization and available resources." v. Bidder should configure auto-scaling of resource as per demand "vi. The bidder should configure CMP with, backup software to enable configuration of backup and restore through self- service Dashboard."				
508	SOR-B	29	The solution should have capability to automate the bring-up process of the entire software platform, including deployment of infrastructure VMs, creation of the management cluster, configuration of VLANs, virtual storage, virtual network, and cluster creation and provisioning.	We understand that VMware cloud management platform with management cluster is already setup in existing RailTel private cloud. So this clause is not applicable. Kindly confirm.	VMware cloud management platform along with management cluster is already setup in existing RailTel private cloud. So bring-up of software platform, management cluster, infrastructure VMs is not required		Clarification: Specification given considering the scenario that bidder may propose the extension of VMware CMP or may propose the entire new CMP.
509	SOR-B	29	The solution should provide true multi tenancy, Each tenant needs to be able to create their own profiles/blueprints, share them to a public catalog, and not be able to see other tenant's build profiles, compute resources, or managed machines. At least 3 tenants will be required to be configured during the Cloud deployment.	Kindly amend this as "The solution should provide true multi tenancy, Each tenant needs to be able to create their own profiles/blueprints, share them to a public catalog, and not be able to see other tenant's build profiles, compute resources, or managed machines. At least 3 Business Groups will be required to be configured during the Cloud deployment."	As per our understanding in present setup different departments are onboarded with business groups. More business groups can be created as per requirement of this clause.		As per RFP
510	SOR-B	31	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.	Request to kindly remove this clause	This feature is not part of the components asked at section 4 page 15 point xvi. Also kindly note this feature is not a part of currently running stack in RailTel eoffice project.		As per RFP

511	SOR –D Licenses for OS, DB and NMS/EMS	41	EDB PostGre SQL support system for DB servers - 860 Nos.	Kindly mention the segregation for cores for active, passive, DR, reporting instances	Clarification required		Corrigendum-III
512	4. Scope of Work-xvi.	15	VMware Site Recovery Manager Standard Latest edition (25 VM Pack) or equivalent -6 Nos.	Kindly amend as "VMware Site Recovery Manager Enterprise Latest edition (25 VM Pack) -6 Nos."	Existing setup has Site Recovery Manager Enterprise edition		Corrigendum-III
513	4. Scope of Work-xvi.	15	VMware vSAN 6 or latest Enterprise for 1 Processor or equivalent - 105 Nos.	Kindly amend as "VMware vSAN Advanced 6 or latest for 1 Processor or equivalent - 105 Nos."	Existing setup is with vSAN Advanced.		Corrigendum-III
514	SOR-B	33	There should be single portal to manage all the Cloud based management software using single sign on functionality.	We understand that this functionality is required for RailTel administrators and there would be 15 to 20 such users. Kindly confirm if we can propose the solution for 20 users.			Corrigendum-III
515	3.5	60	For AMC he will be paid @ 3.5% per annum only. If the Tenderer quotes a higher base rate for AMC, he will be paid at his quoted rate per annum and five-year differential cost shall be added to offered cost. AMC would have to be valid for minimum period of 5 years after the warranty.	1) Kindly remove this clause, as a Software OEM, we do not offer AMC for our Software licences at this rate per annum. This is not the Industry standard for AMC for Software. 2) Also please advise if the total Comprehensive Support period is 5 years (Warranty period to be taken as per Page 77, Clause 2)	In this clause it is mentioned 5 years after the warranty period.		As per RFP
516	Chapter 3C, point 3	57	Equipment shall conform to the similar housing standards and shall preferably be integrated in one 19"/21" rack.		Kindly clarify, Is there any additional requirement of Rack or it will be provided by Railtel.		As per RFP
517		New	General		Kindly share the detail of the existing infra product and licenses.		Refer- Existing Inventory Sheet enclosed in "Annexure-A"
518	SOW, point (xvi)	15	VMware vCloud Suite Latest edition or equivalent -114 Nos. VMware NSX Data Center (NSX-T) Advanced per Processor or equivalent- 114 Nos. VMware vSAN 6 or latest Enterprise for 1 Processor or equivalent - 105 Nos. VMware Site Recovery Manager Standard Latest edition (25 VM Pack) or equivalent -6 Nos.	VMware vCloud Suite Latest edition or equivalent -120 Nos. VMware NSX Data Center (NSX-T) Advanced per Processor or equivalent- 120 Nos. VMware vSAN 6 or latest Enterprise for 1 Processor or equivalent - 120 Nos. VMware Site Recovery Manager Standard Latest edition (25 VM Pack) or equivalent -8 Nos.	Kindly clarify, The Vmware stack licenses.		As per RFP
519	Chapter 3A, point 3	12	i. Primary and backup network connectivity between the DC and DR will be provided by the client. ii. Required replication link between DC and DR will be provided by client. iii. Required prerequisites in network links at the time of failover will be provided by client.		We assumed these point comes under the Railtel scope. Please confirm.		As per RFP

520	Chapter 3A, point 3	13	Total 50 nodes each at DC & DR have been envisaged for connectivity with proposed SAN Switch.		Please clarify the vSAN redy node requirement as in SOR the quantity mentioned is 60.		Clarification: Existing Nodes may also be connected with SAN switch which bidder has to implement, however any additional hardware requirement in existing server shall be arranged by RailTel.
521		New		General	Kindly clarify, Is there any requirement of licenses like OS, database across the DR site other than the DC licenses requirement.		As per RFP
522	SOR-D	41	Licenses for OS, DB and NMS/EMS:	We understand from other sections that RailTel requires 24x7 support for all systems. Please confirm same is also applicable for licenses listed under SOR-D	This clarification would help SI/OEM to propose the right product SKU		As per RFP
523	SOR-D	41	Microsoft Windows Server Standard 2019 R2 subscription license 24 core – 10 Nos. MS - SQLSvrStdCore 2017 SNGL MVL 2Lic CoreLic 2 Core Licenses- 10 Nos.		* Windows server License description needs to be corrected from Microsoft Windows Server Standard 2019 R2 subscription license 24 core – 10 Nos to Microsoft Windows Server 2019 Datacenter license per 2 core – 120 Nos. * SQL Server license description needs to be corrected from MS-SQLSvrStdCore 2017 SNGL MVL 2Lic CoreLic 2 Core Licenses- 10 Nos. to Microsoft SQL Server 2019 Standard license per 2 core – 10 Nos.		Corrigendum-III
524	SOR-D	41	Microsoft Windows Server Standard 2019 R2 subscription license 24 core – 10 Nos. MS - SQLSvrStdCore 2017 SNGL MVL 2Lic CoreLic 2 Core Licenses- 10 Nos.	Additional Clause	Railtel should add a line to the tender that – “All the license qty have been put in the RFP by Railtel after checking respective OEM’s licensing policy and minimum license requirements”		Corrigendum-III
525	SOR-A: Storage – A-1 - Unified Storage system of 600 TB: Sl. No. 2	19	The Storage Systems should be supplied with minimum 600TB Usable capacity using 500 capacity on SAS/NLSAS Drives on RAID6 and 100TB using SSD on RAID 6 and scalable up to 1PetaByte usable capacity using SAS/SSD.	Please clarify if the required capacity is effective capacity after considering data reduction functionalities OR physical usable capacity without considering any data reduction functionality like deduplication, compression etc.			Corrigendum-III
526	SOR-A: Storage – A-1 - Unified Storage system of 600 TB: Sl. No. 7	19	Storage System should have multiple Global Hot Spares. One Hot spare disk should be provided for every 30 Disk Drives.	Considering the criticality of the data to be stored on this storage system, we recommend to have 1 hot spare disk for every 20 drives.			As per RFP
527	SOR-A: Storage – A-1 - Unified Storage system of 600 TB: Sl. No. 2		The Storage Systems should be supplied with minimum 600TB Usable capacity using 500 capacity on SAS/NLSAS Drives on RAID6 and 100TB using SSD on RAID 6 and scalable up to 1PetaByte usable capacity using SAS/SSD.	Please clarify if the required capacity is effective capacity after considering data reduction functionalities OR physical usable capacity without considering any data reduction functionality like deduplication, compression etc.			Corrigendum-III

528	SOR-A: Storage – A-1 - Unified Storage system of 600 TB: Sl. No. 7		Storage System should have multiple Global Hot Spares. One Hot spare disk should be provided for every 30 Disk Drives.	Considering the criticality of the data to be stored on this storage system, we recommend to have 1 hot spare disk for every 20 drives.			As per RFP
529		41	SOR –D Licenses for OS, DB and NMS/EMS:	All the Software needs to be Perpetual	The Global Policy of EDB is to provide support to PostgreSQL through support subscriptions, which essentially means a period during which the user can avail Technical Support and use EDB developed Tools during the period after paying the fees.. EDB does not sell or charge any license fee for Postgers Licenses instead EDB sells support subscriptions .		Clarification: Free Downloaded software may not be on the name of RailTel but all procured/purchased licences must be on the name of RailTel.
530		New		EDB PostGre SQL support system for DB servers - 860 Nos	The Unit of Measure (UOM) for EDB to provide support subscriptions is on the Number of Cores that resides in Database server. Please treat 860 Nos as 860 No of Cores		Corrigendum-III
531	2, vii	12	Core router for DC & DR	It is assumed that the core routers are not part of deliverables for this project and will be provided by Railtel. Please confirm	As there are no specs or quantity mentioned in RFP		Corrigendum-III
532	3, ix	13	Veeam is the existing incumbent in the Backup Space. It would be recommended to have Backup Solution co-exist with incumbent solution and enhance the backup capacity. However bidder may propose any other backup solution which needs to be integrated with existing backup solution i.e. Veeam Backup Solution or propose entirely a new backup solution comprising existing and proposed solution capacity.	Back up proposed for this project is assuemd to be for 600TB storage and servers which are part of this project. PI confirm	For sizing and licensing		As per RFP
533	4, v	14	Bidder has to ensure smooth migration from existing SAN switch to proposed SAN switch	PI provide details of existing SAN switch (make an model, ports etc)	NA		Refer- Existing Inventory Sheet enclosed in "Annexure-A"
534	4, xi	14	Bidder needs to provide the network assurance functionality for the existing network environment.	Please specify the details of network assurance functionality to be provided for existing network	NA		Refer- Existing Inventory Sheet enclosed in "Annexure-A"
535	4.vii.	14	RailTel is already using the SDN architecture in its DC and DR , bidder has to ensure that If any integration issue of the proposed Leaf switches with the existing controller and Spine Leaf architecture, bidder to propose Spine switches and SDN controller separately to make the solution up and running without any additional cost to RailTel.	Kindly provide details of existing Spine switches and SDN controllers' Make & Model in order to propose the solution which can seamlessly work with Existing hardware	Needed for for solution design		Refer- Existing Inventory Sheet enclosed in "Annexure-A"

536	4.xii.	14	Any Management switches required for the proposed solution will be provisioned by the bidder in redundant topology.	Kindly provide details of existing management switches and free port details so that we design cost effective design.	Needed for for solution design		Clarification: Bidder needs to provide Minimum 2 numbers of management switch in DC and Two numbers in DR. 48 port 10/100/1000 BaseT with 4x10G uplink Switch with Redundant Power supply and stackable Switch. If in case bidder requires more ports as per the solution proposed , bidder to provision accordingly.
537	xiii	15	Bidder needs to integrate the cloud platform with existing LDAP solution in RailTel	Pl provide details of existing LDAP	Needed for for solution design		Clarification: Open LDAP and Active Directory is used.
538		14	RailTel is already using the SDN architecture in its DC and DR , bidder has to ensure that If any integration issue of the proposed Leaf switches with the existing controller and Spine - Leaf architecture, bidder to propose Spine switches and SDN controller separately to make the solution up and running without any additional cost to RailTel.	RailTel is already using the SDN architecture in its DC and DR. The existing architecture would support IEEE based standard protocols/technologies like BGP EVPN VXLAN or equivalent.	For non-proprietary, standards based solution which is cost neutral solution for wider OEM participation		As per RFP
539	Scope of Work	14	Bidder needs to ensure that Data Center Existing Networking environment can be used seamlessly with following Benefits: policy-driven automation through an integrated underlay and overlay, is hypervisor agnostic, and extends policy automation to any workload — including virtual machines, physical bare-metal servers, and containers.	Network automation through an integrated underlay and overlay and is hypervisor agnostic	Policy can be application or network centric. Application policy driven models are proprietary, please modify the clause for wider OEM participation		As per RFP
540		14	The proposed SDN solution must be able to analyse real time data about the network which includes any metadata, configurations, policies, device states or protocol states and then run automated checks to identify potential errors, misconfigurations and network misbehaviours.	The proposed solution should be able to support real time telemetry and show device and protocol states. It should be able to compare the device state, protocol state, configs etc. against a historic timeline to understand anomalies	As part of the SDN solutioning best practises.		As per RFP
541		14	Bidder needs to provide the network assurance functionality for the existing network environment.	Network Assurance is very broad term, and more clarity is needed on the requirements	To avoid overloading the cost of the solution as additional tools might be needed here		Refer- Existing Inventory Sheet enclosed in "Annexure-A"

542	SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity:	25	Switch should have adequate power supply for the complete system usage with all slots populated and used and provide N+1 redundant.	Switch should have adequate power supply for the complete system usage with all slots populated and used and provide 1+1 redundant.	To align with SR NO 2 which states under SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity: There switch should not have any single point of failure like power supplies and fans etc should have 1:1/N+1 level of redundancy.		As per RFP
543		25	Switch should have a minimum 40MB buffer of more.	Switch should have a minimum 32MB buffer of more.	The industry standard is 32M. Please modify the clause for wider OEM participation		As per RFP
544		25	Switch should have smart buffering mechanism to classify long lived versus short lived flows and must have capability to dynamically prioritize short lived flows during congestion to avoid packet drop of mission critical traffic.	Switch should support dynamic buffer allocation, which is fully shared across all ports, so that buffer is not constrained by ASIC pipeline	Dynamic buffer allocation caters to different types of flows. The mechanism described is specific to a particular OEM. Please modify the clause for wider OEM participation		Clarification: This is required. Bidder can propose more than 2GB Buffer in a switch alternatively, if this feature is not supported in switch.
545		19	Switch should support minimum 512 VRF instances.	Switch should support 128 VRF instances	128 VRF instances sufficiently cater to the requirements of enterprise DCs. Further, 128 is a practical number in terms of functional VRFs, which are implemented in conjunction with other configurations like routing, QOS etc. (and, not just unidimensional number of configurable VRFs)		As per RFP
546		26	Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically.	Switch should support multi OEM hypervisor environment (VMware or Hyper-V or KVM or openstack)	For wider OEM participation		As per RFP
547		14	Switch should integrate and would be part of Existing Fabric (as a Leaf), so that the Data Center Existing Networking environment can be used seamlessly with following Benefits:	Switch should integrate with existing leaf and spine fabric	In alignment to the 4. Scope of work clause vii: RailTel is already using the SDN architecture in its DC and DR , bidder has to ensure that If any integration issue of the proposed Leaf switches with the existing controller and Spine - Leaf architecture, bidder to propose Spine switches and SDN controller separately to make the solution up and running without any additional cost to RailTel.		As per RFP
548		14	policy-driven automation through an integrated underlay and overlay, is hypervisor agnostic, and extends policy automation to any workload — including virtual machines, physical bare-metal servers, and containers.	Network automation through an integrated underlay and overlay and is hypervisor agnostic	Policy can be application or network centric. Application policy driven models are proprietary, please modify the clause for wider OEM participation		As per RFP
549		14	If any integration issue of the Leaf switches in the existing controller and Spine -Leaf architecture, bidder to propose separate Spine switches and SDN controller separately.				As per RFP

550		14	The proposed solution must be able to analyze real time data about the network which includes any metadata, configurations, policies, device states or protocol states and then run automated checks to identify potential errors, misconfigurations and network misbehaviours.	The proposed solution should be able to support real time telemetry and show device and protocol states. It should be able to compare the device state, protocol state, configs etc. against a historic timeline to understand anomalies	As part of the SDN solutioning best practises.		As per RFP
551		14	The proposed solution must be able to verify configurations before been committed to be adherent to configuration best practices and if any check/verification failure occurs then system must notify it to the admin via a suitable mechanism				As per RFP
552		26	Switch should support basic Multicast IGMP v1, v2, v3.	Switch should support basic Multicast IGMP v2, v3.	IGMPv1 has no practical use case. Further, IGMPv2 and v3 are backward compatible with v1		Corrigendum-III
553		26	Switch should support MPLS segment routing and VRF route leaking functionality from day 1.	Switch should support VRF route leaking functionality from Day1	MPLS segment routing are typically required in a Service Provider environment. Please remove the clause for no practical use case in the existing environment and for wider OEM participation		As per RFP
554		26	IGMP v1, v2 and v3	IGMP v2 and v3	IGMPv1 has no practical use case. Further, IGMPv2 and v3 are backward compatible with v1		Corrigendum-III
555		27,38	Switch should support DHCP Snooping	Switch should support DHCP Snooping or equivalent to prevent unauthorized DHCP servers	For wider OEM participation		As per RFP
556		27,38	Switch should support Dynamic ARP Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol.	Switch should support ARP Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol.	For wider OEM participation		As per RFP
557		28,39	Switch should support multicast routing in IPv6 network using PIMv2 Sparse Mode	Remove this clause	For wider OEM participation		As per RFP
558	SOR-C- Network –C-1 – Leaf Switch:	25	Switch should have adequate power supply for the complete system usage with all slots populated and used and provide N+1 redundant.	Switch should have adequate power supply for the complete system usage with all slots populated and used and provide 1+1 redundant.	To align with SR NO 2 which states under SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity: There switch should not have any single point of failure like power supplies and fans etc should have 1:1/N+1 level of redundancy.		As per RFP
559		25	Switch should have a minimum 40MB buffer of more.	Switch should have a minimum 32MB buffer of more.	The industry standard is 32M. Please modify the clause for wider OEM participation		As per RFP
560		25	Switch should have smart buffering mechanism to classify long lived versus short lived flows and must have capability to dynamically prioritize short lived flows during congestion to avoid packet drop of mission critical traffic.	Switch should support dynamic buffer allocation, which is fully shared across all ports, so that buffer is not constrained by ASIC pipeline	Dynamic buffer allocation caters to different types of flows. The mechanism described is specific to a particular OEM. Please modify the clause for wider OEM participation		Clarification: This is required. Bidder can propose more than 2GB Buffer in a switch alternatively, if this feature is not supported in switch.

561		25	Switch should support minimum 512 VRF instances.	Switch should support 128 VRF instances	128 VRF instances sufficiently cater to the requirements of enterprise DCs. Further, 128 is a practical number in terms of functional VRFs, which are implemented in conjunction with other configurations like routing, QOS etc. (and, not just unidimensional number of configurable VRFs)		As per RFP
562		26	Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically.	Switch should support multi OEM hypervisor environment (VMware or Hyper-V or KVM or openstack)	For wider OEM participation		As per RFP
563		26	Switch should integrate and would be part of Existing Fabric (as a Leaf), so that the Data Center Existing Networking environment can be used seamlessly with following Benefits:	Switch should integrate with existing leaf and spine fabric	In alignment to the 4. Scope of work clause vii: RailTel is already using the SDN architecture in its DC and DR , bidder has to ensure that If any integration issue of the proposed Leaf switches with the existing controller and Spine - Leaf architecture, bidder to propose Spine switches and SDN controller separately to make the solution up and running without any additional cost to RailTel.		As per RFP
564		36	policy-driven automation through an integrated underlay and overlay, is hypervisor agnostic, and extends policy automation to any workload — including virtual machines, physical bare-metal servers, and containers.	Network automation through an integrated underlay and overlay and is hypervisor agnostic	Policy can be application or network centric. Application policy driven models are proprietary, please modify the clause for wider OEM participation		As per RFP
565			If any integration issue of the Leaf switches in the existing controller and Spine -Leaf architecture, bidder to propose separate Spine switches and SDN controller separately.				Clarification: Complete scope of work has been defined considering both scenarios that bidder may propose VMware CMP or may propose entirely new CMP platform . If bidder is proposing VMware CMP than high level SOW to be read as but not limited to " VMware cloud management platform is already setup in existing private cloud at RailTel. For VMware solution, scope will be to 1. Prepare new servers being procured as part of this tender and add them as part of existing cloud setup for expansion . 2. Migrate existing NSX-V to NSX-T 3. Integration of cloud portal with Multi factor authentication solution being procured in this tender 4. Implement SSO for cloud management software components for 15 to 20 administrators. 5. Replicate cloud management components to DR site ". If Bidder propose new CMP platform , then bidder has to perform all the activities as defined in tender."

566		37	The proposed solution must be able to analyze real time data about the network which includes any metadata, configurations, policies, device states or protocol states and then run automated checks to identify potential errors, misconfigurations and network misbehaviours.	The proposed solution should be able to support real time telemetry and show device and protocol states. It should be able to compare the device state, protocol state, configs etc. against a historic timeline to understand anomalies	As part of the SDN solutioning best practises.		Clarification: Complete scope of work has been defined considering both scenarios that bidder may propose VMware CMP or may propose entirely new CMP platform . If bidder is proposing VMware CMP than high level SOW to be read as but not limited to " VMware cloud management platform is already setup in existing private cloud at RailTel. For VMware solution, scope will be to 1. Prepare new servers being procured as part of this tender and add them as part of existing cloud setup for expansion . 2. Migrate existing NSX-V to NSX-T 3. Integration of cloud portal with Multi factor authentication solution being procured in this tender 4. Implement SSO for cloud management software components for 15 to 20 administrators. 5. Replicate cloud management components to DR site ". If Bidder propose new CMP platform , then bidder has to perform all the activities as defined in tender."
567		37	The proposed solution must be able to verify configurations before been committed to be adherent to configuration best practices and if any check/verification failure occurs then system must notify it to the admin via a suitable mechanism				As per RFP
568		26,37	Switch should support basic Multicast IGMP v1, v2, v3.	Switch should support basic Multicast IGMP v2, v3.	IGMPv1 has no practical use case. Further, IGMPv2 and v3 are backward compatible with v1		Corrigendum-III
569		26,37	Switch should support MPLS segment routing and VRF route leaking functionality from day 1.	Switch should support VRF route leaking functionality from Day1	MPLS segment routing are typically required in a Service Provider environment. Please remove the clause for no practical use case in the existing environment and for wider OEM participation		As per RFP
570		26,38	IGMP v1, v2 and v3	IGMP v2 and v3	IGMPv1 has no practical use case. Further, IGMPv2 and v3 are backward compatible with v1		Corrigendum-III
571		27,38	Switch should support DHCP Snooping	Switch should support DHCP Snooping or equivalent to prevent unauthorized DHCP servers	For wider OEM participation		As per RFP
572		27,39	Switch should support Dynamic ARP Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol.	Switch should support ARP Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol.	For wider OEM participation		As per RFP
573		28,39	Switch should support multicast routing in IPv6 network using PIMv2 Sparse Mode	Remove this clause	For wider OEM participation		As per RFP

574		14	RailTel is already using the SDN architecture in its DC and DR , bidder has to ensure that If any integration issue of the proposed Leaf switches with the existing controller and Spine -Leaf architecture, bidder to propose Spine switches and SDN controller separately to make the solution up and running without any additional cost to RailTel.	RailTel is already using the SDN architecture in its DC and DR. The existing architecture would support IEEE based standard protocols/technologies like BGP EVPN VXLAN or equivalent.	For non-proprietary, standards based solution which is cost neutral solution for wider OEM participation		As per RFP
575	Scope of Work	14	Bidder needs to ensure that Data Center Existing Networking environment can be used seamlessly with following Benefits: policy-driven automation through an integrated underlay and overlay, is hypervisor agnostic, and extends policy automation to any workload — including virtual machines, physical bare-metal servers, and containers.	Network automation through an integrated underlay and overlay and is hypervisor agnostic	Policy can be application or network centric. Application policy driven models are proprietary, please modify the clause for wider OEM participation		As per RFP
576		14	The proposed SDN solution must be able to analyse real time data about the network which includes any metadata, configurations, policies, device states or protocol states and then run automated checks to identify potential errors, misconfigurations and network misbehaviours.	The proposed solution should be able to support real time telemetry and show device and protocol states. It should be able to compare the device state, protocol state, configs etc. against a historic timeline to understand anomalies	As part of the SDN solutioning best practises.		As per RFP
577		14	Bidder needs to provide the network assurance functionality for the existing network environment.	Network Assurance is very broad term, and more clarity is needed on the requirements	To avoid overloading the cost of the solution as additional tools might be needed here		Refer- Existing Inventory Sheet enclosed in "Annexure-A"
578	SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity:	25	Switch should have adequate power supply for the complete system usage with all slots populated and used and provide N+1 redundant.	Switch should have adequate power supply for the complete system usage with all slots populated and used and provide 1+1 redundant.	To align with SR NO 2 which states under SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity: There switch should not have any single point of failure like power supplies and fans etc should have 1:1/N+1 level of redundancy.		As per RFP
579	SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity:	25	Switch should have a minimum 40MB buffer of more.	Switch should have a minimum 32MB buffer of more.	The industry standard is 32M. Please modify the clause for wider OEM participation		As per RFP
580	SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity:	25	Switch should have smart buffering mechanism to classify long lived versus short lived flows and must have capability to dynamically prioritize short lived flows during congestion to avoid packet drop of mission critical traffic.	Switch should support dynamic buffer allocation, which is fully shared across all ports, so that buffer is not constrained by ASIC pipeline	Dynamic buffer allocation caters to different types of flows. The mechanism described is specific to a particular OEM. Please modify the clause for wider OEM participation		Clarification: This is required. Bidder can propose more than 2GB Buffer in a switch alternatively, if this feature is not supported in switch.

581	SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity:	25	Switch should support minimum 512 VRF instances.	Switch should support 128 VRF instances	128 VRF instances sufficiently cater to the requirements of enterprise DCs. Further, 128 is a practical number in terms of functional VRFs, which are implemented in conjunction with other configurations like routing, QOS etc. (and, not just unidimensional number of configurable VRFs)		As per RFP
582	SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity:	26	Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically.	Switch should support multi OEM hypervisor environment (VMware or Hyper-V or KVM or openstack)	For wider OEM participation		As per RFP
582	SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity:	26	Switch should integrate and would be part of Existing Fabric (as a Leaf), so that the Data Center Existing Networking environment can be used seamlessly with following Benefits:	Switch should integrate with existing leaf and spine fabric	In alignment to the 4. Scope of work clause vii: RailTel is already using the SDN architecture in its DC and DR , bidder has to ensure that If any integration issue of the proposed Leaf switches with the existing controller and Spine - Leaf architecture, bidder to propose Spine switches and SDN controller separately to make the solution up and running without any additional cost to RailTel.		As per RFP
582	SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity:	26	policy-driven automation through an integrated underlay and overlay, is hypervisor agnostic, and extends policy automation to any workload — including virtual machines, physical bare-metal servers, and containers.	Network automation through an integrated underlay and overlay and is hypervisor agnostic	Policy can be application or network centric. Application policy driven models are proprietary, please modify the clause for wider OEM participation		As per RFP
582	SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity:	26	If any integration issue of the Leaf switches in the existing controller and Spine -Leaf architecture, bidder to propose separate Spine switches and SDN controller separately.				As per RFP
582	SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity:	26	The proposed solution must be able to analyze real time data about the network which includes any metadata, configurations, policies, device states or protocol states and then run automated checks to identify potential errors, misconfigurations and network misbehaviours.	The proposed solution should be able to support real time telemetry and show device and protocol states. It should be able to compare the device state, protocol state, configs etc. against a historic timeline to understand anomalies	As part of the SDN solutioning best practises.		As per RFP
582	SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity:	26	The proposed solution must be able to verify configurations before been committed to be adherent to configuration best practices and if any check/verification failure occurs then system must notify it to the admin via a suitable mechanism				As per RFP
583	SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity:	26	Switch should support basic Multicast IGMP v1, v2, v3.	Switch should support basic Multicast IGMP v2, v3.	IGMPv1 has no practical use case. Further, IGMPv2 and v3 are backward compatible with v1		Corrigendum-III

584	SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity:	26	Switch should support MPLS segment routing and VRF route leaking functionality from day 1.	Switch should support VRF route leaking functionality from Day1	MPLS segment routing are typically required in a Service Provider environment. Please remove the clause for no practical use case in the existing environment and for wider OEM participation		As per RFP
585	SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity:	26	IGMP v1, v2 and v3	IGMP v2 and v3	IGMPv1 has no practical use case. Further, IGMPv2 and v3 are backward compatible with v1		Corrigendum-III
586	SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity:	27	Switch should support DHCP Snooping	Switch should support DHCP Snooping or equivalent to prevent unauthorized DHCP servers	For wider OEM participation		As per RFP
587	SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity:	27	Switch should support Dynamic ARP Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol.	Switch should support ARP Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol.	For wider OEM participation		As per RFP
588	SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity:	28	Switch should support multicast routing in IPv6 network using PIMv2 Sparse Mode	Remove this clause	For wider OEM participation		As per RFP
589	SOR-C- Network –C-1 – Leaf Switch:	36	Switch should have adequate power supply for the complete system usage with all slots populated and used and provide N+1 redundant.	Switch should have adequate power supply for the complete system usage with all slots populated and used and provide 1+1 redundant.	To align with SR NO 2 which states under SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity: There switch should not have any single point of failure like power supplies and fans etc should have 1:1/N+1 level of redundancy.		As per RFP
590	SOR-C- Network –C-1 – Leaf Switch:	36	Switch should have a minimum 40MB buffer of more.	Switch should have a minimum 32MB buffer of more.	The industry standard is 32M. Please modify the clause for wider OEM participation		As per RFP
591	SOR-C- Network –C-1 – Leaf Switch:	36	Switch should have smart buffering mechanism to classify long lived versus short lived flows and must have capability to dynamically prioritize short lived flows during congestion to avoid packet drop of mission critical traffic.	Switch should support dynamic buffer allocation, which is fully shared across all ports, so that buffer is not constrained by ASIC pipeline	Dynamic buffer allocation caters to different types of flows. The mechanism described is specific to a particular OEM. Please modify the clause for wider OEM participation		Clarification: This is required. Bidder can propose more than 2GB Buffer in a switch alternatively, if this feature is not supported in switch.
592	SOR-C- Network –C-1 – Leaf Switch:	25	Switch should support minimum 512 VRF instances.	Switch should support 128 VRF instances	128 VRF instances sufficiently cater to the requirements of enterprise DCs. Further, 128 is a practical number in terms of functional VRFs, which are implemented in conjunction with other configurations like routing, QOS etc. (and, not just unidimensional number of configurable VRFs)		As per RFP
593	SOR-C- Network –C-1 – Leaf Switch:	36	Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically.	Switch should support multi OEM hypervisor environment (VMware or Hyper-V or KVM or openstack)	For wider OEM participation		As per RFP
593	SOR-C- Network –C-1 – Leaf Switch:	36	Switch should integrate and would be part of Existing Fabric (as a Leaf), so that the Data Center Existing Networking environment can be used seamlessly with following Benefits:	Switch should integrate with existing leaf and spine fabric	In alignment to the 4. Scope of work clause vii: RailTel is already using the SDN architecture in its DC and DR , bidder has to ensure that If any integration issue of the proposed Leaf switches with the existing controller and Spine - Leaf architecture, bidder to propose Spine switches and SDN controller separately to make the solution up and running without any additional cost to RailTel.		As per RFP

593	SOR-C- Network –C-1 – Leaf Switch:	36	policy-driven automation through an integrated underlay and overlay, is hypervisor agnostic, and extends policy automation to any workload — including virtual machines, physical bare-metal servers, and containers.	Network automation through an integrated underlay and overlay and is hypervisor agnostic	Policy can be application or network centric. Application policy driven models are proprietary, please modify the clause for wider OEM participation		As per RFP
593	SOR-C- Network –C-1 – Leaf Switch:	36	If any integration issue of the Leaf switches in the existing controller and Spine -Leaf architecture, bidder to propose separate Spine switches and SDN controller separately.				As per RFP
593	SOR-C- Network –C-1 – Leaf Switch:	36	The proposed solution must be able to analyze real time data about the network which includes any metadata, configurations, policies, device states or protocol states and then run automated checks to identify potential errors, misconfigurations and network misbehaviours.	The proposed solution should be able to support real time telemetry and show device and protocol states. It should be able to compare the device state, protocol state, configs etc. against a historic timeline to understand anomalies	As part of the SDN solutioning best practises.		As per RFP
593	SOR-C- Network –C-1 – Leaf Switch:	36	Any Management switches required for the proposed solution will be provisioned by the bidder in redundant topology.				Clarification: Bidder needs to provide Minimum 2 numbers of management switch in DC and Two numbers in DR. 48 port 10/100/1000 BaseT with 4x10G uplink Switch with Redundant Power supply and stackable Switch. If in case bidder requires more ports as per the solution proposed , bidder to provision accordingly.
593	SOR-C- Network –C-1 – Leaf Switch:	37	Switch should support basic Multicast IGMP v1, v2, v3.	Switch should support basic Multicast IGMP v2, v3.	IGMPv1 has no practical use case. Further, IGMPv2 and v3 are backward compatible with v1		Corrigendum-III
593	SOR-C- Network –C-1 – Leaf Switch:	37	Switch should support MPLS segment routing and VRF route leaking functionality from day 1.	Switch should support VRF route leaking functionality from Day1	MPLS segment routing are typically required in a Service Provider environment. Please remove the clause for no practical use case in the existing environment and for wider OEM participation		As per RFP
593	SOR-C- Network –C-1 – Leaf Switch:	37	IGMP v1, v2 and v3	IGMP v2 and v3	IGMPv1 has no practical use case. Further, IGMPv2 and v3 are backward compatible with v1		Corrigendum-III
593	SOR-C- Network –C-1 – Leaf Switch:	38	Switch should support DHCP Snooping	Switch should support DHCP Snooping or equivalent to prevent unauthorized DHCP servers	For wider OEM participation		As per RFP
593	SOR-C- Network –C-1 – Leaf Switch:	38	Switch should support Dynamic ARP Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol.	Switch should support ARP Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol.	For wider OEM participation		As per RFP
594	SOR-B- Cloud Solution –B-2- Leaf Switch for Server Connectivity:	28	Switch should support multicast routing in IPv6 network using PIMv2 Sparse Mode	Remove this clause	For wider OEM participation		As per RFP

595	SOR-A: Storage – A-1 - Unified Storage system of 600 TB:	19	The Storage Systems should be supplied with minimum 600TB Usable capacity using 500 capacity on SAS/NLSAS Drives on RAID 6 and 100TB using SSD on RAID 6 and scalable up to 1PetaByte usable capacity using SAS/SSD.	Please define capacity of 500 qty of which type of drive, NL-SAS or SAS?	CLRIFITION		Corrigendum-III
596	SOR-A: Storage – A-1 - Unified Storage system of 600 TB:	19	The storage should support and be configured with automated data tiering between different drive types namely SSD, SAS, and NL-SAS within the same storage array. The storage should be capable of moving data blocks between these drive types (up and down the tier) depending on the access patterns to ensure optimum storage performance.	Request you to amend as below, "The storage should support and be configured with automated data tiering between different drive types namely SSD & SAS or SSD & NL-SAS within the same storage array. The storage should be capable of moving data blocks between these drive types (up to down the tier) depending on the access patterns to ensure optimum storage performance."			As per RFP
597	SOR-A: Storage – A-1 - Unified Storage system of 600 TB:	19	The Storage should be scalable to at least 800 SFF/LFF disk drives on the same set of controllers.	Request you to amend as below, "The Storage should be scalable to at least 1400 SFF/LFF disk drives on the same set of controllers."			Clarification: As per RFP, However bidder may propose higher storage scalable capacity.
598	SOR-A: Storage – A-1 - Unified Storage system of 600 TB:	19	The Storage should support minimum RAID 5, RAID 6 and RAID10 as different applications requires different performance levels	Request you to amend as below, "The Storage should support minimum RAID 6 or equivalent".			As per RFP
599	SOR-A: Storage – A-1 - Unified Storage system of 600 TB:	19	Storage should be equipped with 8*32 Gbps FC ports, 4*10Gbe port for host connectivity. Required SFPs/Optical Module to be populated from day one	Request you to amend as below, "Storage should be equipped with 8*32 Gbps FC ports, 4*40G Ports and 4*10Gbe port for host connectivity. Required SFPs/Optical Module to be populated from day one"			As per RFP
600	SOR-A: Storage – A-1 - Unified Storage system of 600 TB:	19	The storage system should have minimum 512GB global cache on the same set of proposed controllers for both reads & writes. Cache memory should be delivered on DRAM, any other device or HDD should not be considered as cache. Cache shall be completely dynamic for read and write operations.	Request you to amend as below. "The storage system should have minimum 512GB DRAM cache across the same set of proposed controllers for both reads & writes. Cache memory should be delivered on DRAM, any other device or HDD should not be considered as cache. Cache shall be completely dynamic for read and write operations."			As per RFP
601	SOR-A: Storage – A-1 - Unified Storage system of 600 TB:	19	The proposed storage system should support at least 24000 LUNs or volumes	Request you to amend as below, " The proposed storage system should support at least 5000 LUNs or Volumes"			Corrigendum-III
602	SOR-A:Storage – A-3 – SAN Switch:	22	SAN switch should be supplied with minimum 96 * 32Gbps FC ports and all ports should be active with required license and fully populated modules from day one.	Is there any further scale expected? Brocade SAN Switch can offer additional 24 Ports in the same form factor			As per RFP

603	SOR-A-Storage – A-3 – SAN Switch:	22	Required ports shall not be achieved by cascading the number of switches and shall be offered within the common chassis only.	Is Chassis Solution required or regular departmental class SAN Switch with Solution level HA suffice?			As per RFP
604	SOR-A-Storage – A-3 – SAN Switch:	22	Switch should have LED indicators for active system components like FAN, PSU, Ethernet ports, FC Ports, management ports, Chassis status, etc.	Chassis Status ?			As per RFP
605	SOR-A-Storage – A-3 – SAN Switch:	22	Switch should support secure boot to allow only OEM's Genuine software to be loaded on switches.	Need more clarity on this point			Corrigendum-III
606	SOR-C, C-2						Corrigendum-III
607	Scope of Work & Technical Requirement		Scope of Work & Technical Requirement	New			Corrigendum-III
608	Scope of Work & Technical Requirement		Scope of Work & Technical Requirement	New			Corrigendum-III