



RailTel/EOI/NR/BA/20-21/Business Delivery/RO/2

Dt. -02-MAR-2021

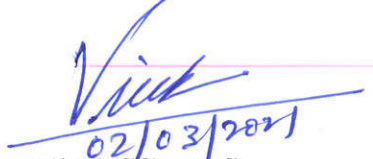
To,

Dear SI Partner

Sub : Corrigendum to EOI No. RailTel/EOI/NR/BA/20-21/Business Delivery/RO/2 Dt. –
26-Feb-2021

Reference is made to the Expression of Interest (EOI) for Selection of Systems Integrator & Implementation Partner for bidding for the requirement of customer of RailTel (CoR) for “Supply, installation and commissioning of IT infrastructure system and application system on back-to-back basis” from RailTel’s empanelled BAs/ SIs / partners.

2. Enclosed herewith find the corrigendum to this EOI.


02/03/2021
(Vivek J. Porwal)
GM-Marketing
RailTel Northern Region

रेलटेल कॉर्पोरेशन ऑफ इण्डिया लिमिटेड (भारत सरकार का एक उपक्रम, रेल मंत्रालय)

RailTel Corporation of India Ltd. (A Government of India Undertaking, Ministry of Railways)

Northern Region Office : 6th Floor, Block-III, Delhi IT Park, Shastri Park, Delhi -110053.

CIN: U64202DL2000GOI107905 Tel. : +91 (11) 22185933, 22185934 • Fax : +91 (11) 22185978

E-mail : ednr@railtelindia.com • www.railtelindia.com

कॉरपोरेट व पंजीकृत कार्यालय : प्लेट-ए, 6वां तल, कार्यालय ब्लॉक, टॉवर-2, पूर्वी किदवाई नगर, नई दिल्ली -110023

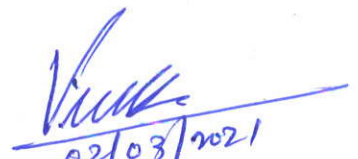
Corporate & Regd. Office : Plate-A, 6th floor, Office Block, Tower -2, East Kidwai Nagar, New Delhi-110023

Tel.: +91 (11) 22900600 • E-mail info@railtelindia.com • www.railtelindia.com

1. Revised bid submission date is as below:

1	EOI No	RailTel/EOI/NR/BA/20-21/Business Delivery/RO/2
2	Submission of EOI documents at https://railtel.enivida.com	05-MAR-2021 by 11:00 Hrs.
3	Opening of EOI (online)	05-MAR-2021 by 11:30 Hrs.

2. Bidder has to submit an undertaking on exclusive participation with RailTel for this opportunity on their letter head dully signed by their authorized signatory along with their offer. In case of non-submission of the undertaking, their offer will be summarily rejected.
3. Clarification and amendments to technical requirements, tender conditions etc. as issued by customer of RailTel is enclosed as annexure-1
4. Other terms & Conditions shall remain same.


02/03/2021
(Vivek J Porwal)
GM-Marketing
RailTel Northern Region

REPLY TO PRE BID QUERIES : GENERAL

<u>Sl No</u>	<u>Query</u>	<u>Relevant Para of RFP on which query has been raised</u>	<u>Reply to the Query</u>
01	<u>Amendment in Payment Terms</u> (a) 15% Advance payment of the base contract price will be paid within 30 days... (b) 65% payment will be paid as per actual supply to the seller in staggered manner in five tranche on pro-rata basis along with 100% taxes (c)15% payment on successful installation & commissioning and training during I&C in all the 05 data 05 nodal locations (d) Balance 5% payment will be made after successful completion of one year warranty and successful completion of post I&C training	Para 5 and Annexure VI of Appendix G	No change in RFP
02	<u>Joint Receipt Inspection (JRI)</u>. The following point is not feasible and hence may be removed:- (a) Complete functional checking of the stores/equipment as per specifications in	Para 9 (a) (ii) of Appendix G of RFP	Please refer Corrigendum Page 33.

	the contract and as per procedures and tests laid down by Buyer but functional checking of spares shall not be done.		
03	<u>Amendment in Liquidated Damages (LD) Clause.</u> (a) Bidder's failure to supply the Hardware, Software, Performance services, installation of equipment including Hardware and Software, the vendor shall be levied LD @ 0.5% per week of delay subject to maximum of 10% of value of delayed stores, calculated on the basis of the Contract Price of delayed stores.	Para 10 of Appendix G of RFP	No change in RFP
04	<u>Amendment in Evaluation Criteria.</u> (a) Items wise AMC cost breakdown is not feasible. So it is requested to kindly confirm that only year wise AMC proposal to be provided in financial bid.	Para 1 (c) of Appendix H of RFP	No change in RFP
05	<u>Amendment in Country of Origin Certificate Clause.</u> (a) Country of Origin certificate in respect to all line items is not feasible. Request if submission of only major OEMs country of origin certificate should be adequate.	Para 6 (b) of Part I of RFP	No change in RFP. It is mandatory to submit the country of origin certificate from respective OEMs, for all deliverable line items.

06	<u>Amendment in Escalation Matrix Clause.</u> (a) Escalation Matrix for all the line items which are part of deliverables is not possible. So it is requested to kindly confirm that escalation matrix for major OEM will be submitted along with the proposal.	Para 1 (h) of Appendix L of RFP	No change in RFP. Escalation matrix of respective OEMs for all deliverable line items, are to be submitted.
07	<u>Integrity Performance Bank Guarantee (IPBG) against Pre Contract Integrity Pact (PCIP).</u> (a) Request clarify whether indemnity bond or IPBG is to be submitted against PCIP.	Para 19 of Part I and Para 4 of Appendix J of RFP	Only DPSUs can submit Indemnity bond. The other firms have to submit IPBG as per Para 4 (b) of Appendix J of RFP

REPLY TO PRE BID QUERIES : SPECIFICATIONS

Clause Nos.	Current Specification	Revised Specification	Clarification/Justification	Remarks of Buyer
	HCI SPECIFICATIONS			
Page 23	Cache offered per node in GB - 500GB	-	Cache offered per node in GB -Min 500GB if required as part of solution to meet the asked performance and availability parameters in specifications.	Refer Page 3-8 of corrigendum on RFP issued vide 01 Mar 21
Page 23	SSD Capacity per Node (Raw) -Min 12TB	-	SSD Capacity per Node (Raw) -Min 12TB or SSD Capacity allocated to each Node (Raw) -Min 12TB	Refer Page 3-8 of corrigendum on RFP issued vide 01 Mar 21
Page 23 &24	No. of Cache drives per node-2 drives	-	No. of Cache drives per node-2 disk if required as per of the solution to meet the asked performance and availability parameters in the specifications.	Refer Page 3-8 of corrigendum on RFP issued vide 01 Mar 21
Page 23&24	No. of Cache drives per node -2	-	No. of Cache drives per node-2 disk if required as per of the solution to meet the asked performance and availability parameters in the specifications.	Refer Page 3-8 of corrigendum on RFP issued vide 01 Mar 21
Page 24	Cache offered per node in GB - 800GB	-	Cache offered per node in GB -Min 800GB if required as part of solution to meet the asked performance	Refer Page 3-8 of corrigendum on RFP issued vide 01 Mar 21

			and availability parameters in specifications.	
Page 24	SSD Capacity per Node - Min 75TB	-	SSD Capacity per Node (Raw) -Min 75TB or SSD Capacity allocated to each Node (Raw) -Min 75TB	Refer Page 3-8 of corrigendum on RFP issued vide 01 Mar 21
Page 24	SSD Capacity per Node - Min 75TB	-	Please confirm is it usable to Raw?	Refer Page 3-8 of corrigendum on RFP issued vide 01 Mar 21
Pg 23 & 24	Operation Management Suite=Qty 01 for Mgmt of all clusters at one site	We understand that one management suite is required to manage all the five cluster from a single site. Please confirm		Two sets of Management suite will be required to manage both Type A & B HCIs independently
Pg 23 & 24	Cloud Automation and Orchestration solution=Qty 01 for Mgmt Of all clusters at one site	We understand that one cloud automation ans orchestration solution is required to manage all the five cluster from a single site. Please confirm		Two sets of Cloud Automation solution will be required to manage both Type A & B HCIs independently
1(h)	Proposed solution should support any two of the following hypervisors :- (a) Microsoft Hyper-V (b) VMware ESXi (c) RHEL KVM (d) Nutanix AHV	Proposed solution should support any one of the following hypervisors :- (a) Microsoft Hyper-V (b) VMware ESXi (c) RHEL KVM (d) Nutanix AHV	CoR mentioned that they required pre-configured appliance with Hypervisor installed on it then there should not be any requirement to support two hypervisors on the solution as it will limit the RFP participation. Changing the hypervisor in the field is	Refer Page 3-8 of corrigendum on RFP issued vide 01 Mar 21

			disruptive and might lead to data loss. Would request you to change it to any one hypervisor.	
1(i)	Also, it should support Guest OS of Windows server and Linux (Red Hat, Suse and CentOS). Certification and support should be from Virtualization Vendor. Virtualization License provided should be of Enterprise versionl edition.	Also, it should support Guest OS of Windows server and Linux (Red Hat, Suse and CentOS). Certification and support should be from Virtualization Vendor & from Guest Operating System. Virtualization License provided should be of Enterprise versionl edition.	Its important that since CoR has requested for Virtualisation certification then the Guest OS OEM should also certify them and link should be publically available.	No Change
1(K)	The solution must deliver zero data loss in case of disk, host, and network or node failure. The HCI platform should have ability to replicate VM's independently & irrespective of the Hypervisor SW (2 way/3 way replication)	With multiple sites installation, it will be very helpful to have a "one-to-many" site data replication, as well as "many-to-one" site data consolidation on HCI. Without this, it will become very siloed data distribution.	The solution must deliver zero data loss in case of disk, host, and network or node failure. The HCI platform should have ability to replicate VM's independently & irrespective of the Hypervisor SW (2-way/3 way replication) (from one-site to many sites, as well as from many-sites to one site)	No Change
1(m)	The solution should be able to extend the storage resources of the HCI system to external hosts to	The solution should be able to extend the storage	Since the RFP asks for connecting Bare Metal Servers and the existing	No Change

	allow additional consolidation of workloads onto the HCI platform.	resources of the HCI system to external hosts to allow additional consolidation of workloads onto the HCI platform. HCI System should be able to connect on FC Protocol and iSCSI Protocol for the storage connectivity in the near future.	workloads, its important that the HCI Solution should be able to connect on the FC and iSCSI Protocols to support the existing infrastructure of workloads.	
1(p)	SELLER/ Vendor will submit separate valid Manufacturers Authorization Form (MAF), along with complete technical details/ specifications of the solution in the bid, from OEM/ Technology partner for HCI solution and for the Scale Out NAS and block Storage solution. For OEM's with providing the solution on commercial off the shelf (COTS) servers (hardware) of other OEMs, they should provide datasheets I documented proof stating alliance I support by the hardware OEM for running the HCI software I Hypervisor I Scale Out NAS Storage I block storage solution on the selected hardware	-	(p)SELLER/ Vendor will submit separate valid Manufacturers Authorization Form (MAF), along with complete technical details/ specifications of the solution in the bid, from OEM/ Technology partner for HCI solution and for the Scale Out NAS and block Storage solution. For OEM's with providing the solution on commercial off the shelf (COTS) servers (hardware) of other OEMs, they should provide datasheets I documented proof stating alliance I support by the hardware OEM for running the HCI software I Hypervisor I NAS Storage I block	Refer Page 3-8 of corrigendum on RFP issued vide 01 Mar 21

			storage solution on the selected hardware	
1(c)	The proposed software defined solution must be listed as a valid and certified solution on the server hardware OEM's website.	(c) The proposed software defined solution must be listed as a valid and certified solution on the server / storage hardware OEM's website.	Request you to remove either server or add server / Storage.	Refer Page 3-8 of corrigendum on RFP issued vide 01 Mar 21
2(c)	The proposed solution must support various replication methods (RF=2 & RF=3) or (FTT=1 & FTT=2) or (RAID + RAIN protection) for data protection. Any software license required for the same must be quoted on day one.	The proposed solution must support various replication methods (RF=2 & RF=3) or (FTT=1 & FTT=2) or (RAID + RAIN protection) or (RAID Protection with min 3 drive failure) for data protection. Any software license required for the same must be quoted on day one.	Different OEM's have different solutions , request you to allow the requested changes for wider participation.	Refer Page 3-8 of corrigendum on RFP issued vide 01 Mar 21
3(o)	The HCI storage must have integrated wizard for batch clones of virtual machines and customization.	The HCI storage must have integrated wizard/cli for batch clones of virtual machines and customization.	Would urge to accept our change sor supporting batch of clones with either CLI/GUI.	Refer Page 3-8 of corrigendum on RFP issued vide 01 Mar 21
3(k)	The HCI should support native file services over NFS, CIFS ISMB, for file replication across clusters and data centers.. It must support Soft	To be Removed	Since NAS Services has been asked in the Enterprise Storage Category, would recommend	Refer Page 3-8 of corrigendum on RFP issued vide 01 Mar 21

	/ Hard quotas for File shares', .at a user level and group level.		customer to remove this clause for HCI Specifications. Multiple File Services/Shares will lead to complexity and unnecessary downtime.	
3© & 7(j)	The HCI software must pool all SSD from all the nodes in the cluster to present a single storage resource pool to all server nodes in the cluster. The SSD storage should support a minimum 50K IOPS per node Each cluster should provide min 400000 IOPS with less than 2ms response time at 70:30 read: write ratio in 8K block size and should be configured to provide min 3GB/sec throughput at 32K block size for the available capacity. Reports for the same should be attached as a part of technical proposal	-	Both clauses are contradictory to each other. Our understanding is that per node shall be scalable / support 50,000 IOPS. Also considering 50,000 iops per node - for achieving 400000 iops - Minimum 8 nodes are required whereas RFP ask for either 5 node (Type A) or 4 node (Type B) HCI solution. Request to provide the clarity here?	Refer Page 3-8 of corrigendum on RFP issued vide 01 Mar 21
4(a) (i)	(a) (i) The proposed storage solution hardware should consist of minimum 01 nodes resources per site I cluster to cater for N+1 redundancy at 06 sites/locations and with minimum 04 controllers at each site /locate ion of which each controller will have 4 cores, 128GB RAM each with a san switch consisting of minimum 04 number of 25 Gbps ports per node.	(a) (i) The proposed storage solution hardware should consist of minimum 01 nodes resources per site I cluster to cater for N+1 redundancy at 06 sites/locations and with minimum 04 controllers at each	Please also allow a storage array based solution with 10/25Gig /FC connectivity to the HCI nodes.	Refer Page 3-8 of corrigendum on RFP issued vide 01 Mar 21

		site /location of which each controller will have 4 cores, 128GB RAM each with a san switch consisting of minimum 04 number of 25 Gbps ports per node. or Storage array based solution with asked usable capacity provisioned to the HCI nodes via 10/25Gig /FC interfaces.		
5(b)	(b) The platform must support management of multiple individual clusters I sites (from multiple OEM I Hypervisors) from a Single Console, and with single sign-on. The platform should support management of the offered Scale-Out NAS solution.	(b) The platform must support management of multiple individual clusters I sites (from multiple OEM I Hypervisors) from a Single Console, and with single sign-on. The platform should support management of the offered Scale-Out NAS or NAS solution.	Our NAS based offerings on the HCI is called as NAS , please allow the changes for the more wider participation.	Refer Page 3-8 of corrigendum on RFP issued vide 01 Mar 21
5(d)	The cloud management cluster should have a high availability design which should be accessible from atleast two locations spread across the WAN. It should support multi-site deployment architecture with	We understand that CoR is looking for cloud management solution in HA spread across two		Confirmed

	automated DR. It should be capable to perform non-disruptive DR drill/testing of recovery plan for full and selected applications without impacting production applications running in primary environment.	location/sites. Please confirm.		
7€ (i)	(e) Each node must be configured with:- (i) Minimum 02 of latest generation Intel® Xeon Cascade Lake Processor with minimum 24 or higher cores per socket (CPU), min 2.1 Ghz and 64-bit x86 processor fully binary compatible to 32-bit applications. Number of Cores or a single die/ socket will be treated as a single processor. RAM per Node should be min 1 TB. RAM per Node (DDR 4) -Min512GB (Part of HCI Type B Specification)	-	Please clarify if the RAM required per node needs to be 512GB or 1TB , since the specs for Type B HCI specs mentions 512GB RAM.	Refer Page 3-8 of corrigendum on RFP issued vide 01 Mar 21
8(c)	Installation and migration of existing virtualized applications / services / virtual machines max 10 in numbers must be done by OEM. Additional, installation and migration of existing virtualized applications / services / virtual machines max 10 in numbers must be supported by the SI, for applications which are mostly web based applications with a database.	Need Clarity	Please help us clarify the amount of Data, Type of VM's and type of Databases to be migrated with number of site. to check the interoperability	CoR existing set up has multiple OS and multiple DB applications. These need to be migrated in the new infrastructure. OEM would assist in setting up atleast 10 VM Applications and SI would hand hold 10 VMs migration to gain

				confidence for users to undertake other applicationss
NA	Cluster (Geographically Distributed) - 6	NA	Please help us clarify on the location of the deployment of these 6 clusters.	Will be 06 Data centers. Location would be shared to successful bidder
<u>AI ENGINE PROCESSORS SPECIFICATIONS</u>				
7	Capacity : The system should be quoted with 3.2TB SSD*6=192TB RAW capacity with cluster capacity to be enhanced to 68PB	Looks like typo mistake as 3.2TB*6 = 19.2TB only. Also, please clarify the enhanced cluster capacity of 68PB.		Refer Page 8-9 of corrigendum on RFP issued vide 01 Mar 21
500 TB SAN STORAGE				
1	To be configured with min 500TB raw and 250 TB usable (without considering any data reduction i.e. deduplication, compression etc.) usable storage using NVMe/SSD drives each for five Datacentres.	To be configured with min 500TB raw and 250 TB usable (without considering any data reduction i.e. deduplication, compression etc.) usable storage using NVMe/SSD drives each for five Datacentres.	1) Kindly confirm if you need 250TiB or 250TB after mirror protection? 2) Inline to Clause 7, kindly delete SSD from this clause.	Refer Page 9-12 of corrigendum on RFP issued vide 01 Mar 21
2	Offered Storage array must be a True Enterprise Grade Storage. The storage must have true symmetric Active-Active Controller architecture where a LUN must be accessible by all the controllers simultaneously . No Single Point of Failure (NSPOF) and	2. Offered Storage array must be a True Enterprise Grade Storage. The storage must have true symmetric Active-Active Controller	Different OEM's have different solution and current specifications on the enterprise storage are tending to a specific offerings. Request you to please change the clause.	Refer Page 9-12 of corrigendum on RFP issued vide 01 Mar 21

	single Microcode/operating system instead of running different Microcode I Operating system/Controllers for File & block services respectively . Controller must be scalable in future.	architecture where a LUN must be accessible by all the controllers simultaneously .	We also dont recommend running file services on the NVMe drives. Additionally ,File services are already asked as part of the HCI solution.	
3	The storage system must have minimum 2 TB or higher Global Cache and must support scalability. Only write cache must be mirrored. If Read Cache is mirrored then additional 25% Cache capacity must be provided. Cache memory must be delivered on DRAM, any other device or HDD must not be considered as cache	The storage system must have minimum 2 TB or higher Global Cache and must support scalability.	We request you to change this to 2 TB global cache as we offer better resiliency features. Recent RFP from CoR had allowed requested change. We do mirroring for read and write operations but at the same time we confirm that 2TB cache is good enough to support 250TB usable capacity asked.	Refer Page 9-12 of corrigendum on RFP issued vide 01 Mar 21
11	11. Storage system must support Controller-based Data-At-Rest Encryption.	Request you to please change clause as " Storage system must support FIPS 140 certified Data-At-Rest Encryption." Self Encrypting drives shall be offered.	Request you to please specify SED Drives with FIPS140 certification for the enterprise grade encryption.	Refer Page 9-12 of corrigendum on RFP issued vide 01 Mar 21
17	Offered Storage array must be supplied with Min 24x32Gbps Ports (NVMeOF) and 8 ports of 10/24 Gbps for replication and scalable to double in future on the same set of proposed controllers without compromising on the Back End Directors or Storage Processors.	Offered Storage array must be supplied with Min 24 x 32Gbps Ports (NVMeOF), 4x10Gbps NAS ports and 8 ports of 10 Gbps for replication and	1) Clause 2 asks for Unified Storage i.e. Block + File. So request you to ask 4x10Gbps ports for replication 2) We suggest you to look for 16x32Gbps Ports for NVMeOF and 8x10Gbps ports for replication.	Refer Page 9-12 of corrigendum on RFP issued vide 01 Mar 21

		scalable to double in future on the same storage system .	3) Also request you to allow scalability within system as scale-out architecture allow additional controllers within the same storage system.	
34	The storage must support multiple operating systems such as Windows, Unix, Linux, Solaris and Mainframe etc	The storage must support multiple operating systems such as Windows, Unix, Linux, Solaris and Mainframe etc	As we understand CoR is not using Mainframes, so requesting removal of Mainframes.	Refer Page 9-12 of corrigendum on RFP issued vide 01 Mar 21
42	The replication solution must have capability to support three-way remote replication in both Concurrent with Delta Resync for zero-data-loss and Cascaded configuration with minimal impact on the primary storage system	Request CoR to please change the clause as " The replication solution must have capability to support three-way remote replication in both Concurrent with Delta Resync for zero-data-loss and Cascaded / concurrent configuration with minimal impact on the primary storage system.	Different OEM have there own best practices for providing zero data loss solution using different topologies , we recommend to allow cascade / concurrent based approach since concurrent based approach reduces the hops and dependency on the NDR site for replication between DC to DR etc.	Refer Page 9-12 of corrigendum on RFP issued vide 01 Mar 21
44	System must be able to automate the complete replication process.	Need Clarity	Our understanding is if there is any interruption of replication process, then replication should automatically resume from where it was stopped due to link issue or some other issue.	Refer Page 9-12 of corrigendum on RFP issued vide 01 Mar 21

53	The solution must be able to define storage-centric data replication policies and automate the storage-based replications	Need Clarity	Our understanding is if there is any interruption of replication process, then replication should automatically resume from where it was stopped due to link issue or some other issue.	Refer Page 9-12 of corrigendum on RFP issued vide 01 Mar 21
New	The tender has asked for 500TB RAW block storage at five locations along with SAN Switches. kindly confirm if we can provide the 500TB RAW storage from the HCI nodes itself, by increasing the number of disk and nodes in the HCI cluster at each of these 5 sites? =This will mean the specifications asked on page number 36 to 40 will not hold true for the vendors providing block storage from HCI nodes itself.			No, The scope envisages, 300 TB of block storage along with each HCI cluster and 500 TB is separate SAN storage to be provided for integration of other legacy servers available in data center
BACKUP SOLUTIONS				
1(a)	Project Scope is related to Disk Based Backup Platform of Customer of RailTel for existing Setup			Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21
1(b)	Implementation would be done in 6 sites in different locations across the country		As per the BOQ requested at page#22, the backup solution is requested at 5 sites only , however here the implementation is requested at 6 sites. Kindly confirm if the backup solution is required at 5 sites or 6.	Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21

1(c)	Each location should have 2 Copies of the Data Backup with High Availability/Clustered Solution with 99.997% uptime of the storage platform integrated with the existing Backup solution.		Please share the details of the existing backup solution & capacity of backup software license required	Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21
1(d)	Each individual location would have 2 Replication copies of Data and 3'd Replication copy of the Data would be on one of the six sites earmarked as DR site.	The proposed backup appliance should be recognised as a purpose built backup appliance The proposed solution should sized appropriately for FETB of 120 TB at each site with 2% daily change & 10% YOY Growth. The proposed solution should be sized appropriately for maintaining the below retention policies: 1> Daily Incr Backup: 28 Days 2> Weekly Full: 1 Month 3> Monthly full: 12 Months Yearly Full: 3 Years Daily backup is to be replicated at the secondary site & central DR site. The solution must be	Please share what is implied by 2 replication copies. Please confirm whether the asked capacity is for backup or replication or archival. > Basis the standards on the backup technology & recommendations of various data protection published reports "GDPR & Srikrishna committee report" data protection is a valuable component of data availability & security. As per the standard guidelines of data protection it is advised to maintain multiple copies to backup data to safeguard the environment from accidental deletion, corruption & audit requirements. Hence request you to accept the proposed changes.	Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21

		offered with minimum 120 TB usable capacity. Any software/Hardware required by the bidder to apart from 120 TB capacity must be provided by the bidder at the time of bid. > The bidder must provide the capacity based backup software license of XX TB		
1 (e)	Further, DR site will have DR Backup location for all the Data.		All 5 sites should replicate the backup copy to DR site.	No Change
1(f)	Replication Factor should be managed either by the Backup Storage Archival Vendor or by the Backup Application Software Solution (subject to best possible design).			No Change
1(g)	System should be compatible with the existing Backup Solution or the Bidder can propose a new Backup Solution with Disk Based Backup Storage. Backup Solution offering should be compatible with Existing Tape Library for Migration Services.		Please share licensing details & Retention policies maintained in the existing backup solution.	Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21
1(h)	The Solution should cater to min 200 Workloads or 600TB of storage capacity.		This is a conflict, Please confirm weather the asked capacity is for backup or replication or archival? Please share the requirement details like 200 TB FETB or BETB.	Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21

<u>Compliance features for disk based backup platform 2(a)</u>	(a) The Archive shall have an initial useable, protected storage capacity of 120TB Each Location as N+N failover concept and shall be based on hard disk media or Data Tape but non-linear access to Backup / Archive Content is preferred.	The proposed backup appliance should be recognised as a purpose built backup appliance The proposed solution should sized appropriately for FETB of 120 TB at each site with 2% daily change & 10% YOY Growth. The proposed solution should be sized appropriately for maintaining the below retention policies: 1> Daily Incr Backup: 28 Days 2> Weekly Full: 1 Month 3> Monthly full: 12 Months Yearly Full: 3 Years The solution must be offered with minimum 120 TB usable capacity. Any software/Hardware required by the bidder to apart from 120 TB capacity must be provided by the bidder at the time of bid.	Kindly confirm if the 120 TB data has to be backed up or it is the target capacity for backup solution.. As per the standard guidelines of data protection it is advised to maintain multiple copies to backup data to safeguard the environment from accidental deletion, corruption & audit requirements. Genrally customer's keep 120 copies of the backup data. maintaining only 3 backup copies would not be enough to safeguard the complete production environment.	Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21
--	--	---	---	---

		> The bidder shall propose XX TB of capacity based backup software at each site.		
2(b)	(b) DR Location would have 3rd Backup replica of each Location.	a copy of daily backup has to be replicated to the secondary site to maintain data availability in case of any issue at the primary DC.	As per the standard guidelines of data protection it is advised to maintain multiple copies to backup data to safeguard the environment from accidental deletion, corruption & audit requirements. Genrally customer's keep 120 copies of the backup data. maintaining only 3 backup copies would not be enough to safeguard the complete production environment and meet the audit requirements.	Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21
2(c)	(c) DR Location would have 100% Data of each site.	Daily backup copies to be maintained at the DR site for XX days. Hence maintaining 100% data for each site & provide protection against accidental/delibrate deletion & corruption.	the 250 Tb usable in HCI & 250 TB usable on the block storage makes the total production capacity of 500 TB. Please share how do you intend to store the same 500 TB within 120 TB of backup appliance. Since 6th site is the common DR for all the 5 sites, hence it should have the capacity to store 2.5 PB of data. Kindly confirm.	Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21

2(d)	(d) The Archive shall be based on a modular architecture and the configuration must be capable of expansion by adding modules as required.	The backup solution shall be based on a modular architecture and the configuration must be capable of expansion by adding modules as required.	This is conflicting. Please confirm whether the solution required is for backup or archive or Replication.	Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21
2 (e)	(e) The Archive shall be fully redundant with no single point of failure in the storage media. All Power Supplies and Disks must be hot swappable without loss of service.	The proposed backup solution shall be fully redundant with no single point of failure in the storage media. All Power Supplies and Disks must be hot swappable without loss of service. It must be offered with NVRAM/BBWC to protect data against abrupt power loss.	Archival, Backup & replication are three different use case. Since the RFP ask is for the backup solution, hence request you to accpet the requested change.	Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21
2(f)	(f) If the Archive is based on RAID technology, then the Array should be offered on a Clustered or Replicated Mode for resilience purpose.	The Offered PBBA must support RAID 6 & hot spare in each offered enclosure.		Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21
2(g)	(g) The Archive must support mixed disks drive capacities or mixed Tape Capacities within the same array. It is anticipated that 18TB disks will be used initially with the option to use 20 TB and larger disk capacities as they become available, in any mix without loss of storage yield, whatsoever	The proposed backup solution must be offered with 4/8 TB drives to minimize the impact of rebuilding in case of any drive failure.	Higher capacity drives in the backup solution have an overhead on performance due to RAID rebuilding. This can also impact the performance of the backup solution. Hence request you to accpet the proposed change.	Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21

2(h)	(h) Compatible 3.5" Disks must be available and be capable of mixed operation within the same module. The system must be compatible with 2.5" disks in future, and capable of supporting mixed 2.5" and 3.5" disks in the same module.	Please remove this specification as none of the backup appliance OEM support mixing different form factor drives.	Please remove this clause as every OEM has its own unique design.	Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21
2(j)	(j)The Archive shall support individually removable disk drives for shelf storage, and media transportation. Data shall be written as complete nonsegmented files on the disks and replicated for protection against individual disk failure.	The proposed backup solution shall support individually removable disk/Tape storage drives for shelf storage, and media transportation for replacement in case of disk failure. The backup appliance must be offered with HOT swappable drives.	A purposed built backup appliance (PBBA)always write the backup data in a deduplicated mode and it the application specific format. Hence request you to accept the requested change.	Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21
2(k)	(k) For disaster recovery purposes, it should be possible to remove any individual Disk or Tape and recover media files using an external computer without special software	For disaster recovery purposes, it should be possible to remove any individual Disk or Tape and recover media files using an external computer with backup software. The PBBA must be offered with HOT swappable drives.	A purposed built backup appliance (PBBA)always write the backup data in a deduplicated mode and it the application specific format which is not readable by any other software. Hence request you to accept the requested change.	Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21
2(l)	(t) The security of the Archive So shall be based on keeping at least two Replicas of every media file by	The Proposed PBBA must maintain data security for the	Data security of the backup data cannot be just maintained by keeping	Refer Page 12-15 of corrigendum on

	default with the option to keep a third replica of strategically important content, or a single replica where the storage is deemed to be a backup volume, on a user selectable basis.	backup data by supporting retention lock (WORM) feature which ensures that no data is deleted/modified accidentally. Even Administrator should not be able to delete the data deliberately or accidentally till the retention of the backup get expired. Once this data is replicated to DR/Secondary site, no additional licenses must be required at DR site to maintain retention lock on replicated data.	multiple copies. The backup data mounted on NFS/CISF shared can be deleted by anyone with access. Hence additional layer of data security must be maintained by PBBA.	RFP issued vide 01 Mar 21
2(m)	(m) The power budget for the Archive storage shall not be more than 1.5 Watts per useable Terabyte of Storage capacity in normal operation, to minimize power consumption and A/C provisioning.	The proposed purpose built backup appliance must write the backup data in the deduplicated format to help with reduction in the storage capacity, Power & cooling requirement for the proposed solution. Data must not rehydrate while replicating to the secondary/DR site.		Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21

2(n)	(n) Suppliers should specify the expected operational disk life. Disk life and replacement cost will be taken into account as part of the total lifetime cost of ownership of the quoted Archive Solution.			Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21
2(o)	Vault Management should be supplied with Third party IT standard Server as per the Archive Vault Management Designing.	Please remove this clause as it is tape library specific & not the asked backup solution of backup software & disk based backup appliance.	This is a Tape library specifications	Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21
2(p)	The system shall be capable of integrating with Media Management Applications at low level using a publicly available and license-free API. All functions of the Archive shall be accessible through the API including Partial File Restore for specified formats.			Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21
2(q)	Optionally the system shall be capable of integrating with Media Management Applications at a high level using a Virtual File System which shall emulate a NFS / SaMBa / CIFS file system and should support FTP, FXP and Vendor Specific protocols listed separately. Where this approach is offered, the Virtual File System shall be capable of creating the necessary file replicas to meet the requirements of section 10 above.	Proposed disk based backup appliance should be able to interface with various industry leading server platforms, operating systems and Must support LAN/SAN based D2D backup and VTL backup simultaneously via NFS v3, CIFS, FC , OST and NDMP	Purpose built backup appliances rely on the efficient & secure data protection protocols like VTL & OST along with the standard storage protocols line NFS & CIFS. OST protocol helps in source based deduplication that reduces the backup & restore window for any environment.	Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21

		protocols. Proposed appliance should support global and inline data duplication using automated variable block length deduplication technology.		
2(r)	Where a high-level Virtual File System approach is offered, the file system shall be maintained in dual fault tolerant RAID storage with the option for dual redundancy. The Virtual File System shall also be capable of using a share on an existing Near-Line storage system as the Cache.	The proposed purpose built backup appliance must use RAID 6 & Hot spare in each enclosure. The appliance should support backup standard protocols like CIFS,NFS,OST & VTL simultaneously. Proposed appliance should support global and inline data duplication using automated variable block length deduplication technology.	Purpose built backup appliances rely on the efficient & secure data protection protocols like VTL & OST along with the standard storage protocols like NFS & CIFS. OST protocol helps in source based deduplication that reduces the backup & restore window for any environment.	Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21
2(s)	Proposed System should be able to create and managed Shelf / Vault workflow as a Copy of Last Resort for all, or strategically important static parts of the Archive Solution.	Please remove this clause as it is tape library specific & not the asked backup solution of backup software & disk based backup appliance.	This is a Tape library specifications	Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21

2(t)	Vault Management should be supplied with Third party IT standard Server as per the Archive Vault Management Designing.	Please remove the clause as this is only applicable for tape media		Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21
2(u)	Vault Management system should be supplied by QR Code Printer and Android Tablet scanner. Printer & Tablet should be certified by the Archive Solution OEM.	Please remove this clause as it is tape library specific & not the asked backup solution of backup software & disk based backup appliance.	This is a Tape library specifications	Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21
2(v)	(v) Main Archive Storage unit can be expandable with 10 Expansion as scale up and can add multiple Main Archive Chassis to increase the required throughput and Scale out capacity with multiple Storage Arrays.	The proposed purpose built backup appliance should be offered with minimum 10X of data deuplication & should have the capability to complete the XX TB of data backup in 4/8 hours. The proposed appliance should have the 2x scalability of the proposed storage capacity.		Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21
2(w)	(w) All the Units should have at least 4U Rack Space			Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21
2(x)	(x) The offered Archive Solution should offer minimum of 12TB Raw Capacity supported in a Single Node Array with 3.8/7.6 TB per slots combination.	The offered purpose built backup appliance must be offered with 120 TB of usable capacity by using 4 TB disks in	The purpose built backup appliances work on multiple data protection protocol. The current clause is not inline to the backup requirement.	Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21

		each enclosure. The proposed backup solution must be physically different from HCI solution. Thus maintaining a segregation among production data & backup data.		
2(y)	(y) Solution should be offered with 3 Years Warranty + 5 Extended Warranty / Comprehensive AMC.			Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21
	New	Request to Add	Proposed solution should support backup of various OS platforms like Windows, Linux and Unix and should provide integrated view of backup, archival and replication.	Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21
	New	Request to Add	The offered software must support application aware backups for MS SQL, Oracle, MySQL, PostGreSQL, Exchange, Share-Point etc. Software should work with both standard and enterprise Database editions.	Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21
	New	Request to Add	The offered software must have compatibility to perform agentless backup for all the editions of Windows Server 2019 Hyper-V environment, Nutanix Hypervisor,	Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21

			VMware 6.5 and above and RHEV 7.1 and above.	
	New	Request to Add	The proposed backup software should be independent of storage hardware and should provide all functionality listed here for various major storage technology like Dell-EMC, HPE, Hitachi, NetApp, IBM etc.	Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21
	New	Request to Add	Proposed backup solution should be able to protect the backed up disk volume from Ransomware.	Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21
	New	Request to Add	Backup software must support both source side and target side deduplication and this feature should work with various disk storage vendors.	Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21
	New	Request to Add	The proposed software must provide Global deduplication across all backup jobs and different Workloads across various storage OEM vendor.	Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21
	Missing Component in the Backup Solution	We did not find any Backup Application Software in the tender which is mandatory to deploy the required workflow of the Backup solution.	Request adding the Backup Application Software as part of the Tender Specs.	Refer Page 12-15 of corrigendum on RFP issued vide 01 Mar 21
SAN SWITCHES				

NA	SAN Switches - 12 qty	Need Clarification	Please help us clarify on the number of SAN Switches since the storage asked is only on 5 sites which ideally means that number of SAN Switches should be 10.	SOR changed to Qty – 10. Refer Page 02 of corrigendum on RFP issued vide 01 Mar 21
TOR / VX LAN SWITCHES				
1	Generic Objective. Datacenter solution proposed fabric must be the close network two tier hierarchical topology architecture defined using Core (also referred as Spin) and top-of the-rack (TOR) (also referred as Leaf switches) with VXLAN (RFC7348) overlay. Network fabric must provide REST APIs from the Central management appliance / SDN Controller in order to integrate with popular Management, Monitoring, Hypervisor and Infrastructure automation software. There are two types of switches which are required to be supplied as part of this project. Type I is 48 port TOR switch with 48*10/25 G and 6*40/100 G , Type II is 36 port VX LAN switch with 36* 40/100 G.	Generic Objective. Datacenter solution proposed fabric must be the close network two tier hierarchical topology architecture defined using Core (also referred as Spin) and top-of the-rack (TOR) (also referred as Leaf switches) with VXLAN (RFC7348) overlay. There are two types of switches which are required to be supplied as part of this project. Type I is 48 port TOR switch with 48*10/25 G and 12*40/100 G , Type II is 36 port VX LAN switch with 36* 40/100 G.	Please remove controller based closed solution specs for interoperable solution. more uplinks to achieve line-rate fabric performance with zero over-subscription when required. These ports can also be used to connect downstream Chassis over 100G links in future.	Refer Page 16-17 of corrigendum on RFP issued vide 01 Mar 21
2 (e)	Multi-Datacenter Design. The proposed architecture should be	Multi-Datacenter Design. The	Please remove controller based closed solution	Refer Page 16-17 of corrigendum on

	extensive to multiple data centers and should have single management controller to push consistent policies across all the sites.	proposed architecture should be extensive to multiple data centers	specs for interoperable solution and wider participation.	RFP issued vide 01 Mar 21
2(D)	Deterministic Latency - The proposed fabric must provide predictable latency between any two endpoints connected to the fabric		Please provide predictable latency between any two endpoints connected to the fabric (VX LAN Switch) or it should be default to OEM Switch	Refer Page 16-17 of corrigendum on RFP issued vide 01 Mar 21
4	In case the fabric controller licenses have dependency on number of Core switches or TOR switches or Server Cores or Server Sockets or VMs or L4 to L7 devices with requisite licenses for the all the ports/ cores to be provisioned by the OEM without any financial implication to CoR from day one.	-	please remove this clause	Refer Page 16-17 of corrigendum on RFP issued vide 01 Mar 21
6 (b)	Fabric must auto discover all the hardware and auto provision the fabric based on the policy.	-	please remove this clause	Refer Page 16-17 of corrigendum on RFP issued vide 01 Mar 21
6 (f)	Fabric must integrate with different virtual machine manager viz. VIMWare vCenter, RHEL Openstack ,hyper V etc. and manage virtualize networking from the single pane of Glass - Fabric Controller/ SDN Controller.	-	please remove this clause	Refer Page 16-17 of corrigendum on RFP issued vide 01 Mar 21
6 (h)	Fabric must integrate with popular L4 - L7 physical and virtual appliances e.g. ADCs, NGFW etc" and manage using- Fabric Controller/ SDN Controller.	-	please remove this clause	Refer Page 16-17 of corrigendum on RFP issued vide 01 Mar 21

6 (i)	Fabric must provide deeper visibility into the fabric in terms of latency and packet drop between any two endpoints on the fabric.	-	please remove this clause	Refer Page 16-17 of corrigendum on RFP issued vide 01 Mar 21
7 (a)	Fabric must have policy models starting hosts to help in protecting against any kind of attacks like Unauthorized Access, man-in-the-middle- attack, Replay Attack, Data Disclosure, Denial of Service.	-	please remove this clause	Refer Page 16-17 of corrigendum on RFP issued vide 01 Mar 21
7 (b)	Fabric must provide RBAC policies and support AAA using Local User authentication, External RADIUS, External TACACS+, External LDAP, External AD.	-	Fabric must provide RBAC policies and support AAA using Local User authentication, External RADIUS, External TACACS+	Refer Page 16-17 of corrigendum on RFP issued vide 01 Mar 21
7 (C)	Fabric must support VM attribute based zoning and policy	-	please remove this clause	Refer Page 16-17 of corrigendum on RFP issued vide 01 Mar 21
7 (d)	Fabric must support Micro Segmentation for the Virtualize and Non- Virtual ize envi ronment.	-	please remove this clause	Refer Page 16-17 of corrigendum on RFP issued vide 01 Mar 21
7 (e)	Fabric must support true multi-tenancy	-	please remove this clause	Refer Page 16-17 of corrigendum on RFP issued vide 01 Mar 21
8 (a)	Fabric must provide Centralized Management Appliance or SDN Controller - for managing, monitoring and provisioning the entire Fabric within Data Center & across all Data Center.	-	please remove this clause	Refer Page 16-17 of corrigendum on RFP issued vide 01 Mar 21
8 (b)	Fabric must Auto discover all the Spine and Leaf switches and auto	-	please remove this clause	Refer Page 16-17 of corrigendum on

	provision them based on the Fabric policy using Centralized Management appliance or SDN Controller.			RFP issued vide 01 Mar 21
8 (c)	Centralized management appliance or SDN Controller must provide necessary report for compliance and audit.	-	please remove this clause	Refer Page 16-17 of corrigendum on RFP issued vide 01 Mar 21
8 (d)	Centralized management appliance or SDN Controller must communicate to south bound devices using open standard protocol i.e. OPFLEX/ OPENFLOW /OVSDB/ NETCONF etc. or using Device APIs.	-	please remove this clause	Refer Page 16-17 of corrigendum on RFP issued vide 01 Mar 21
8 (e)	Centralized management appliance or SDN Controller must run in "N + 1" redundancy to provide availability as well as function during the split brain scenario.	-	please remove this clause	Refer Page 16-17 of corrigendum on RFP issued vide 01 Mar 21
8 (f)	In Event of all Centralized management appliances or SDN Controllers fails, the fabric must function without any performance degradation and with the current configuration.	-	please remove this clause	Refer Page 16-17 of corrigendum on RFP issued vide 01 Mar 21
8 (g)	Centralized management appliance or SDN Controller must support multi tenancy from management perspective and also provide Role Based Access Control per tenant for the tenant management.	-	please remove this clause	Refer Page 16-17 of corrigendum on RFP issued vide 01 Mar 21
8 (h)	All infrastructure required by fabric controllers i.e. licenses, hardware, software etc. to support the listed features and scale, should be provided by the OEM.	-	please remove this clause	Refer Page 16-17 of corrigendum on RFP issued vide 01 Mar 21

SMART RACK				
10	Sturdy frame section construction, consisting of multi folded 16 folded 16- Fold rolled hollow frame section punched in 25mm DIN pitch pattern. Removable top and bottom cover with cable entry provision. Frames should be bayable, scalable and modular. Should be interchangeable at site within DCs. Must comply with all the leading Industry standards yye ISO 9001,14001,1800&UL2416,UL60950-1, Listed complying EIA 310,DIN 41494 and IEC 297 standards.	Please confirm if you need 1.Access Control System 2,Power Distribution Arrangement at Site 3.Fan Tray in Rack,		Refer Page 18-19 of corrigendum on RFP issued vide 01 Mar 21
ADC & WAF				
Traffic Ports	6 x 40 GbE QSFP+ 12 x 10 GbE SFP+ (2 x 40G, 6 x 10G, 4x1G populated from Day-1	"4 x 40 GbE QSFP+ 12 x 10 GbE SFP+ (2 x 40G, 6 x 10G, 4x1G populated from Day-1"	min 6 x 40 GbE QSFP+ 12 x 10 GbE SFP+ (without use of Breakout Cables) (2 x 40G, 6 x 10G, 4 x 1G populated from Day-1)	Refer Page 20 of corrigendum on RFP issued vide 01 Mar 21
Device L4 throughput		<i>Request to change the clause as: "150 Gbps"</i>	As we have not asked for any scalability in terms of number of L4 connections per second or L7 request per second, how would throughput increase without increasing the connections, both should be in proportion hence either number of connections should be also made scalable?	Refer Page 20 of corrigendum on RFP issued vide 01 Mar 21
SSL throughput		<i>Request to change the clause as: "SSL throughput of 65 Gbps and</i>	As we have mentioned about the SSL	No Change

		<i>ECC TPS of minimum 110K and RSA TPS of minimum 190K”</i>	throughput, which is on the lower side considering the total throughput, since we all know that HTTPS is increasingly used, and the department would require more secure transactions understanding the attack from neighbor countries and criticality of data and nature of the applications of defense. Also, it is strange that only SSL throughput is mentioned without any TPS, how would throughput be possible when no SSL connections (also all OEM mention this in Datasheets). We need to mention as otherwise that can be bottle neck. So, since we have asked for 4 million I7 connections atleast close to 5 percent should be count for SSL RSA TPS understanding that out of total Web traffic 5% would be HTTPS !	
--	--	--	--	--

Virtualization	The proposed device should have hypervisor based virtualization feature that virtualizes the device resources—including CPU, memory, network and acceleration resources.	<i>Request to change the clause as:</i>	Since we have asked for virtualization of network and in the RFP, its mentioned 6 x 40 GbE QSFP+ 12 x 10 GbE SFP+ (, which means total 18 interfaces, how can we virtualize these across 60 virtual instances? So, considering other resource parameters as well, 60 is on very higher side as well as standard network does not have these many segments.	Refer Page 20 of corrigendum on RFP issued vide 01 Mar 21
Redundancy	The Proposed Device should support Standard VRRP (RFC-2338), for High Availability purpose (no proprietary protocol)	“The Proposed Device should support Standard VRRP (RFC-2338), for High Availability purpose or equivalent”	Since by redundancy we need to achieve the appliances should support High Availability in the network. Different OEMs use different Operating systems and protocols, to optimize the failover downtime etc, hence equivalent protocols should be allowed as there is advantage to it and no disadvantage.	No Change
TOWER SERVERS				
Capacity of Drive	2 TB or more	We understand that 2x2TB SSD is required, please confirm	No Change	Capacity of Drive (Primary Storage)

(Primary Storage)				
Number of drives	2	We understand that 2x2TB SSD is required, please confirm	No Change	Number of drives
Type of Ethernet Ports	Dual Gigabit NIC 10/100/1000	Here Dual Gigabit NIC is required	No Change	Type of Ethernet Ports
Number of Ethernet Ports	4	Here Quad Gigabit NIC is required, which one is correct?	NOT REQUIRED	Number of Ethernet Ports
Number of VGA Ports	01 or more	No direct VGA shall be available. We shall provide Display Port to VGA Port Dongle - Please change it to Display Ports	DISPLAY PORT DUAL	Number of VGA Ports
Specifications for Tower Servers	Operating System (Factory Preloaded) : Windows 10 Professional 64 Bit	Windows 10 is desktop operating system and not supported on server. Request to change it to Microsoft Windows Server 2019	No Change	Specifications for Tower Servers
Response time	5 millisecond	6-8 MS	Refer Corrigendum	Refer Page 20 of corrigendum on RFP issued vide 01 Mar 21
Expansion Slots (PCIe x 16) = 04 or more	Request you to ask for " 2 PCIe x16, 3 PCIe x4, 1 PCIe x8 (All Gen3 Ports) "	Request the kind authorities to amend this so that customer can get more competitive bids	2 PCIe x16, 3 PCIe x4, 1 PCIe x8 (All Gen3 Ports)	Expansion Slots (PCIe x 16) = 04 or more
RAM Expandable upto (GB) = 3072 GB	Request you to ask for "768 GB or more"	Request the kind authorities to amend this so that customer can get more competitive bids	768 GB OR MORE	Refer Page 20 of corrigendum on RFP issued vide 01 Mar 21

Number of VGA Ports = 01 or more	Request you to give option for "Through DP to VGA adaptor" to achieve the same.	Request the kind authorities to amend this so that customer can get more competitive bids	DISPLAY PORT DUAL	Number of VGA Ports = 01 or more
DESKTOP PCs				
	Chipset Series	Intel Q Series	We suggest to ask for entry level Workstation with "Intel W Series" Chipset because 16GB Graphics Cards may not be compatible with the Desktop PCs. It may not be able to manage the heat dissipation within the system as well as the acoustics, and would not be able to deliver the required performance in Q Series Desktop Chipset.	Q SERIES
	Chipset Generation	Intel Q 470	We suggest to ask for entry level Workstation with "Intel W480" Chipset Generation because 16GB Graphics Cards may not be compatible with the Desktop PCs. It may not be able to manage the heat dissipation within the system as well as the acoustics, and would not be able to deliver the required	

			performance in Q Series Desktop Chipset.	
	Expansion Slots (PCI x 1) (Number)	01 or more	Please remove PCIe x1	PLS REMOVE
	Cache	22MB	The asked CPU "Intel Core i9-10900" do not have Cache beyond 20MB	Refer Page 20 of corrigendum on RFP issued vide 01 Mar 21
	Graphics card	NVIDIA QUADRO RTX 2070 16 GB or more	The asked Graphics Card is the Consumer Grade Graphics Card. The Recommended System Power of such cards are 550W which may not be possible in Desktop PCs with Small Form Factor. The lead time of 1000+ Consumer Grade Graphics Card would be not less than 12 Weeks. The Consumer Graphics Card have higher failure rate. Also the asked NVIDIA QUADRO RTX 2070 is 8GB Card and not 16GB Card. We suggest to ask for Professional Graphics Card "Nvidia Quadro RTX 5000, 16GB".	Refer Page 20 of corrigendum on RFP issued vide 01 Mar 21

			Which can be more reliable and sustainable for the required application.	
	Storage SSD	1TB	Please confirm that the requirement is 1TB SSD + 1TB HDD or only one SSD	1TB SSD + 1TB HDD
	HDD Capacity (GB)	1TB	Please confirm that the requirement is 1TB SSD + 1TB HDD or only one HDD	1TB SSD + 1TB HDD
	Cabinet volume	08 or Lower	Minimum 20.41 L Cabinet Volume is required for the asked configuration.	Refer Page 20 of corrigendum on RFP issued vide 01 Mar 21
	Cabinet Form Factor	SFF (7 to 8)	Minimum Tower Cabinet Form Factor is required for the asked configuration. SFF may not be sufficient for the asked configuration.	Refer Page 20 of corrigendum on RFP issued vide 01 Mar 21
	Audio-in	Yes	It's not available	OK
	Number of VGA Ports (CPU)	01 or more	VGA Port shall be only through DP to VGA adapter. Direct VGA in the system would not work with Graphics Card Installed.	DISPLAY PORT DUAL
	Number of HDMI Ports (CPU)	01 or more	HDMI Port shall be only through DP to HDMI adapter. Direct HDMI in the system	REQUIRED

			would not work with Graphics Card Installed.	
	Desktop and Tower Server		Please share the location wise quantity of desktop and Tower server .	This would be six nodal locations across India. Details would be shared to successful bidder
ADDL MONITORS FOR TOWER SERVERS				
	Antiglare Coating	No	Yes	YES
	HDMI port	Available	VGA - Please add VGA	DUAL DISPLAY PORT ALONG WITH HDMI PORT IS REQUIRED
	Graphic Card	NVIDIA QUADRO RTX 2070 16GB or more	NVIDIA GeForce® RTX 2080 Super 8GB	NVIDIA GeForce® RTX 2080 Super 8GB
	Cabinate Volume	08 or lower	19.14 litres	OK
	Cabinate Form Factor	SFF (7 to 8)	Tower	OK
	Audio-in	YES	NO	OK
	Audio-Out	Yes	YES	
	Number of VGA Ports (CPU)	01 or more	please remove this clause	OK
	RAM Expandable upto (GB)	3072 GB or more	768 GB or more	OK
	Number of VGA Ports	01 or more	Through DP to VGA adaptor	DISPLAY PORT REQUIRED DUAL
	Number of RAID Controller Ports	8	6 or more	OK
UPS SPECIFICATIONS				

	Technology (1KVA and 2KVA)	IGBT- PWM with inbuilt isolation transformer	Transformer not required in new technology UPS Systems. Hence requested to delete this parameter.	Refer Page 20 of corrigendum on RFP issued vide 01 Mar 21
	Input power (1KVA and 2KVA)	Single phase 160V - 260V sinewave , 50Hz	Input Range shall be 175V to 280V on full load of 0.9PF	OK
	Min VAH (2KVA)	1600 or more	Shall be min. 2000VAH instead of 1600VAH	OK
	Min VAH (1KVA)	800 or more	Shall be min. 1000VAH instead of 800VAH	OK
	Degree of protection (1KVA and 2KVA)	IP 21	IP 21 also to be changed to IP 20	OK
	Single phase 160V - 260V sinewave , 50Hz	Request the kind authorities to amend "Input Range shall be 175V to 280V on full load of 0.9PF"	Request the kind authorities to amend this so that customer can get more competitive bids	OK
	Certifications (mandatory)	BIS ,ISO 9001 , 14001 and OHSAS 18001,ROHS,CE,PeP	As per the Guidelines of GOI, the product should have minimum harmful substances for environment and its very much environmental friendly when it will be decompose after EOL.	CERTIFICATION MANDATORY
	EMC	EN 62040-2	These certifications are required for Safety and Performance of the required Device.	YES REQUIRED
	Safety	EN 62040-1,IS 16242-Part1		
	Proformance	IEC 62040-3		

	OEM Criteria Clause	OEM criteria/ Service Centers / Turnover		
		ISO 9001, 14001 and 45001/50001 also shall be asked for both 1 kva and 2kva	Request the kind authorities to amend this so that customer can get more compititive bids	
		Kindly incorporate below points in the specs : UPS Shall be Rack mountable Online Double Conversion Technology Input PF (0.99)O/p P.F(0.9), Operating Temp(0 to 40 deg C), LCD display, USB port	Request the kind authorities to amend this so that customer can get more compititive bids	NOT REQUIRED
		Factory calibration lab of manufacturer should be NABL accredited in India.	Request the kind authorities to amend this so that customer can get more compititive bids	
	Preference of Make In India Product		Make in India point as per goverenment of india guidelines	Preferred
CABLING AND FIC				
Page no 60	Cabling (As Reqd)	What kind of Cabling is been referred to? Tender spec doesn't have any cabling Specifications		No Change
Page no 60	Regarding Pigtails	As there is no Spec of Pigtails , Should We Consider FDF as fully Loaded with Pigtails & Splice Holders		No Change. No Pig tails are envisaged
Page no 60	FDF & Fibre Patchcords	Single Mode or Multimode, Kindly Clarify.		Refer Page 21 of corrigendum on RFP

				issued vide 01 Mar 21
Page no 60	LC -LC Fibre Patchcords are factored separately in the Tender Spec for TOR Switches & VX LAN, Qty of these switches as per BOQ is 20. Whereas the Qty of FDF is only 10.	Kindly clarify . Should we consider 48 Pair FDF 10 Nos for TOR switch & 36 Pair FDF 10 Nos of VX LAN Switch.		Refer Page 21 of corrigendum on RFP issued vide 01 Mar 21
Page no 60	SAN Switches , Qty 12. No FDF/ LC LC Patchcords is been factored for SAN switches in RFP.	Do we need to consider any connectivity for SAN switches, Please clarify.		No Change. Refer Para 20 of SOW at Page no 19 of RFP dated 19 Feb 21
APPLICATION AND NETWORK MONITORING				
22	Number of flows per minute not exceeding 1.5 Million should be licensed from Day 1		Is this license of 1.5 Million Flow analysis/minute for Data Centre only or it is a combine of Data centre and Data Recovery site also. Kindly clarify	Refer Page 21-23 of corrigendum on RFP issued vide 01 Mar 21
23	Assuming there are 50 capture points with max upto 30k flow analysis per minute per site		Is this 50 capture points with max 30k flow analysis per minute per site are only for Data Centre where license of 1.5 Million will be implemented or it's a total of 50 capture points including DC and DR . Kindly clarify	Refer Page 21-23 of corrigendum on RFP issued vide 01 Mar 21
24	Qty 60 Sensors for 1GbE smart SFP -FPGA ,Multimode ,850nm,550m		Kindly clarify if this 60 sensors for 1GbE	Refer Page 21-23 of

			smart SFP -FPGA ,Multimode ,850nm,550m will be sending data to Data Centre analytic only or there are any additional sensors need to be considered from a compute/storage requirement on analytic layer ?	corrigendum on RFP issued vide 01 Mar 21
25	Qty 20 Sensors for 1GbE smart SFP -FPGA ,RJ45 copper		Kindly clarify if this 20 sensors for 1GbE smart SFP -FPGA ,RJ45 copper will be sending data to Data Centre analytic only or there are any additional sensors need to be considered from a compute/storage requirement on analytic layer ?	Refer Page 21-23 of corrigendum on RFP issued vide 01 Mar 21
26	Qty 20 Sensors for 10 GigE SFP+ ,single Mode .1310 nm, 10km ,LC connector		Kindly clarify if this 20 sensors for 10 GigE SFP+ ,single Mode .1310 nm, 10km ,LC connector will be sending data to Data Centre analytic only or there are any additional sensors need to be considered from a	Refer Page 21-23 of corrigendum on RFP issued vide 01 Mar 21

			compute/storage requirement on analytic layer ?	
	Generic		The Supplier/bidder should exclude any server hardware/VMs required to run the Application and Network monitoring solution . Is our understanding correct ?	Refer Page 21-23 of corrigendum on RFP issued vide 01 Mar 21
VA TOOLS				
Pg 78	Database scanning Coverage	7. NA	Request to clarify the requirement	Refer Page 24 of corrigendum on RFP issued vide 01 Mar 21
EEP & HIPS/ AV				
<u>P 84 Pt 5 SECURITY SOLUTION FOR EPP/HIPS AND AV</u>	Endpoint based EDR solution to protect all the endpoints across Network from Advanced Targeted Attacks and APT's	Clause must be read as proposed below: The proposed solution shall be proposed with layered approach keeping in view the defense in depth security architecture framework. Buyer intends to procure below key capabilities and solution areas as an enterprise grade, dedicated solution to secure deployed infrastructure. 1. Endpoint Protection (EPP), 2. Endpoint Detection and Response (EDR), 3. Data Loss Prevention (DLP)	As per Defense in Depth Architecture and other best practices for Enterprise security, it is expected that the proposed solution must utilize a layered defense in depth approach, wherein the solution must not be of the same nature as at various levels and layers of security solutions. We request to	Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21

		4. Host Intrusion Prevention System (HIPS) Solution from the same OEM could be agreed on three major areas viz; 1. Known Threat Prevention(EPP) 2. Data Security viz Data Loss (DLP) 3. Endpoint Detection & Response viz EDR The proposed solution must confirm to specifications and features as mentioned in detailed specifications below	incorporate the changes as recommended in changed clause	
P 79 Pt 4	4. HIPS solution must be sized for 1000 endpoints. Bidder needs to provision for the incremental licenses up to 1000 endpoints to meet the futuristic requirements of Buyer as part of solution.		Are we talking about 1000 server nodes since you have asked for support for Windows server, Linux, RHEL, Virtualization platforms, openstack, etc. Kindly confirm. Also confirm if the bidder need to quote for the incremental 1000 server nodes licenses.	Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21
P 79 Pt 5	Host Intrusion Prevention System (HIPS) Feature	The Solution must offer anti-malware, firewall, application control, change control, HIPS, network visibility and micro-segmentation based firewall and virtualization security in a single	We request you to add file integrity monitoring along with change control as term "change control" is OEM specific. Clause should read as:	Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21

		agent functionality to ensure optimal security and compliance for critical servers.	The Solution must offer anti-malware, firewall, application control, change control/File Integrity Monitoring , HIPS, network visibility and micro-segmentation based firewall and virtualization security in a single agent functionality to ensure optimal security and compliance for critical servers.	
P 79 Pt 5	The solution must offer anti-malware, firewall, application control, change control, HIPS, network visibility and micro-segmentation based firewall and virtualization security in a single agent functionality to ensure optimal security and compliance for critical servers.	Clause should read as : "5. The solution must offer anti-malware, network visibility and virtualization security in a single agent functionality to ensure optimal security and compliance for critical servers."	The Host Security Solution for Servers is part of our EDR functionality. However, functions like Application control, Firewall, micro-segmentation etc is not part of Host intrusions functionalite which are typically part of EPP category of solutions We will provide Solution for Known & Unknown threats and Application Exploit detection & prevention aongwith fully funcitonal EDR capabilities.	Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21
P 79 Pt 9	The solution must offer true zero day protection along with application containment, application and change	Clause should read as : The solution must offer true zero day protection along with	File Integrity Monitoring is not part of HIPS. FIM solutions are a dedicated	Refer Page 25-31 of corrigendum on RFP

	control, file integrity monitoring for zero day malware prevention	application containment, application exploit prevention, monitoring for zero day malware detection & prevention	functionality and not HIPS functionality Kindly remove the File Integrity monitoring requirement	issued vide 01 Mar 21
P 80 Pt 13	Host Intrusion Prevention System (HIPS) Feature	The Solution must be able to block unauthorized changes to critical system files, directories and configurations	Due to limitaions to straight away block the changes in file system, we recommend to put the solution under detection mode rather then blocking mode w.r.t change control module. Hence we request you to ammend the clause as below: Clause Should read as: The Solution must be able to detect/block unauthorized changes to critical system files, directories and configurations	Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21
P 80 Pt 13	The solution must be able to block unauthorized changes to critical system files, directories, and configurations	Clause should read as : The solution must be able to detect, alert & prevent unauthorized malicious changes to critical system files, directories, and configurations	Not all activities are to be blocked as this can impact the business operations. Any solution must be able to detect & then prevent activities based on confidence and risk of malicoousness. We request to change the clause as proposed	Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21

P 80 Pt 14	Host Intrusion Prevention System (HIPS) Feature	The Solution must protect against system misconfigurations	Since this is OEM specific clause, hence we request you to remove this clause	Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21
P 80 Pt 15	Host Intrusion Prevention System (HIPS) Feature	The Server Security solution must have HIPS control to restrict application and operating system behaviour using policy-based least privilege access control	Since this is part of Privilege access management solution, hence we request you to remove this clause from HIPS solution	Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21
P 80 Pt 15	The Server Security solution must have HIPS control to restrict application and operating system behaviour using policy-based least privilege access control.	Clause should read as : The Server Security solution must have HIPS control to restrict malicious application and operating system using application control and behavior analysis	This clause favours single OEM in nature and not allowing our participation. Hence request you to please allow us to participate by amending this clause.	Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21
P 80 Pt 16	Server agent must prevent malicious applications from inserting code into trusted applications. The HIPS, HIDS, file integrity monitoring, host based firewall, application control should be offered using a single agent.	Clause should read as : Server agent must prevent malicious applications from inserting code into trusted applications. The intrusion detection & prevention alongwith continuous system monitoring for malicious activity detection, Exploit prevention should be offered using a single agent.	File Integrity Monitoring is not part of HIPS. FIM solutions are a dedicated functionality and not HIPS functionality. Likewise, Firewall, Application control are also EPP functionalities which some vendors bundle together in their solutions. Please allow the	Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21

			amendment for us to be able to bid for the solution	
P 80 Pt 17	Host Intrusion Prevention System (HIPS) Feature	The Solution must provide the dynamic management of execution capability of applications on a server system, prevent unauthorized registry manipulation and in memory protection of application	Kindly clarify on execution capability of application	Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21
P 80 Pt 18	Host Intrusion Prevention System (HIPS) Feature	The Solution apart from allowing only authorized applications to run, should block any changes from being done to authorized applications like DLL's, system files, registry etc. thus providing application threat protection	As HIPS solution, we can detect for any unauthorized changes to registry files, registry values, process, services & files. Blocking action needs to be taken at administrative level. Also considering HIPS solution, asked features related to change control is part of different solution. Hence we request you to kindly exclude change control specs from HIPS solution.	Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21
P 80 Pt 19	Host Intrusion Prevention System (HIPS) Feature	The Solution must ensure that only authorized software/applications/executables codes are allowed to run and provides tamper protection to them. Solution must be capable of creating whitelist for each system dynamically and no manual intervention in creating the list	As HIPS solution, we can detect for any unauthorized changes to registry files, registry values, process, services & files. Blocking action needs to be taken at administrative level. Also considering HIPS solution, asked features related to change control is part of different solution. Hence we	Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21

			request you to kindly exclude change control specs from HIPS solution.	
P 80 Pt 25	Host Intrusion Prevention System (HIPS) Feature	The proposed change control solution must support real-time change tracking of files and registry. Audit log should include file, user information, program name and contents that have changed	As HIPS solution, we can detect for any unauthorized changes to registry files, registry values, process, services & files. Blocking action needs to be taken at administrative level. Also considering HIPS solution, asked features related to change control is part of different solution. Hence we request you to kindly exclude change control specs from HIPS solution.	Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21
P 80 Pt 26	Host Intrusion Prevention System (HIPS) Feature	The proposed change control solution must be capable of change monitoring as well as control/prevention	As HIPS solution, we can detect for any unauthorized changes to registry files, registry values, process, services & files. Blocking action needs to be taken at administrative level. Also considering HIPS solution, asked features related to change control is part of different solution. Hence we request you to kindly exclude change control specs from HIPS solution.	Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21
P 81 Pt 28	The solution must offer intelligent filters which are pre-configured or	Clause should read as : The solution must offer intelligent	We have multiple engines including a	Refer Page 25-31 of

	configured using professional services to track the relevant objects on the system, for each standard operating system covering systems files including Windows, Linux. It should also include application filters for Apache, Tomcat, Websphere and JBOSS, IIS, Weblogic, Websphere etc	filters or engines which are pre-configured or can be configured to track the relevant objects on the system, for each standard operating system files including Windows, Linux. If only filtering mechanism is used solution should also include application filters for Apache, Tomcat, Websphere and JBOSS, IIS, Weblogic, Websphere etc	dedicated Machine learning and Exploit Guard engine for application detection and prevention purpose. The analysis of application access, executables, processes etc is done on continuous basis and checked against exploits or any such unknown behaviours without any filtering or rules to be created. Any known attack behaviours can also be detected and prevented. We do not need any specific Filters or patterns for applications hence no overloads or professional service requirements. The clause asked is typically asking for an onpremise signature/pattern development to filter application traffic. This is dependent on manual intervention and hence prone to	corrigendum on RFP issued vide 01 Mar 21
--	---	--	--	---

			threats getting bypassed or missed. We recommend to adopt the amended clause.	
P 81 Pt 3	The solution must be able to manage EPP/ HIPS, EDR and encryption solution centrally through common or separate management console.	Clause to be read as: The vendors positioning their unified solution must be able to manage EPP and encryption solution centrally through common or separate management console. The EDR & HIPS solution must have its own management through common or separate management console with no dependency on EPP.	The clause support a single OEM and provides edge and preference to such vendors. Requets to amend the cluse	Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21
P 81 Pt 30	Solution must offer granular read, read-write or no access to identified process or users.			Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21
P 81 Pt 31	Solution must mitigate patching for new and legacy systems and enable application and instance level security.			Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21
P 81 Pt 32	Solution must have host firewall to control inbound and outbound network traffic to and from servers			Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21

P 81 Pt 34	HIPS must support firewall capabilities to directly block unwanted traffic			Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21
P 81 Pt 38	The solution must be able to manage application control, change control and policy auditing solution from a single management console.	Clause should read as : The solution must be able to manage HIPS detection & prevention features from a single management console at DC & DR.	Change control and policy auditing features are not HIPS functionality. This clause favour single OEM and not allowing our participation. Hence request you to please amend this clause.	Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21
P 82 Pt 1	Introduction. The Central Management System (CMS) must be supplied with Endpoint Protection (EPP)/ Host Intrusion & Prevention System (HIPS}, Endpoint Detection & Response (EDR), as part of comprehensive Endpoint Security Solution and must be able to support management of supplied solutions from remote central locations. It must offer following of configuration management of devices as described in subsequent paragraphs. The proposed solution architecture for CMS must be designed for high-availability and there should not be any single point-of-failure. The solution architecture must be	Clause to be read as: Introduction. The Central Management System (CMS) must be supplied with Endpoint Protection (EPP)/ Host Intrusion & Prevention System (HIPS}, Endpoint Detection & Response (EDR), as part of comprehensive Endpoint Security Solution and must be able to support management of supplied solutions from remote central locations. It must offer following of configuration management of devices as described in subsequent paragraphs. The proposed solution architecture for CMS must be designed for high-	EDR by its design is a tool designed for centralization of security and advance threat response. All the Threat response activity using EDR must be done at central site with direct access of endpoints. The hierarchical design typically used by traditional endpoints actually designed for update relays is not the correct solution deployment strategy for EDR. EDR solution needs bidirectional	Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21

	distributed across multiple sites for geo redundancy.	availability and there should not be any single point-of-failure. The solution architecture must be managing endpoints from multiple sites centrally and provide DC-DR redundancy.	exchange of data and full control of endpoints during forensics, response and remediation. In this regards, we suggest the amendment in caluse.	
P 84 Pt 1	1. Must be deployed in centralized architecture in DC-DR at two geographically separated datacenters for 10,000 clients.		Kidnly confirm on the total number of endpoints/workstations for EPP/EDR solution.	Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21
P 84 Pt 2	Patch update servers and architecture should be distributed across five Datacenter to significantly reduce load on network. It must offload the heaviest traffic from the master server to proxies or satellite servers, allowing optimizing costly and high-latency traffic.	Clause to be read as below: Any content update servers required in architecture should be distributed across five Datacenter to significantly reduce load on network. If solution does not require the DAT orsignature updates the districbuted servers are not required. The Solution must be allowing optimizing costly and high-latency traffic in the proposed architecture.	There are no patches or Signatures like AV solutions to be updated in EDR solution that may impact the bandwidth. EDR solution by design is a tool designed for centralization of security and advance threat response. All the Threat response activity using EDR must be done at cnetral site with direct access of endpoints. The hierarchial design	Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21

			typically used by traditional endpoints actually designed for update relays is not the correct solution deployment strategy for EDR. EDR solution needs bidirectional exchange of data and full control of endpoints during forensics, response and remediation. The clause is relating to EPP focussed solution and not EDR solution vendors. We request to amend the clause as proposed.	
P 84 Pt 3	The solution should have Datacenter wise redundancy architecture. Bidder and OEM of EDR solution must plan deployment options with clustering of nodes or cross site failover for disaster recovery scenarios but ensures delivery of services with redundancy. Failure of a management server of a particular Datacenter must not affect the client management	Clause to be read as below: The solution should be centralized with Datacenter wise (DC-DR) redundancy architecture. Bidder and OEM of EDR solution must plan deployment options with clustering of nodes or cross site failover for disaster recovery scenarios but ensures delivery of services with redundancy. Failure of a management server of a particular Datacenter must not affect the client detection and management.	As described above, the EDR solution typically is a centralized deployment with DC-DR redundancy architecture. Due to the nature of activities required in EDR solution during operations, dedicated EDR solutions are built on Certificate exchange mechanism which is a secure channel directly from centralized console.	Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21

			The control and access will break in case of distributed deployment and solution would not provide a centralized view and would be required to operate in a non-distributed management. Please amend the clause as proposed.	
P 84 Pt 6	EDR solution must work on both signature based and a signature-less mechanism to stop threats via a single agent on the endpoint	Clause to be read as below: The proposed EDR solution must have no dependency on signature based solution with typical use cases covered like Exploit Detection , IOC Detection (Malware & Methodology TTP's), Intelligence sharing, Intelligence feed integration, Custom Real-time IOC, Sweeping for openIOC, Compliance searches & hunt operations, Triaging an alert, Containing a threat, Track compromised user activity , Command-line review, Investigating lateral movement, , Investigating staging and exfiltration, Investigating suspected anti-forensics activity Investigating suspected rootkits & Backdoors including Hunting exercise like Stacking data &	EDR solution does not need signatures based detection approach and is mainly used to detect threats which have been missed by signature based solutions. Recommend to change the clause as requested.	Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21

		finding the unknown threats based on activity anomalies		
P 84 Pt5	Endpoint based EDR solution to protect all endpoints across network from Advanced Targeted Attacks and APTs	Kindly clarify if endpoints includes virtualised servers or only the desktop/laptops.		Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21
P 85 Pt 14	EDR solution must continuously monitor a critical event and its change of state in the system. It should generate an event that can execute responses.	Cause to be read as below: EDR solution must continuously monitor a critical events in the system and should generate an alert/event that can capture the entire rail of execution flow and system responses.	This is a sepecific OEM language and workflow. Please amend the clause as proposed	Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21
P 85 Pt 14	EDR solution must continuously monitor a critical event and its change of state in the system. It should generate an event that can execute response	Kindly clarify on Response execution.		Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21
P 85 Pt 15	EDR solution must create a response in case of files deleted from the system by file hash.		This is an EPP activity to detect on known hashes (MD5 or SHA1). Request to move this clause in EPP category specifications Please remove from EDR	Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21
P 85 Pt 15	EDR Solution must create a response in case of files deleted from system by file hash	Files deletion is not supported. Hence request you to kindly delete the clause		Refer Page 25-31 of corrigendum on RFP

				issued vide 01 Mar 21
P 85 Pt 17	EDR solution search box must understand simple syntax to combine collectors and build powerful search expressions and filters.	Cause to be read as below: EDR solution search box must understand simple syntax to query on large dataset of endpoint data and build powerful search expressions and filters on stored or real-time system data.	The clause has OEM specific marketing keywords used. Request to Please condier theproposed changed clause	Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21
P 85 Pt 21	EDR solution must share threat intelligence with endpoint protection solution so that the endpoint can take action on a previously detected malicious file	In order to share customized threat intel with other point products like endpoint protection in this case, sandboxing is required which will share custom threat intelligence in form of (VASO). If sandboxing is not required users can upload their own available Suspicious objects in EPP solution.		Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21
P 85 Pt 24	EDR solution must be able to able to run reactions like delete a selected folder or folders and deletes a windows registry values	Folder and registry values deletion is not supported. Hence request you to kindly delete this clause		Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21
P 85 Pt 25	EDR solution must able to kill process on endpoint by process ID, hash value, name, path and kill a process and its sub-processes	We terminate/kill the process by name itself and can block the hash if its file. Hence request you to ammend the clause as below: EDR solution must able to kill process on endpoint by process Name or ID and kill the hash if its file.		Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21

P 86 Pt 28	EDR solution must be able to trigger a response when a particular process is created or terminated	We can terminate the process by EDR, but trigerring a response is not possible. Hence request you to delete the clause or ammend the same		Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21
P 86 Pt 29	EDR solution must be able to trigger a response when a particular registry key is created, modified or deleted	Not Supported. Hence request you to delete the clause		Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21
P 86 Pt 38	Threat intelligence database provided with the EDR solution should act as a reputation broker to enable adaptive threat detection and response.	Clause to be read as below: Threat intelligence database provided with the EDR solution should act as a reputation broker to enable adaptive threat detection and response. The database can be inherent within the application or deplyed as a seprate server/broker depending upon design of EDR vendor application solution	This is limited to few vendors as per their solution design. Our solution does not need any separate Threat intelligence database server or broker to be installed for solution functioning. We have a defined Airgap threat intel & Content update process which is done via the EDR Management console only and need not have any intermediate or additional components to be deployed. Request to amend the clause as proposed	Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21

P 86 Pt 41	If more information on a file is needed, Threat intelligence database must be able to send the file automatically to advanced analysis solutions e.g. Endpoint sandboxing solution, to immediately gain additional insight to potential new threats and determine the reputation of a file in question.	Clause to be read as below: "If more information on a file is needed, Threat intelligence database must be able to send the file automatically to advanced analysis solutions e.g. Endpoint sandboxing solution, to immediately gain additional insight to potential new threats and determine the reputation of a file in question. The sandbox solution must be provided to scan minimum 5000 files/day with coverage on O.S like Windows, Macintosh & Linux fully on premise."	The additional enrichment and context using Sandbox would need to be quantified. The sizing of sandbox required for the solution must be provided as no of files to be analyzed per day. Also, the sandbox must be fully onpremise with capability for sandboxing for all leading O.S;s like Windows, Linux Request to see the amendment proposed.	Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21
P 86 Pt 41	If more information on a file is needed, Threat Intelligence database must be able to send the file automatically to advanced analysis solutions e.g. Endpoint sandboxing solution to immediately gain additional insights to potential new threats and determine the reputation of a file in question	Will the internet connectivity be provided for running files in sandboxing environment.		Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21
P 87 Pt 42	Threat intelligence database must be able to share relevant security intelligence in real time among endpoint solutions so that they can take the required actions against previously detected malicious files.	For EDR solution there is no dependency on other solutions to take any actions. Please remove this clause.		Refer Page 25-31 of corrigendum on RFP issued vide 01 Mar 21
			Solution to be sized for 1000 nodes &	Refer Page 25-31 of

			provision for 1000 incremental license Details required EPP & HIPS bifercation details /devices type - to be scanned HIPS soluton to be deployed in DC-DR centralized Architect & must have redudant DC Architect. - - Clarity required as DC-DR both need to be deployed in HA CMS soluton to be deployed in centralized Architect with geo redudancy DC -DR Architect - Clarity required All the H/w along with DB & replication license required for HIPS/EPP deployment will be provided by CoR. Please clarify that bidder have to consider only the OS - Windows/RHEL or have to cater OS along with DB &	corrigendum on RFP issued vide 01 Mar 21
--	--	--	---	---

			replication license. Asked for zero day protection with application containment - Is sandboxing solution required. Who will provide the OS, DB license for sandboxing	
PRIVILEGE ACCESS MANAGEMENT				
	PAM solution must support High Availability (load balancing and DC-DR) and must not have any single point of failure without any additional costs	Please provide the total number of admins / privileged users		Refer Page 31 of corrigendum on RFP issued vide 01 Mar 21
		How many target devices/assets to be integrated with PAM ?		Refer Page 31 of corrigendum on RFP issued vide 01 Mar 21
LOG ARCHIVAL AND ANALYSIS				
13.a.iv	(iv) Collectors must support integration with N Flow, Jflow.	(iv) Collectors must support integration with N Flow, Jflow.	Collectors must support integration and analysis with Netflow data	Refer Page 31-32 of corrigendum on RFP issued vide 01 Mar 21
13.b.(ii)	(ii) The software must have in build capability for block-level de-duplication for data across different electronic data repository for storage optimization.	(ii) The software must have in build capability for block-level de-duplication for data across different electronic data repository for storage optimization.	Remove this Point	Refer Page 31-32 of corrigendum on RFP

				issued vide 01 Mar 21
13.b.(iii)	(iii) The software must be able to compress and encrypt data at client side, support for 128 bit AES, 256 Bit AES etc encryption algorithm is required.	(iii) The software must be able to compress and encrypt data at client side, support for 128 bit AES, 256 Bit AES etc encryption algorithm is required.	The software must be able to compress and keep the data in a tamper proof manner to provide log authenticity	Refer Page 31-32 of corrigendum on RFP issued vide 01 Mar 21
NETWORK PACKET BROKER				
2	1:N mirror function should be supported with max latency of 5ns	1:N mirror function should be supported with max latency of 6ns	Requesting to relax latency parameter for wider participation	Refer Page 32-33 of corrigendum on RFP issued vide 01 Mar 21
6	Device should support Port to port L1 Latency of less than 5ns for TAP/mirror function	Device should support Port to port L1 Latency of less than 6ns for TAP/mirror function	Requesting to relax latency parameter for wider participation	Refer Page 32-33 of corrigendum on RFP issued vide 01 Mar 21
25	Network Packet Broker = Qty 15 is required as per the BOM	Request you to consider " 5 Tap + 5 TapAgg "	Requesting to clarify individual quantity of Tap and TapAgg. It is suggested to have at least 1 tap and 1 TapAgg at each DC site.	Refer Page 32-33 of corrigendum on RFP issued vide 01 Mar 21
New	New	All proposed taps, proposed tap aggregation devices and existing tap aggregation devices at Customer Location should be managed from a single pane of glass.	This is to simplify manageability of overall solution.	Refer Page 32-33 of corrigendum on RFP issued vide 01 Mar 21
New	New	Quoted Management solution should support real time telemetry	So that devices can be monitored in realtime	Refer Page 32-33 of

		and timeline view of various parameters	and historical troubleshooting	corrigendum on RFP issued vide 01 Mar 21
New	New	Management solution should be VM based and appropriate licences for managing the complete active TAP and Tap Agg infrastructure at should be quoted at customer site for centralised management across the DCs. Compute resources for Tap & TapAgg mgmt. solution will provided by the Customer.	For centralised monitoring and management of the solution across DC locations	Refer Page 32-33 of corrigendum on RFP issued vide 01 Mar 21
LUCIAD SOFTWARE				
	Luciad Software (Luciad End User Licenses) will fall under deliverable category		Kindly confirm	YES
	No application development would be part of this project(Luciad Products). We will only provide deployment Licenses		Kindly confirm	YES
	Training – 3 days product training for 2 batches each product. 1 times in a year. Total 6 days of product training free.		We assume that,it only includes the Product training, not the Application.	YES

CORRIGENDUM TO EOI ISSUED

AMENDMENTS TO PART - I

Clause / Para Number	Existing Clause	Revised Clause
COMMERCIAL CLAUSE PAGE 138		
Para 9 (a) (ii)	The Parties agree that the Joint Receipt Inspection (JRI) of delivered goods shall be conducted on arrival at each consignee site to be nominated by the Buyer. JRI shall be completed within 45 days of arrival of good at the Consignee. JRI will consist of (i) Quantitative checking to verify that the quantities of the delivered goods correspond to the quantities defined in this contract and the invoices. (ii) Complete functional checking of the stores/equipment as per specifications in the contract and as per procedures and tests laid down by Buyer but functional checking of spares shall not be done.	The Parties agree that the Joint Receipt Inspection (JRI) of delivered goods shall be conducted on arrival at each consignee site to be nominated by the Buyer. JRI shall be completed within 45 days of arrival of good at the Consignee. JRI will consist of Quantitative checking to verify that the quantities of the delivered goods correspond to the quantities defined in this contract and the invoices.

AMENDMENTS TO ANNEXURE '1' TO APPENDIX 'A'
OF ABOVE MENTIONED EO

Para Number	Existing Clause	Revised Clause
TECHNICAL SPECIFICATIONS PAGE 22		
Page 22 Annexure 1 to Appendix 'A'	Technical Specifications	Schedule of Requirement
Page 22 Annexure 1 to Appendix 'A' Heading	Qty	Min Qty
Page 22 Annexure 1 to Appendix 'A' Line No 3	AI Engine Processor	AI Engine Processor(Nodes)
Page 22 Annexure 1 to Appendix 'A' Line no 4	Block Storage 500 TB Raw	SAN Storage 500 TB Raw
Page 22 Annexure 1 to Appendix 'A' Line no 8	Top of the Rack (TOR) 48 Port Qty- 10	Top of the Rack (TOR) 48 Port Qty- 12
Page 22 Annexure 1 to Appendix 'A' Line no 9	Smart Rack Qty- 24	Smart Rack Qty- 12
Page 22 Annexure 1 to Appendix 'A' Line no 17	Cabling (As Req'd) and Fiber Distribution Frame Qty-10	Cabling (As Req'd) and Fiber Distribution Frame Qty-22
Page 22 Annexure 1 to Appendix 'A' Line no 25	Network Packet Broker Qty -15	Network Packet Broker Qty - 5 + 5

<u>HCI SPECIFICATIONS TYPE – A. PAGE 23</u>		
Page 23 HCI Type A	Cache offered Per node in GB – 500 GB	To be deleted
Page 23 HCI Type A	No. of Cache drives per node- 02	To be deleted
Page 23 HCI Type A	Block storage requirement per cluster – 500TB(Raw) and 250 TB usable	Block storage requirement per node (NL-SAS/ SAS/SSD)*- Min 60 TB (Raw). Block storage requirement per cluster (NL-SAS/ SAS/SSD)*– Min 300 TB(Raw) and 150 TiB usable *- In case the required block storage is not part of HCI node/cluster, the Block storage may be provided through per node HBA card connectivity to external storage.
Page 23 HCI Type A	To be added in specs table	To be added in specs table Encryption- All drives should be encrypted with either native / external KMS or SED
Page 23 HCI Type A	Switch with min 48 x 10 G ports and min 6 x 25G. 48 ports*2 with port licenses including SFPs. Detailed specs of the switch are elaborated under Network Switch heading given below.	Switch with min 48 x 10 /25 G ports and min 6 x 40/100G. 48 ports with port licenses including SFPs. Detailed specs of the switch are elaborated under Network Switch heading given below.
Page 23 HCI Type A	Cloud Automation and Orchestration solution- Qty 01 for Mgmt of all clusters at one site	Cloud Automation and Orchestration solution- Qty 01 for Mgmt of all clusters at one site with capability of min 50 VMs per cluster (06*50VMs).
<u>HCI SPECIFICATIONS TYPE – B. PAGE 24</u>		
Page 24 HCI Type B	No. of Cache drives per node- 02	To be deleted
Page 24 HCI Type B	SSD Capacity per Node Min 75TB	SSD Capacity per Node (Raw) – 75 TB
Page 24 HCI Type B	SSD Capacity per Cluster (Useable) without data efficiency Min 300TB	SSD Capacity per Cluster without data efficiency(RAW) - Min 300 TB
Page 24 HCI Type B	To be added in Specs table	Graphics Processing Unit on board- QTY 16 of 48 GB capacity each. Qty 02 of these to cater to min 4 nodes.
Page 24 HCI Type B	Switch with min 48 x 10 G ports and min 6 x 25G. 48 ports*2 with port licenses including SFPs. Detailed specs of the switch are elaborated under Network Switch heading given below.	Switch with min 48 x 10 /25 G ports and min 6 x 40/100G. 48 ports with port licenses including SFPs. Detailed specs of the switch are elaborated under Network Switch heading given below.

Page 24 HCI Type B	Cloud Automation and Orchestration solution- Qty 01 for Mgmt of all clusters at one site	Cloud Automation and Orchestration solution- Qty 01 for Mgmt of all clusters at one site with capability of min 50 VMs per cluster(05*50VMs).
<u>HCI SPECIFICATIONS : GENERAL PAGE 25 – 33</u>		
HCI Para 1(c)	The proposed software defined solution must be listed as a valid and certified solution on the server hardware OEM's website.	The proposed software defined solution must be listed as a valid and certified solution on the OEM's website.
HCI Para 1(h)	Proposed solution should support any two of the following hypervisors :- (a) Microsoft Hyper-V (b) VMware ESXi (c) RHEL KVM (d) Nutanix AHV	Proposed solution should support any one of the following hypervisors :- (a) Microsoft Hyper-V (b) VMware ESXi (c) RHEL KVM (d) Nutanix AHV
HCI Para 1(p)	SELLER/ Vendor will submit separate valid Manufacturers Authorization Form (MAF), along with complete technical details/ specifications of the solution in the bid, from OEM/ Technology partner for HCI solution and for the Scale Out NAS and block Storage solution. For OEM's with providing the solution on commercial off the shelf (COTS) servers (hardware) of other OEMs, they should provide datasheets / documented proof stating alliance / support by the hardware OEM for running the HCI software / Hypervisor / Scale Out NAS Storage / block storage solution on the selected hardware	SELLER/ Vendor will submit separate valid Manufacturers Authorization Form (MAF), along with complete technical details/ specifications of the solution in the bid, from OEM/ Technology partner for HCI solution and for the Scale Out NAS and block Storage solution. For OEM's with providing the solution on commercial off the shelf (COTS) servers (hardware) of other OEMs, they should provide datasheets / documented proof stating alliance / support by the hardware OEM for running the HCI software / Hypervisor / block storage solution on the selected hardware
HCI Para 2(c)	The proposed solution must support various replication methods (RF=2 & RF=3) or (FTT=1 & FTT=2) or (RAID + RAIN protection) for data protection. Any software license required for the same must be quoted on day one.	The proposed solution must support various replication methods (RF=2 & RF=3) or (FTT=1 & FTT=2) or (RAID or RAIN protection) for data protection. Any software license required for the same must be quoted on day one.
HCI Para 3(k)	The HCI should support native file services over NFS, CIFS /SMB, for file replication across	To be deleted

	clusters and data centers. It must support Soft / Hard quotas for File shares, at a user level and group level.	
HCI Para 3(m)	The HCI storage must have integrated wizard to schedule weekly/ monthly snapshot policies.	The HCI storage must have GUI based wizard, natively or through third party integration (as part of the solution), to schedule weekly/ monthly snapshot policies.
HCI Para 3(o)	The HCI storage must have integrated wizard for batch clones of virtual machines and customization.	The HCI storage must have integrated GUI based wizard, natively or through third party integration (as part of the solution), for batch clones of virtual machines and customization.
HCI Para 4(a) (i)	The proposed storage solution hardware should consist of minimum 01 nodes resources per site / cluster to cater for N+1 redundancy at 06 sites/locations and with minimum 04 controllers at each site/location of which each controller will have 4 cores, 128GB RAM each with a san switch consisting of minimum 04 number of 25 Gbps ports per node.	The proposed solution hardware should consist of minimum 01 nodes resource per cluster to cater for N+1 redundancy at 06 sites/locations where N=5.
HCI Para 4(a) (ii)	block storage must provide balancing of the stored capacity across all nodes in a cluster, ensuring, the load gets evenly distributed across all nodes The network load balancer requirements, if any, for load distribution across the nodes should be included as part of the solution.	The block storage in the proposed solution must provide balancing of the stored capacity across all nodes in a cluster, ensuring, the load gets evenly distributed across all nodes.
HCI Para 4(a) (iv)	The proposed block storage solution should be supplied with minimum 250 TB useable and 500TB raw capacity per site.	The proposed block storage solution should be supplied with minimum 150 TiB (useable) and 300TB raw capacity per site.
HCI Para 5(b)	The platform must support management of multiple individual clusters / sites (from multiple OEM / Hypervisors) from a Single Console, and with single sign-on. The platform should support	The platform must support management of multiple individual clusters / sites (from multiple OEM / Hypervisors) from a Single Console, and with single sign-on. The platform should support management of the offered solution.

	management of the offered Scale-Out NAS solution.	
HCI Para 6(c)	The cataloguing solution should provide a single pane for automated provisioning with model-based orchestration of compute, network, storage, applications and custom services through a unified multi-tenant IT service catalogue with support for show back and resource usage, providing a truly Software defined data center. The vendor should provide customized blue-prints to enable deployments involving Web, Application, Data base with high availability.	The cataloguing solution should have life cycle management workflow provisioning (Blueprint for min 50 VMs per cluster for both Type A & Type B configurations). It should provide a single pane for automated provisioning with model-based orchestration of compute, network, storage, applications and custom services through a unified multi-tenant IT service catalogue with support for show back and resource usage, providing a truly Software defined data center. The vendor should provide customized blue-prints to enable deployments involving Web, Application, and Data base with high availability.
HCI Para 6(g)	The solution should provide SDN for auto provisioning of networks including ability to automate delivery of virtual networking & virtual security services such as switching, routing, load balancing and micro-segmentation. The provided solution should be able to integrate with Vxlan and SDN infrastructure of major network OEMs.	To be deleted
HCI Para 7(c)	One TOR switches per cluster (Total qty 12 switches) with min 48 x 10 / 25Gbps ports (with Trans-Receiver cables) and with 6x100Gbps uplink ports (with Trans-Receiver) must be supplied. Minimum 48 Ports supporting 10G/25G optical ports for downlink connectivity to IT devices and 06 optical Ports supporting both 40G/100G for uplink connectivity with Core Switches. Each switch must be populated with 24x10G and 24 x 25 G SFP+ connectivity and 6 x 40 G QSFP Multimode fiber Trans receivers. The switch	One TOR switches per cluster (Total qty 10 switches) with min 48 x 10 / 25Gbps ports (with Trans-Receiver cables) and with 6x100Gbps uplink ports (with Trans-Receiver) must be supplied. Minimum 48 Ports supporting 10G/25G optical ports for downlink connectivity to IT devices and 06 optical Ports supporting both 40G/100G for uplink connectivity with Core Switches. Each switch must be populated with 24x10G and 24 x 25 G SFP+ connectivity and 6 x 40 G QSFP Multimode fiber Trans receivers. The switch should integrate with the existing Vxlan Fabric.

	should integrate with the existing Vxlan Fabric.	
HCI Para 7(e)(i)	Minimum 02 of latest generation Intel® Xeon Cascade Lake Processor with minimum 24 or higher cores per socket (CPU), min 2.1 Ghz and 64-bit x86 processor fully binary compatible to 32-bit applications. Number of Cores or a single die/ socket will be treated as a single processor. RAM per Node should be min 1 TB.	Minimum 02 of latest generation Intel® Xeon Cascade Lake Processor with minimum 24 or higher cores per socket (CPU), min 2.1 Ghz and 64-bit x86 processor fully binary compatible to 32-bit applications. Number of Cores or a single die/ socket will be treated as a single processor.
HCI Para 7(g)	10% of additional cores of compute and 10% additional memory should be mandatorily reserved for IO control / management / overheads per node over and above the core and memory requirements specified above. Further overheads to be catered additionally. This also does not include the compute and memory resource required for Scale out NAS and block Storage	10% of cores of compute and 10% memory per node, reserved for IO control / management / overheads per node catered in the sizing specified above. Details of the overhead requirements to be submitted along with the Technical bid.
HCI Para 7(j)	Each cluster should provide min 400000 IOPS with less than 2ms response time at 70:30 read:write ratio in 8K block size and should be configured to provide min 3GB/sec throughput at 32K block size for the available capacity. Reports for the same should be attached as a part of technical proposal.	Each node should provide min 50k IOPS with less than 2ms response time at 70:30 read: write ratio in 8K block size and should be configured to provide min 3GB/sec throughput at 32K block size for the available capacity. Reports for the same should be attached as a part of technical proposal.
HCI Para 8(a)	OEM / OEM authorized partner training in each of the technology components such HCI, Virtualization, block Storage, Cloud operation and management, along with OEM certification for 4 batches (15 days) of 25 personnel, at OEM/ Authorized Partner location, must be part of the contract	To be deleted

	deliverable. SI training and support is not acceptable.	
HCI Para 8(b)	The OEM should provide 24x7x365 infrastructure maintenance and support, for all hardware and software components of the proposed solution, including updates and patches, as well as technical support should available via telephone, email and web 24x7. Support for software components should include L1, L2 and L3 level support from each of the OEMs involved in the solution. The OEM / SELLER should provide single point of support for the HCI solution including Virtualization. Should include OEM Specialist /Certified expertise for hand holding and on premises/site solutions and trouble shooting for min 01 Month (at random or continuous) of 08 man hours per each day for every Year of warranty.	The OEM should provide 24x7x365 infrastructure maintenance and support, for all hardware and software components of the proposed solution, including updates and patches, as well as technical support should available via telephone, email and web 24x7. Support for software components should include L1, L2 and L3 level support from each of the OEMs involved in the solution. The OEM / SELLER should provide single point of support for the HCI solution including Virtualization.
AI ENGINE PROCESSORS : PAGE 34-35		
AI Engine-GPU Interconnects Para 2	System capability to process higher bandwidths (≥ 100 Gbps), more links, and should support improved scalability for multi-GPU and CPU system configurations, delivering more than 1 petaflops at full precision for processing. Should be equivalent to or better than 4*V100-SXM2-16GB or 4*V100-SXM2-32GB.	System capability to process higher bandwidths (≥ 100 Gbps), more links, and should support improved scalability for multi-GPU and CPU system configurations, delivering more than 1 petaflops at full precision for processing.
AI Engine-Storage. Para 6	Must Support 1. Mix of all SAS/ /SSD with option of quoting NVMe drives 2. Protocols like NFS, CIFS,SMB,SFTP. 3.Two drive protection 4. Current and new generation of nodes. Controllers with inter mixing	Must Support 1. Mix of all SAS/SSD/NVMe drives 2.Two drive protection 3. Current and new generation of nodes.

	5. All drives should be encrypted with either native /external KMS or SED. 6.Linear performance increase while expanding in future,	
AI Engine-Capacity Para 7	The system should be quoted with 3.2TB SSD*6=19.2TB RAW capacity with cluster capacity to be enhanced to 68PB	The system should be quoted with 3.2TB SSD*6=19.2TB RAW capacity with cluster capacity to be enhanced to 68PB
AI Engine-Software Libraries Para 14	The systems should be provided software library should have common frameworks like Pytorch, Tensor Flow, NVCAffe, TensorRT, Mxnetetc	The systems provided with software library should have common frameworks like Pytorch / Tensor Flow / NVCAffe, TensorRT / Mxnet etc.
	The Software libraries for single support should be provided by HW OEM	To be deleted
AI Engine-Power Supply Para 15	Hot Plug Dual Redundant platinum grade capable of supporting the load of all the connecting equipment in the chassis along with required ancillaries.	Hot Pluggable Dual Redundant capable of supporting the load of all the connecting equipment in the chassis along with required ancillaries.
<u>500 TB SAN STORAGE : PAGE 36-40</u>		
Title	500 TB BLOCK STORAGE	500 TB SAN STORAGE
500 TB Storage Para 1	To be configured with min 500TB raw and 250 TB usable (without considering any data reduction i.e. deduplication, compression etc.) usable storage using NVMe/SSD drives each for five Datacentres.	To be configured with min 500TB raw and 250 TiB usable (without considering any data reduction i.e. deduplication, compression etc.) usable storage using NL –SAS/SAS drives each for five Datacentres.
500 TB Storage Para 2	Offered Storage array must be a True Enterprise Grade Storage. The storage must have true symmetric Active-Active Controller architecture where a LUN must be accessible by all the controllers simultaneously. No Single Point of Failure (NSPOF) and single Microcode/operating system instead of running different Microcode / Operating system/Controllers for File & block services respectively. Controller must be scalable in future.	The storage must have true symmetric/asymmetric Active-Active Controller architecture where a LUN must be accessible by all the controllers simultaneously. No Single Point of Failure (NSPOF) and single Microcode/operating system instead of running different Microcode / Operating system/Controllers for File & block services respectively. Controller must be scalable in future.
500 TB Storage Para 3	The storage system must have minimum 2 TB or higher Global Cache and must support scalability. Only write cache must	To be deleted

	be mirrored. If Read Cache is mirrored then additional 25% Cache capacity must be provided. Cache memory must be delivered on DRAM, any other device or HDD must not be considered as cache.	
500 TB Storage Para 4	Rack Units.	To be deleted
500 TB Storage Para 6	The offered storage vendor must be placed in the leader's quadrant of the latest Gartner's report for General Purpose or ALL Flash Enterprise Storages.	To be deleted
500 TB Storage Para 7	Storage system capacity must be NVMe based scale-up and active-active architecture with 99.9999% availability and end-to-end NVMe connectivity. The storage offered must be NVMe drive.	To be deleted
500 TB Storage Para 8	The Storage must be scalable to at least 96 disk drives on the same set of controllers.	To be deleted
500 TB Storage Para 9	The proposed solution must support various replication methods (RF=2 & RF=3) or (FTT=1 & FTT=2) or (RAID + RAIN protection) for data protection.	The proposed solution must support various replication methods (RF=2 & RF=3) or (FTT=1 & FTT=2) or (RAID / RAIN protection) for data protection.
500 TB Storage Para 10	Offered Storage array must support block protocols like NVMe OF, FC & iSCSI. To be configured with only NVMe Protocol on day one.	To be deleted
500 TB Storage Para 11	Storage system must support Controller-based Data-At-Rest Encryption.	Storage system must support Data-At-Rest Encryption.
500 TB Storage Para 17	Offered Storage array must be supplied with Min 24 x 32Gbps Ports (NVMeOF) and 8 ports of 10 / 24 Gbps for replication and scalable to double in future on the same set of proposed controllers without compromising on the Back End Directors or Storage Processors.	Offered Storage array must be supplied with Min 8 x 32Gbps Ports and Min 4 ports of Min 10 / 24 Gbps for replication and scalable to double in future on the same set of proposed controllers without compromising on the Back End Directors or Storage Processors.
500 TB Storage Para 29	The proposed storage system must support non-disruptive firmware upgrades without rebooting any controller.	The proposed storage system must support non-disruptive firmware upgrades without any downtime.

500 TB Storage Para 34	The storage must support multiple operating systems such as Windows, Unix, Linux, Solaris and Mainframe etc.	The storage must support multiple operating systems such as Windows, Unix, Linux, etc.
500 TB Storage Para 35	The storage must support clustering solutions such as Microsoft cluster, MS SQL cluster, SUN Solaris cluster, Linux cluster etc.	The storage must support clustering solutions such as Microsoft cluster, MS SQL cluster and Linux cluster etc.
500 TB Storage Para 36	Storage must support VMware vStorage API for Array Integration including but not limited to VAAI, VVOL, VASA etc. and ODX for Microsoft Hyper-V.	To be deleted
500 TB Storage Para 39	The Storage solution should consist of min 04 Controllers with 128 GB RAM each.	The Storage solution should consist of min 04 Controllers with min 128 GB RAM each.
500 TB Storage Para 42	The replication solution must have capability to support three-way remote replication in both Concurrent with Delta Resync for zero-data-loss and Cascaded configuration with minimal impact on the primary storage system	The replication solution must have capability to support three-way remote replication in Concurrent/ Cascaded configuration with minimal impact on the primary storage system
500 TB Storage Para 43	The proposed storage system must have capability to support active-active configurations across 2 geographically separated sites at metro distance, where a single application must be active across both the sites, delivering 0-RPO and 0-RTO.	The proposed storage system must have capability to support active-active configurations across geographically separated sites, where a single application must be active across both the sites.
500 TB Storage Para 56	The solution must show end to end physical and logical topology view of the infrastructure from virtual host to storage devices including SAN interconnect	To be deleted
500 TB Storage Para 59	The solution must be able to identify performance bottleneck, Root Cause Analysis at host, SAN and storage level and must be able to troubleshoot storage performance problems	To be deleted
500 TB Storage Para 61	Must support for industry-leading Operating System platforms including LINUX, Microsoft Windows, HP-UX, SUN Solaris, IBM-AIX etc.	Must support for industry-leading Operating System platforms including LINUX, Microsoft Windows and IBM-AIX etc.
500 TB Storage	63. VMWare Integration.	To be deleted

Para 63 to 68 and 72	64. Management of storage array from VMWare vCenter using plug-in. 65. Storage management console must be VMWare aware and must report virtual machines running on storage datastore/VVOL container, including VM level performance and capacity details. 66. Storage array must support VAAI and VASA integration. 67. Storage array must support VmwarevRO and VRA plug-ins. 68. Support for VMware SRM for integration with storage based replication.	
500 TB Storage Para 72	Support for Ansible using official Ansible modules	To be deleted
500 TB Storage Para 76	There must be unconditional warranty and not returnable disk and memory support for any drives and memory during seven years of support after warranty starts.	No hard disk would be returned back to supplier during warranty/ AMC period even against replacement of unserviceable hard disk.

BACK UP SOLUTION PAGE 41-43		
Backup Solution Para 1(a)	Project Scope is related to Disk Based Backup Platform for existing Setup of Customer.	Project Scope is pertains to Disk Based Backup Platform of BUYER.
Backup Solution Para 1(c)	Each location should have 2 Copies of the Data Backup with High Availability/Clustered Solution with 99.997% uptime of the storage platform integrated with the existing Backup solution.	Each location should have 2 Copies of the Data Backup with High Availability/Clustered Solution with 99.997% uptime of the storage platform integrated with the supplied Backup solution.
Backup Solution Para 1(g)	System should be compatible with the existing Backup Solution or the Bidder can propose a new Backup Solution with Disk Based Backup Storage. Backup Solution offering should be compatible with Existing Tape Library for Migration Services.	To be deleted
Backup Solution Para 1(h)	The Solution should cater to min 200 Workloads or 600TB of storage capacity.	The Solution should be licensed for min 400 Workloads or 160 sockets or 6*120TB (Front end) of storage capacity. (Total Raw storage requirement would be 720 TB *3 =2.1 PB)

Backup Solution Para 2(g)	The Archive must support mixed disks drive capacities or mixed Tape Capacities within the same array. It is anticipated that 18TB disks will be used initially with the option to use 20 TB and larger disk capacities as they become available, in any mix without loss of storage yield, whatsoever.	The solution must support mixed disks drive within the same array.
Backup Solution Para 2(j)	The Archive shall support individually removable disk drives for shelf storage, and media transportation. Data shall be written as complete non-segmented files on the disks and replicated for protection against individual disk failure.	To be deleted
Backup Solution Para 2(k)	For disaster recovery purposes, it should be possible to remove any individual Disk or Tape and recover media files using an external computer without special software.	To be deleted
Backup Solution Para 2(m)	The power budget for the Archive storage shall not be more than 1.5 Watts per useable Terabyte of Storage capacity in normal operation, to minimize power consumption and A/C provisioning.	To be deleted
Backup Solution Para 2(q)	Optionally the system shall be capable of integrating with Media Management Applications at a high level using a Virtual File System which shall emulate a NFS / SaMBa / CIFS file system and should support FTP, FXP and Vendor Specific protocols listed separately. Where this approach is offered, the Virtual File System shall be capable of creating the necessary file replicas to meet the requirements of section 10 above.	Optionally the system shall be capable of integrating using applications a Virtual File System which shall emulate a NFS / SaMBa / CIFS file system.
Backup Solution Para 2(r)	Where a high-level Virtual File System approach is offered, the file system shall be maintained in dual fault tolerant RAID storage with the option for dual redundancy. The Virtual File System shall also be capable of using a share on an existing Near-Line storage system as the Cache.	To be deleted
Backup Solution Para 2(s)	Proposed System should be able to create and Managed Shelf / Vault workflow as a Copy of Last Resort for	To be deleted

	all, or strategically important static parts of the Archive Solution.		
Backup Solution Para 2(t)	Vault Management should be supplied with Third party IT standard Server as per the Archive Vault Management Designing.	To be deleted	
Backup Solution Para 2(u)	Vault Management system should be supplied by QR Code Printer and Android Tablet scanner. Printer & Tablet should be certified by the Archive Solution OEM.	To be deleted	
Backup Solution Para 2(v)	Main Archive Storage unit can be expandable with 10 Expansion as scale up and can add multiple Main Archive Chassis to increase the required throughput and Scale out capacity with multiple Storage Arrays.	Main Archive Storage unit can be expandable with min 06 disks Expansion as scale up and can add multiple Main Archive Chassis to increase the required throughput and Scale up capacity with multiple Storage Arrays.	
Backup Solution Para 2(w)	All the Units should have at least 4U Rack Space.	To be deleted	
Backup Solution Para 2(x)	The offered Archive Solution should offer minimum of 12 TB Raw Capacity supported in a Single Node Array with 3.8/7.6 TB per slots combination.	To be deleted	
Backup Solution Para 2(y)	Solution should be offered with 3 Years Warranty + 5 Extended Warranty / Comprehensive AMC.	To be deleted	
Backup Solution	To be added Backup Software Specifications.	To be added Backup Software Specifications. (a) The offered software must support application aware backups for MS SQL, ORACLE, My SQL, DB2, Exchange, SharePoint etc. Software should work with both Standard and Enterprise Database editions. (b) The offered software must have compatibility to perform backup for all the editions of Windows Server 2019 and above, Hyper-V environment, Nutanix Hypervisor, VMware 6.5 and above, and RHEV 7.1 and above. (c) The proposed backup software must be independent of the backup hardware and should provide all the functionality listed here for all the major storage vendors, especially for	

		the Storage hardware being supplied in the bid.(500TB SAN and Back-up hardware. (d) Backup software must support both the source side and target side de-duplication capability, especially on the hardware being supplied in the bid. (500TB SAN and backup hardware. (e) The proposed software must provide global de-duplication across workloads configured in a backup job across various storage vendors. (f) The proposed backup software should provide cross hypervisor support between VMware, Nutanix and Hyper-V. (g) The offered backup software should be able to restore backed up data. (i) To original host (ii) To different host (iii) From failed job till the last point of data written on disk (dedupe) (h) The proposed software should include file archival feature to move historical data based on file attributes/policy for long term retention. (j) The offered software must support complete integration of server backup, virtual machines backup, no-virtualised servers, HCI workloads, Data archival and replication solution with a single management console. (k) The backup software license should be for 400 workloads or 160 sockets or 720TB (06x120TB) front-end capacity with perpetual licenses in the name of the buyer.
--	--	--

SAN SWITCH PAGE 44 & 45		
San Switch	The SAN switch must have complete non-blocking architecture with minimum 48 FC ports of 32 Gbps speed each and with no oversubscription. All ports must concurrently active and will all necessary licenses from day one.	The SAN switch must have complete non-blocking architecture with minimum 48 FC ports of 32 Gbps speed each and with no oversubscription. All ports must be concurrently active and with all necessary licenses from day one.
TOR / VX LAN : PAGE 46-48		
TOR Switch	Para 1-8 of Specifications for TOR/VX LAN mentioned in Page 46-48.	To be deleted
	TO BE ADDED IN SPECIFICATIONS Specifications of 48 Port TOR switch	Switch should support min 48 X min 10/25 G interfaces (Natively or using break-out cables) and populated with 24 nos of 10G and 24 nos 25G MM connectivity with SFP or using breakout interfaces. Optics / Cables to be included accordingly.
		Device should provide additional 8 nos of 40/100G QSFP interfaces with 40G-SR4 optics populated from day 1.
		Device should have deep packet buffers of 4 GB or more to handle congestion scenarios arising out of TCP incast and varying link speed situations.
		Device should be based on industry standards based virtual output queue based architecture to avoid head-of-line blocking issues.
		Device should have support 20K or more ingress/egress ACL entries.
		Device should support VXLAN and MPLS for L2 and L3 VPN support from day 1
		Should support VXLAN routing, bridging and gateway capability for physical to virtualization communication.
		Switch should support advance automation with support for onboard python, bash, docker containers and Open config over GRPC
		Switch should support BGP, OSPF, ISIS from day 1
		Should be capable of overall throughput of min 2.0 TBPS

		Should have redundant and hot swappable power supply and be supplied with C 13-C 14 power cords
		Should be capable of front to rear or rear to front cooling (Reversible air flow option) and should have redundant and hot swappable (N+1) fans
		Transceiver and switch should be from the same OEM
	TO BE ADDED IN SPECIFICATIONS Specifications of 32 Port VX LAN switch	Device should have min 32 nos of min 40/100G QSFP interfaces with required no. of 40G-SR4 optics included as per solution.
		Should be capable to support VXLAN based fabrics, with routing, bridging and gateway capability for physical to virtualization communication.
		Should support advance automation with support for onboard python, bash, docker containers and open config over GRPC
		Switch should support BFP, OSPF, ISIS from day 1
		Should support breakouts on all the ports
		Should be capable of overall throughput of min 6.4 TBPS
		Should have capable of front to rear or rear to front cooling (reversible air flow option) and should have redudant and hot swappable (N+1) fans
		Should have redundant and hot swappable power supply and supplied with C13 – C14 power cords
		Transceiver and switch should be from the same OEM

SMART RACK SPECIFICATIONS : PAGE 49 & 50			
Smart rack para 1		Heavy Duty, 42U Premium Rack cabinet that accommodates all standard 19-inch rack mount equipment which will be used for commissioning of standard switches, and termination of optical fiber and CAT VI cable fully assembled for quick and easy deployment in secure, high-density server and IT networking environments. Preferably dust proof rack.	Heavy Duty, 42U Premium Rack cabinet that accommodates all standard 19-inch rack mount equipment which will be used for commissioning of standard switches, and termination of optical fiber and CAT VI cable fully assembled for quick and easy deployment in secure, high-density server and IT networking environments.
Smart rack para 2		Remote management software for integrated monitoring of physical servers and client software to control server shutdown via the PMC UPS to be catered by the HCI Integrator and must support all the versions of Windows 10, and server 2012 onwards, UNIX/LINUX and VMWARE Sphere/ESX Server, CITRIX XEN.	To be deleted.
Smart rack para 3		It should be integrated with a Live CAM for recording and monitoring. Monitoring facility of the rack from remote control location. The smart rack should be Free-standing/all Mountable and meet following specifications:-	It should be integrated with a Live / IP-CAM for recording and monitoring. Monitoring facility of the rack from remote control location. The system should be fitted with an IP enable CCTV based surveillance system for monitoring of the activities outside the smart rack. The system must be supplied with adequate IP cameras per site to cover the complete surveillance of rack along with NVR system having at least 4TB storage space. The smart rack should be Free-standing/all Mountable and meet following requirement:-
Smart rack para 3(a)		Front perforated steel door. Rear door of CRCA 1.5 and with split door design. Enclosure with IP 41 and with	To be deleted.

	Standard dimension. 2100Htx800Wdx1200Depth	
Smart rack para 3(b)	Must have touch screen control of TFT display (128x128pixels RGB) with backlighting, energy saving mode, separate keyboard tray sliding and Rotary. Should have pre-installed casters and levelling feet. Stationary shelf's 02 per rack. Multi colour LEDs to indicate switching states and limits per individual output slot.	The smart rack should be fitted with Touch screen display and all SNMP parameters should be visible on the display such as IPPDU, Temperature, Humidity, access. The smart rack SNMP parameters should be compatible and configurable in DCIM solution. Bidder has to include the requirements of power modifications at sites for installation of these smart racks in existing DCs. Must have integrated Infrared access sensor
Smart rack para 3(c)	Should have provisions of rear and front panel. Front panel should be made of 4mm safety perforated sheet steel section and rear panel to be made of perforated sheet steel. Rack should be \permanently bolted and welded to the ground	Should have provisions of rear and front panel. Front panel should be fitted with perforated sheet steel section and rear sheet steel perforated double door with four point locking and spring loaded comfort handle. Rack should be \permanently bolted and welded to the ground or as per existing norms of DC.
Smart rack para 4	It should be fitted with Qty 02, 3-Phase IP based PDU (Power Distribution Units). Capable of remote monitoring of all electrical parameters and must support minimum 20KW load per phase. IP PDU must contain a min of 06 C-13/C-14 sockets per phase and min 2 C-19 sockets per phase.	It should be fitted with Qty 02, 3-Phase IP based PDU (Power Distribution Units). Capable of remote monitoring of all electrical parameters and must support minimum three phase 32Amps IP PDU for 15 KW load must contain a min of 06 C-13/C-14 sockets per phase and min 2 C-19 sockets per phase.
Smart rack para 7	Gasketing: Poly Urethane gasketing. By using dust & water cannot enter the rack and IP41 Protection.	To be deleted.
Smart rack para 9	Copper earth bar with Earthing cables.	Copper earth bar with 20 point for earth connection using Earthing cables.

APPLICATION DELIVERY CONTROLLER AND WEB APPLICATION FIREWALL : PAGE 51-54		
ADC and WAF- Traffic Ports Page 51	6 x 40 GbE QSFP+ 12 x 10 GbE SFP+ (without use of Breakout Cables) (2 x 40G, 6 x 10G, 4 x 1G populated from Day-1)	min 6 x 40 GbE QSFP+ 12 x 10 GbE SFP+ (without use of Breakout Cables) (2 x 40G, 6 x 10G, 4 x 1G populated from Day-1)
ADC and WAF- Device L4 throughput	Device L4 Throughput : 150 Gbps scalable to 200 Gbps	Device L4 Throughput : Minimum 150 Gbps
ADC and WAF - Virtualisation Page 52	The proposed device should support 5 Virtual Instance from Day 1 and support upto 60 Virtual Instances for future Scalability on the same hardware. It should NOT use Open Source/3rd party Network Functions.	The proposed device should support 5 Virtual Instance from Day 1 and support upto 20 Virtual Instances for future Scalability on the same hardware. It should NOT use Open Source/3rd party Network Functions.
DESKTOP PC : PAGE 55		
PCI Slot	Expansion Slots (PCI x 1) (Number)	To be deleted
Cache	Cache – 22 MB	Cache – 20 MB or More
Cabinet FF & Volume	Cabinet volume 8 or lower Cabinet Form Factor (7-8)	Lowest SFF to accommodate the solution
Graphics Card	NVIDIA QUADRO RTX 2070 16GB or more	NVIDIA GeForce® RTX 2080 Super 8GB
TOWER SERVER : PAGE 57		
Tower Server	Response time 5 ms	Response time 6-8 ms
Cache	Cache – 22 MB	Cache – 20 MB or More
	RAM Expandable upto (GB) = 3072 GB	RAM Expandable upto (GB) = 768 GB or More
Graphics Card	NVIDIA QUADRO RTX 2070 16GB or more	NVIDIA GeForce® RTX 2080 Super 8GB
Monitor Resolution	1920*1080FHD	3840*2160 UHD (4K)
UPS 1 & 2 KVA : PAGE 59		
UPS 1 KVA	IGBT- PWM with inbuilt isolation transformer	IGBT- PWM
UPS 2 KVA	IGBT- PWM with inbuilt isolation transformer	IGBT- PWM

CABLING AND FIBER DISTRIBUTION FRAME PAGE 60 & 61		
Cabling and FDF Para 1	The Fiber Distribution frame for 36/48 port switch should support following specifications:-	Every layer -2 switch should be provided with FDF with LC type adapter. The Fiber Distribution frame of Min 32 pair port/48 pair ports for 32/48 port switch respectively should support following specifications:-
Cabling and FDF Para 2	LC-LC Fiber Patch Cord	LC-LC Fiber Patch Cord (Multi Mode)
APPLICATION PERFORMANCE MONITORING : PAGE 62 & 63		
Appln Performance Monitoring Para 1	In this era of Information Technology and automation, Application Performance Management (APM) tools are used to monitor the performance of software applications. APM ensures that it provides services to the customers up to the defined by the user and identifies the problems related to the application performance. Application performance can be monitored or tracked using different categories like load time, the response time of the application, etc. Nowadays, with the use of technology the applications are becoming more and more complex and distributed. Hence it is necessary to monitor the performance of an application to provide greater satisfaction to the end-user. The proposed solution should cover the following aspects.	In this era of Information Technology and automation, Application Performance Management (APM) tools are used to monitor the performance of software applications. APM ensures that it provides services to the customers up to the defined by the user and identifies the problems related to the application performance. Application performance can be monitored or tracked using different categories like load time, the response time of the application, etc. Nowadays, with the use of technology the applications are becoming more and more complex and distributed. Hence it is necessary to monitor the performance of an application to provide greater satisfaction to the end-user. The proposed solution should be licensed for min 60 applications running on OS(Windows/Linux)/DB to cover the following aspects.
Appln Performance Monitoring Para No 2	<u>Full stack Visibility.</u> Monitor the health and performance of custom on-premises distributed applications across services, hosts, containers, and platforms down to the code. Monitoring capability of infrastructure and application metrics and correlating them in order to identify root cause of	<u>Full stack Visibility.</u> Monitor the health and performance of custom on-premises distributed applications across services, hosts, containers, and platforms down to the code. Monitoring capability of infrastructure and application metrics in order to identify root cause of a failure or raise an alert of a possible failure.

	a failure or raise an alert of a possible failure.	
Appln Performance Monitoring Para 10	<u>Service, and trace-level summaries</u> Pinpoint the root cause of performance problems without drilling down, enabling to troubleshoot issues like latency, volume, error rate, and slowdowns without digging into the details.	<u>Service, and trace-level summaries</u> Pinpoint the root cause of performance problems with/ without drilling down, enabling to troubleshoot issues like latency, volume, error rate, and slowdowns without digging into the details.
APPLICATION AND NETWORK MONITORING PAGE 64- 73		
Appln and Network Monitoring Para 1	BUYER is planning to implement network performance management solution in order to monitor and ensure optimal performance levels of a BUYER network. Solution should provide the visibility and insights to Network and application performance for a flawless, agile, and cost-effective application delivery over Customer network. Complete solution (Network, application performance monitoring and Visualization/Analytics) should be a product from a single vendor.	BUYER is planning to implement network performance management solution in order to monitor and ensure optimal performance levels of a BUYER network. Solution should provide the visibility and insights to Network and application performance for a flawless, agile, and cost-effective application delivery over BUYERs network. Complete solution of Network and application performance monitoring including Visualization/Analytics meeting the Tech specs listed below should be a product from a single vendor.
Appln and Network Monitoring Para 8	The offered Performance monitoring solution should support at least the following. The detailed technical specifications are mentioned in this RFP document. All the proposed Components for NPM/APM/EUR should be from single vendor.	To be deleted.
Appln and Network Monitoring Para 10	Provides insight into the performance of all BUYER monitored links and application components.	Provides insight into the performance of all BUYER's monitored links and application components.
Appln and Network Monitoring Para 15	Solution should support combined high-definition network testing and wire-data analytics in a single pane of glass for complete visibility of BUYER on Customer network.	Solution should support combined high-definition network testing and wire-data analytics in a single pane of glass for complete visibility on BUYER's network.
Appln and Network Monitoring Para 22	Number of flows per minute not exceeding 1.5 Million should be licensed from Day 1.	Number of flows per minute not exceeding 1.5 Million should be licensed from Day 1. (Total Qty requirement is 1.5 Million * 05 Sites)

Appln and Network Monitoring Para 23	Assuming there are 50 capture points with max upto 30k Flows analysis per minute per site.	Assuming there are 50 capture points with max upto 30k Flows analysis per minute per site. (Total Qty requirement is 50 capture points * 05 Sites)
Appln and Network Monitoring Para 24	Qty 60 Sensors for 1GbE smart SFP -FPGA, Multimode, 850nm, 550m.	Qty 60 Sensors for 1GbE Sensor - FPGA, Multimode, 850nm, 550m. (Total Qty requirement is 60 * 05 Sites)
Appln and Network Monitoring Para 25	Qty 20 Sensors for 1GbE smart SFP with FPGA, RJ45 Copper.	Qty 20 Sensors for 1GbE sensor with FPGA, RJ45 Copper. (Total Qty requirement is 20 * 05 Sites)
Appln and Network Monitoring Para 26	Qty 20 Sensors for 10 GigE SFP+, Single Mode, 1310 nm,10km,LC connector	Qty 20 Sensors for 10 GigE Sensor, Single Mode, 1310 nm,10km,LC connector. (Total Qty requirement is 20 * 05 Sites)
Appln and Network Monitoring Para 121	The solution must be offer the possibility to deploy virtual sensors to capture traffic between machines on VMWare ESX/ESXi, HyperV and KVM chassis	The solution must be offer the possibility to deploy virtual sensors to capture traffic between machines on virtualised environment. All hardware sizing required for the solution to be catered additionally in the HCI sizing for the software, OS & DB (including any replication licenses) required for successful deployment of solution to be provided by bidder.
APPLICATION LOAD TESTING TOOLS : PAGE 74&75		
Application load testing tools Para 16	<u>Real Browser Support.</u> Support for Real browser testing (This feature is available only with one tool: "LOADVIEW", may result in single vendor)	To be deleted

VA ASSESSMENT TOOLS : PAGE 76-78		
VA Tools OEM SUPPORT Features	24 x 7 x 365 Support by respective OEM., Updating for patches and bug fixes after immediate realise by OEM., Upgradation of version after immediate realise by OEM	24 x 7 x 365 Support by respective OEM. Updation for patches and bug fixes after any immediate release by OEM.,
VA Tools Para 2 Generic features of vulnerability management	VA scanner capable to check credentials authentication before launching scan.	VA scanner capable to check with and without credentials authentication before launching scan.
VA Tools Para 4 Vulnerability Management features	Agent and scanner capable to communicate directly with management console over encryption without any other intermediate device	Agent / Agentless and scanner capable to communicate directly with management console over encryption without any other intermediate device.
VA Tools Para 5 Vulnerability Management features	Offered product capable to support private cloud workloads in Azure/VMware/Open Stack etc. IaaS on premises.	Offered product must be capable to support private cloud workloads in virtual environment . IaaS on premises.
VA Tools Database scanning Coverage	1. MS-SQL(All versions). 2. MySQL (All versions). 3. Oracle (All versions). 4. PostgreSQL (All versions). 5. DB2. 6. Mongo DB (All version). 7. NA	1. MS-SQL(All versions). 2. MySQL (All versions). 3. Oracle (All versions). 4. DB2.
VA Tools- Secure configuration assessment- Technology coverage (8)	Mobile OS	To be deleted.

SECURITY SOLUTION FOR EPP/ HIPS & EDR		
Security Solution For Endpoint Protection (EPP/ HIPS) Para 3	1. Bidder must quote solution which will be deployed on virtualized infrastructure. All hardware, software (i.e. Compute, Memory, storage, VMWare, Operating Systems (only Windows and RHEL, in case any other OS then must be quoted by bidder along with bid), DB and replication licenses) required for successful deployment will be provided by Buyer as per sizing requirements. Sizing of hardware and software is to be certified by prospective OEM and certificate from OEM along with bid is to be submitted by Bidder. Any other hardware or software or license required for deployment of HIPS solution must be quoted by Bidder along with bid.	2. Bidder must quote solution which will be deployed on virtualized infrastructure. All hardware sizing required for the solution to be catered additionally in the HCI sizing. Further the software, OS and DB (including any replication licenses) required for successful deployment will be provided by Bidder. Sizing of hardware and software is to be certified by prospective OEM and certificate from OEM along with bid is to be submitted by Bidder. Any other hardware or software or license required for deployment of HIPS solution must be quoted by Bidder along with bid.
Security Solution For Endpoint Protection (EPP/ HIPS) Para 4	HIPS solution must be sized for at-least 1000 end points. Bidder needs to provision for the incremental licenses up to 1000 endpoints to meet the futuristic requirements of Buyer as part of solution.	HIPS solution must be sized for at-least 1000 end points.
Security Solution For Endpoint Protection (EPP/ HIPS) Para 5	The solution must offer anti-malware, firewall, application control, change control, HIPS, network visibility and micro-segmentation based firewall and virtualization security in a single agent functionality to ensure optimal security and compliance for critical servers	3. The solution must offer anti-malware, network visibility and virtualization security in a single agent functionality to ensure optimal security and compliance for critical servers.
Security Solution For Endpoint Protection (EPP/ HIPS) Para 9	The solution must offer true zero day protection along with application containment, application and change control, file integrity monitoring for zero day malware prevention.	The solution must offer true zero day protection along with application containment, application exploit prevention, monitoring zero day malware detection and prevention.
Security Solution For	The solution must be able to block unauthorized changes to	The solution must be able to detect, alert and prevent

Endpoint Protection (EPP/ HIPS) Para 13	critical system files, directories, and configurations.	unauthorized changes to critical system files, directories, and configurations.
Security Solution For Endpoint Protection (EPP/ HIPS) Para 15	The Server Security solution must have HIPS control to restrict application and operating system behaviour using policy-based least privilege access control.	The Server Security solution must have HIPS control to restrict malicious application and operating system behaviour, using application control and behaviour analysis.
Security Solution For Endpoint Protection (EPP/ HIPS) Para 16	Server agent must prevent malicious applications from inserting code into trusted applications. The HIPS, HIDS, file integrity monitoring, host based firewall, application control should be offered using a single agent.	The Server agent must prevent malicious applications from inserting code into trusted applications. The Intrusion detection and prevention along with continuous system monitoring for malicious activity detection, exploit prevention should be offered using single agent.
Security Solution For Endpoint Protection (EPP/ HIPS) Para 28	The solution must offer intelligent filters which are pre-configured or configured using professional services to track the relevant objects on the system, for each standard operating system covering systems files including Windows, Linux. It should also include application filters for Apache, Tomcat, Websphere and JBOSS, IIS, Weblogic, Websphere etc.	The solution must offer intelligent filters which are pre-configured or configured using professional services to track the relevant objects on the system, for each standard operating system covering systems files including Windows, Linux.
Security Solution For Endpoint Protection (EPP/ HIPS) Para 30	Solution must offer granular read, read-write or no access to identified process or users.	To be deleted
Security Solution For Endpoint Protection (EPP/ HIPS) Para 31	Solution must mitigate patching for new and legacy systems and enable application and instance level security.	To be deleted
Security Solution For Endpoint Protection (EPP/ HIPS)	Solution must have host firewall to control inbound and outbound network traffic to and from servers.	To be deleted

Para 32		
Security Solution For Endpoint Protection (EPP/ HIPS) Para 34	HIPS must support firewall capabilities to directly block unwanted traffic.	To be deleted
Security Solution For Endpoint Protection (EPP/ HIPS) Para 38	The solution must be able to manage application control, change control and policy auditing solution from a single management console.	The solution must be able to manage HIPS, detection and prevention features from a single management console at DC & DR.
Central Management System for EPP/HIPS, EDR Para 1	The Central Management System (CMS) must be supplied with Endpoint Protection (EPP)/ Host Intrusion & Prevention System (HIPS), Endpoint Detection & Response (EDR), as part of comprehensive Endpoint Security Solution and must be able to support management of supplied solutions from remote central locations. It must offer following of configuration management of devices as described in subsequent paragraphs. The proposed solution architecture for CMS must be designed for high-availability and there should not be any single point-of-failure. The solution architecture must be distributed across multiple sites for geo redundancy.	1. The Central Management System (CMS) must be supplied with Endpoint Protection (EPP)/ Host Intrusion & Prevention System (HIPS), Endpoint Detection & Response (EDR) as part of comprehensive Endpoint Security Solution and must be able to support management of supplied solutions from remote central locations. It must offer following of configuration management of devices as described in subsequent paragraphs. The proposed solution architecture for CMS must be designed for high-availability and there should not be any single point-of-failure. The solution architecture must be managing endpoints of multiple sites, centrally and provide DC-DR redundancy:-
Central Management System for EPP/HIPS, EDR Para 2	Bidder must quote solution which will be deployed on virtualized infrastructure. All hardware, software (i.e. Compute, Memory, storage, VMWare, Operating Systems (only Windows and RHEL, in case any other OS then must be quoted by bidder along with bid), DB and replication licenses) required for	2. Bidder must quote solution which will be deployed on virtualized infrastructure. All hardware, sizing required for the solution to be catered additionally in the HCI sizing. Further the software, OS and DB (including any replication licenses) required for successful deployment will be provided by Bidder. Sizing of hardware and software is to be

	successful deployment will be provided by Buyer as per sizing requirements. Sizing of hardware and software is to be certified by prospective OEM and certificate from OEM along with bid is to be submitted by Bidder. Any other hardware or software or license required for deployment of CMS solution must be quoted by Bidder along with bid.	certified by prospective OEM and certificate from OEM along with bid is to be submitted by Bidder. Any other hardware or software or license required for deployment of CMS solution must be quoted by Bidder along with bid.
Central Management System for EPP/HIPS, EDR Para 3	The solution must be able to manage EPP/ HIPS, EDR and encryption solution centrally through common or separate management console.	The solution must be able to manage EPP/ HIPS and EDR centrally through common or separate management console.
Central Management System for EPP/HIPS, EDR Para 4	The solutions must support report customization and allow viewing directly using a web browser and also as a dashboard using the management console for EPP, EDR and HIPS solution.	3. The solutions must support report customization and allow viewing directly using a web browser and also as a dashboard using the management console for EPP/HIPS and EDR solution.
Central Management System for EPP/HIPS, EDR Para 5	Each of the proposed solution (EPP, EDR and HIPS) must be able to manage and update agents and policies from either from one management platform or centrally management platform of respective solution. Solution must have inbuilt capability to push/ deploy agent or using its management console or should integrate with 3rd part patch management solution.	Each of the proposed solution (EPP/HIPS and EDR must be able to manage and update agents and policies from either from one management platform or centrally management platform of respective solution. Solution must have inbuilt capability to push/ deploy agent or using its management console or should integrate with 3rd party patch management solution.
Security Solution For Endpoint Detection And Response Para 2	Patch update servers and architecture should be distributed across five Datacenter to significantly reduce load on network. It must offload the heaviest	To be deleted

	traffic from the master server to proxies or satellite servers, allowing optimizing costly and high-latency traffic.	
Security Solution For Endpoint Detection And Response Para 3	The solution should have Datacenter wise redundancy architecture. Bidder and OEM of EDR solution must plan deployment options with clustering of nodes or cross-site failover for disaster recovery scenarios but ensures delivery of services with redundancy. Failure of a management server of a particular Datacenter must not affect the client management.	The solution should be centralised with DC-DR Datacenter wise redundancy architecture. Bidder and OEM of EDR solution must plan deployment options with clustering of nodes or cross-site failover for disaster recovery scenarios but ensures delivery of services with redundancy. Failure of a management server of a particular Datacenter must not affect the client detection and management.
Security Solution For Endpoint Detection And Response Para 4	Bidder must quote solution which will be deployed on virtualized infrastructure. All hardware, software (i.e. Compute, Memory, storage, VMWare, Operating Systems (only Windows and RHEL, in case any other OS then must be quoted by bidder along with bid), DB and replication licenses) required for successful deployment will be provided by Buyer as per sizing requirements. Sizing of hardware and software is to be certified by prospective OEM and certificate from OEM along with bid is to be submitted by Bidder. Any other hardware or software or license required for deployment of EDR solution must be quoted by Bidder along with bid.	Bidder must quote solution which will be deployed on virtualized infrastructure. All hardware, sizing required for the solution to be catered additionally in the HCI sizing. Further the software, OS and DB (including any replication licenses) required for successful deployment will be provided by Bidder. Sizing of hardware and software is to be certified by prospective OEM and certificate from OEM along with bid is to be submitted by Bidder. Any other hardware or software or license required for deployment of EDR solution must be quoted by Bidder along with bid.
Endpoint Detection & Response (EDR) Features. Para5	Endpoint based EDR solution to protect all the endpoints across Network from Advanced Targeted Attacks and APT's.	The EDR solution must protect all the endpoints using a layered approach keeping in view the defence in depth security framework architecture across Network from Advanced Targeted Attacks

Endpoint Detection & Response (EDR) Features. Para 6	EDR solution must work on both signature based and a signature-less mechanism to stop threats via a single agent on the endpoint.	To be deleted
Endpoint Detection & Response (EDR) Features. Para 14	EDR solution must continuously monitor a critical event and its change of state in the system. It should generate an event that can execute responses.	EDR solution must continuously monitor a critical event in the system and should generate an alert /event that can capture the entire trail of execution flow and system responses.
Endpoint Detection & Response (EDR) Features. Para 17	EDR solution search box must understand simple syntax to combine collectors and build powerful search expressions and filters.	EDR solution search box must understand simple syntax to query large data set of end point data and build powerful search expressions, filters on stored or real time system data. Combine collectors and build powerful search expressions and filters.
Threat Intelligence Database for EDR Para 38	Threat intelligence database provided with the EDR solution should act as a reputation broker to enable adaptive threat detection and response.	To be deleted
Threat Intelligence Database for EDR Para 39	Threat intelligence database must have threat intelligence from imported global sources and allows local sources, including Endpoints and EDR solution to utilize/ query the same.	To be deleted
Threat Intelligence Database for EDR Para 40	Threat intelligence database must help in making decisions on never-before-seen files, based on endpoint context (file, process, and environmental attributes) blended with collective threat intelligence.	To be deleted
Threat Intelligence	If more information on a file is needed, Threat intelligence database must be able to send	To be deleted

Database for EDR Para 41	the file automatically to advanced analysis solutions e.g. Endpoint sandboxing solution, to immediately gain additional insight to potential new threats and determine the reputation of a file in question.	
Threat Intelligence Database for EDR Para 42	Threat intelligence database must be able to share relevant security intelligence in real time among endpoint solutions so that they can take the required actions against previously detected malicious files.	To be deleted
Endpoint Detection & Response (EDR) Features. Para 15	EDR solution must create a response in case of files deleted from the system by file hash.	EDR solution must create a response in case of files created / modified and deleted from the system file hash.
PRIVILEGE ACCESS MANAGEMENT : PAGE 88-90		
PAM Multi Factor Authentication Para 1	The MFA solution must support multiple authentication mechanism e.g. Hardware USB Token, Hardware Token, Mobile Token, email Token & SMS Token. A total of Qty 100 Tokens to be provided along with the solution.	The MFA solution must support multiple authentication mechanism e.g. Hardware USB Token, Hardware Token, Mobile Token, email Token & SMS Token. A total of Qty 100 Tokens to be provided along with the solution. 100 users and 1000 devices/ virtual machines to be integrated in this solution.
PAM Multi Factor Authentication Para 3	Support Android, IOS, Windows mobile, windows 10 (all build), Windows 8 and Windows 7 for soft token implementation.	Support windows 10 (all build), for soft token implementation.
LOG ARCHIVAL AND ANALYSIS SOLUTION : PAGE 91-95		
Log Archival And Analysis Solution Para 3	LA&A solution must be deployed in centralized architecture at five Datacentres have capability to handle 5,000 sustained EPS and 10,000 peak EPS from day one. LA&A solution architecture, licensing and hardware & software sizing must be designed and planned accordingly.	LA&A solution must be deployed in centralized architecture at five Datacentres in DC-DR with capability to handle 5,000 sustained EPS and 10,000 peak EPS from day one. LA&A solution architecture, licensing and hardware & software sizing must be designed and planned accordingly.

Log Archival And Analysis Solution Para 4	Bidder must quote solution which will be deployed on virtualized infrastructure. All hardware, software (i.e. Compute, Memory, storage, VMWare, Operating Systems (only Windows and RHEL, in case any other OS then must be quoted by bidder along with bid), DB and replication licenses) required for successful deployment will be provided by Buyer as per sizing requirements. Sizing of hardware and software is to be certified by prospective OEM and certificate from OEM along with bid is to be submitted by Bidder. Any other hardware or software or license other than mentioned above, required for deployment of LA&A solution must be quoted by Bidder along with bid.	Bidder must quote solution which will be deployed on virtualized infrastructure. All hardware sizing required for the solution to be catered additionally in the HCI sizing. Further the software, OS and DB (including any replication licenses) required for successful deployment will be provided by Bidder. Sizing of hardware and software is to be certified by prospective OEM and certificate from OEM along with bid is to be submitted by Bidder. Any other hardware or software or license other than mentioned above, required for deployment of LA&A solution must be quoted by Bidder along with bid.
Log Archival And Analysis Solution Para 13 (a)(iv)	Collectors must support integration with N Flow, Jflow.	Collectors must support integration with Netflow/ IPfix
Log Archival And Analysis Solution Para 13 (b)(ii)	The software must have in build capability for block-level de-duplication for data across different electronic data repository for storage optimization.	To be deleted
Log Archival And Analysis Solution Para 13 (b)(iii)	The software must be able to compress and encrypt data at client side, support for 128 bit AES, 256 Bit AES etc encryption algorithm is required.	The software must be able to compress and store the data in tamper proof manner to provide log authenticity.
NETWORK PACKET BROKER : PAGE 96 & 97		
Network Packet Broker para 2	1: N mirror function should be supported with max latency of 5ns.	1: N mirror function should be supported with max latency of 6ns.
Network Packet Broker para 6	Device should support Port to port L1 latency of less than 5 ns for TAP/ mirror function.	Device should support Port to port L1 latency of less than 6 ns for TAP/ mirror function.

Network Packet Broker para 18	TAP and Tap Aggregator should be from same OEM.	TAP and Tap Aggregator should be managed from a single pane of glass from same OEM. The management solution should be VM based and the required sizing and the licenses for managing the complete TAP and the TAP aggregator infrastructure of the buyer should be catered by the vendor. Total devices required are 05 TAP + 05 TAP Aggregator
-------------------------------------	--	---

CORRIGENDUM TO EOI I

AMENDMENTS TO APPENDIX 'D' ON

COMMERCIAL CLAUSES OF RFP

Clause / Para Number	Existing Clause	Revised Clause
COMMERCIAL CLAUSE PAGE 138		
Para 9 (a) (ii)	The Parties agree that the Joint Receipt Inspection (JRI) of delivered goods shall be conducted on arrival at each consignee site to be nominated by the Buyer. JRI shall be completed within 45 days of arrival of good at the Consignee. JRI will consist of (i) Quantitative checking to verify that the quantities of the delivered goods correspond to the quantities defined in this contract and the invoices. (ii) Complete functional checking of the stores/equipment as per specifications in the contract and as per procedures and tests laid down by Buyer but functional checking of spares shall not be done.	The Parties agree that the Joint Receipt Inspection (JRI) of delivered goods shall be conducted on arrival at each consignee site to be nominated by the Buyer. JRI shall be completed within 45 days of arrival of good at the Consignee. JRI will consist of Quantitative checking to verify that the quantities of the delivered goods correspond to the quantities defined in this contract and the invoices.

CoR= Customer of RailTel