

Request for Proposal
for
Private Server Cloud of SAC

April 2024



**Space Applications Centre
Indian Space Research Organization
Department of Space, GOI
Ambawadi Vistar PO
Ahmedabad 380001**

This Page is deliberately left blank.

**Request for Proposal
For
Private Server Cloud of SAC**

1. Introduction

Space Applications Center (SAC) is having its IT infrastructure running on 24 X 7 basis that offers services related to Web, FTP, Email, Internet Surfing, Library Resources, video resources and much more on Intranet as well as Internet. There is a need for augmenting the infrastructure using state of the art IT technology to manage it effectively and efficiently enhancing the quality of service of the offered IT services.

SAC already has Server Cloud based on Hyper Converged Infrastructure (HCI) technology that integrates compute and storage on x86 hardware with unified management console. SAC intends to extend the facility by procuring, and implementing HCI infrastructure to provide infrastructure, storage, networking and computing capacity to various ongoing projects and services as well as to different upcoming projects. The cloud solution will be used for all future hosting of applications that are cloud ready.

The RFP provides the specifications for the proposed solution/infrastructure for one time procurement as well as for Rate Contract. Vendor should propose the technical and commercial offer, which shall be complete in nature and as per the format requested in the RFP with no multiple options. The offer should include complete details like compliance with specifications, make and model/version no. etc. Vendor should propose commercial offers in the requested format for one time procurement (Annexure-2) as well as for Rate Contract of 3 years (Annexure-3) from the date of acceptance of solution. SAC reserves right to reject the incomplete or partial proposals without asking any further clarifications.

We are looking forward to the vendors who have experience in installation, commissioning and providing operational support for the stated infrastructure. The qualification criteria for Vendors and Original Equipment Manufacturers (OEM) are detailed in the RFP in later sections.

The Bidders are expected to examine all instructions, forms, terms, project requirements and other information in the RFP documents. Failure to furnish any information required as mentioned in the RFP documents or submission of a proposal not substantially responsive to the RFP documents in every respect will be at the Bidder's risk and may result in rejection of the proposal.

SAC reserves the rights to procure partial or complete solution of the RFP. Rights to decide appropriate solution and qualified vendors for the given RFP are also reserved with SAC.

2. Scope of work

The requirements are well defined and clearly mentioned in this RFP. As SAC has covered all elements required, this RFP will be treated as Scope of work.

If vendor finds any item which may be out of scope of work, it should be clearly mentioned in this section only. Vendor may quote additional item specific to their requirement which SAC may consider it within the scope of work.

The Scope of work includes the following but is not limited to:

1. Providing responses to the requirements and comply to the specifications mentioned in the RFP for one time procurement as well as for Rate Contract.
2. Provide demonstration by means of Proof of Capability and product walk-through (clearly demonstrating the capabilities as mentioned in the RFP) at SAC campus, without any cost implication to SAC, before commercial offer opening.
3. Supply, Installation, configuration, commissioning, operationalization and successful testing of the solution.
4. Supply & Integration of any additional component of the Rate Contract with the existing infrastructure procured under one-time procurement option.
5. Impart necessary on-site training (at SAC) and provide necessary documents regarding the solution.
6. Conversion/Migration of existing physical machines/virtual machines on proposed solution on best effort basis.
7. Providing Comprehensive 5 years 24 X 7 onsite warranty. The warranty period will start from successful completion of Acceptance Tests.
8. Providing onsite operational support and maintenance during warranty period.
9. Supply updates and upgrades including new versions of all the software licenses supplied as part of the tender during the warranty, support & subscription period.

For more details, Refer Section 3.0 to Section 10.0

3. Qualification Criteria

Note: Original Equipment Manufacturer (OEM) refers for all the items referred in Bill of Materials.

3.1. Solution Qualification Criteria

Sr. No.	Statement	Compliance by Vendor (Yes/No)
1	Vendor confirms that the offered solution meets all the requirements given in this RFP section 4 to 10.	

3.2. Vendor qualification

Sr. No.	Statement	Compliance by Vendor (Yes/No)
1	Should have Information Technology (IT) service and support center within Ahmedabad or Gandhinagar municipal limits since last 1 year, through which Vendor is providing services and support to his clients in Ahmedabad/Gujarat. Vendor should submit Documentary Proof to support this.	
2	“Vendor should have installed, commissioned and operationalized minimum 1 setup of HCI of at least 10 nodes, in India.” It is mandatory for the Vendor to provide the complete details of their installations in Annexure-1. Vendor should provide Documentary Proof to support this. These criteria	

	will be used in the final decision making. PI see Annexure-1.	
3	Should have minimum two OEM certified expert engineers (in HCI) to carry out installation & maintenance and to meet subsequent Operational Requirements. Vendor should provide Documentary Proof to support this.	
4	Should submit valid Manufacturer Authorization Form (MAF) from respective OEMs.	
5	Certificate from respective OEMs for back to back support during the complete warranty, support & subscription period for proposed solution mentioning SAC purchase tender reference number on their letter heads	
6	Vendor should submit documentary proof from HCI/Private Cloud software OEM as well as from the hardware OEM stating that hardware configuration and sizing are meeting the required specifications and the quoted hardware (including model/version details) is compatible with HCI and Private Cloud components and vice-versa.	
7	Non-Submission of any of the supporting documents for the above mentioned requirements will result in rejection of the proposal/offer.	
8	Vendor should not have been blacklisted by any government organization in India. Vendor shall submit the undertaking/self-declaration clearly supporting the same.	

3.3. OEMs qualification

Sr. No.	Statement	Compliance by -OEM (Yes/No)
1.	HCI OEM must have minimum 10 installation bases for its proposed HCI software in India with at least one setup of minimum 20 nodes in a single cluster. Documentary Proof for the same should be attached.	
2.	OEMs should have experience of at least 5 years in the field of proposed solution.	
3.	Supplied hardware and software are Virtualization compliant.	
4.	Any OEM participating in this bid should not have been blacklisted by any government organization in India. OEM shall submit the undertaking/self-declaration clearly supporting the same.	

4. Requirement Specifications

Following are the minimum required specifications for the proposed solution/infrastructure.

Respective OEM should confirm compliance with each of the specifications in the respective columns specified. Each page of the compliance should be duly signed with seal by the respective OEM.

Latest datasheets for the respective quoted product shall be enclosed with the offer, for verification of the technical requirements/specifications/features. Non-submission or incorrect submission of the latest datasheets may result in the offer getting rejected.

4.1. Common Specifications for Hyper Converged Infrastructure Solution

Compliance should be on respective OEM letterhead. Each page should have OEM seal, signature (not initials), name, designation and contact information of authorized signatory.

Item	Qty	Make and Model
Hyper Converged Infrastructure Solution		

Following are the minimum specification of each HCI setup.

Sr. No	Item Description	Compliance by OEM (Yes/No)
1.	HCI Platform-should be based on software-centric architecture and virtualization technology that integrates compute and storage on x86 hardware with unified management console.	
Hardware Specifications		
2.	The solution should use latest HCI-compliant x86 server hardware with 5th or latest generation of Intel Xeon Gold/Platinum CPU.	
3.	The solution should be able to support different generation of Intel processors in the same cluster.	
4.	The proposed HCI solution should be scalable to atleast 64 nodes in a single cluster.	
5.	Each server node in the solution must have its own Redundant Hot swappable Power Supply & cooling fans.	
6.	The hardware should provide features such as: (a) UEFI/BIOS Secure Boot (b) Secure Recovery i.e. recovery of critical firmware to last good known state in case of detection of untrusted/compromised firmware image (c) Immutable Silicon Hardware Root of Trust (d) TPM 2.0 compliance (e) Digitally signed and verified firmware updates (f) Ability to Roll-back firmware (g) Secure "System" Data erase	
7.	The hardware shall provide remote management & security features as follows: (a) Agentless management using out-of-band IPMI 2.0 compliant remote management port (b) Embedded features to manage servers in physical, local and remote environments.	

	(c) Remote Power management including group power control. (d) Monitoring, change recording and alerts for all system components such as BIOS, NICs, PCIe slots, Power supplies, disk drives, etc.	
8.	The solution shall provide scale-out (by adding nodes) and scale-down (by removing node from cluster) architecture with no disruption to the workloads already running on the platform.	
9.	Proposed HCI Solution should support industry standard hypervisors like Vmware VSphere or MS Hyper-V or Citrix Xen or Acropolis Hypervisor(AHV).	
10.	The HCI licenses should be hardware agnostic i.e. the licenses shall be transferrable to hardware from any other vendor/OEM (as certified by the HCI OEM) in case of hardware EOL, EOS or non-availability.	
11.	The proposed solution should support All Flash configuration from day one.	
Feature and Functionality		
12.	The solution shall provide a single console for management and automated provisioning of compute, network, storage, applications to conduct activities such as onboarding /managing hosts, virtual machines and storage through a multi-tenant IT service catalogue.	
13.	The HCI solution should support automatic replication/rebalancing in event of Disk/Node failure.	
14.	HCI nodes must automatically redistribute data equally across all nodes without migrating VMs while scaling out.	
15.	Resiliency: The solution should have ability to replicate VMs. The proposed solution must provide Synchronous/Near Synchronous and asynchronous replications and any licenses required for the same should be incorporated as part of the proposal.	
16.	Scalability: HCI solution should support dynamic scalability with Zero downtime and automated resource allocation during upgrades. The upgrade should be granular and in 1 node increments.	
17.	Interoperability: Proposed HCI solution should support mix and match various node configurations in the same cluster.	
18.	The proposed solution should provide upgrade for Firmware, Hypervisor, Storage OS, BIOS and other such functions, which are required in the HCI platform. The upgrade should be onsite and shall not affect the running workloads.	
19.	The proposed solution should provide File Services (NFS/ CIFS/ SMB) and iSCSI/ NFS protocols with or without use of 3rd party tools .	
20.	The solution should have QoS for IOPS at virtual machines and virtual disk level to provide granularity control. The HCI solution should have visibility on the virtual disk to physical disk mapping for easier fault isolation and monitoring.	
21.	The solution should provide per VM RAID configuration and shall be configurable on the fly i.e. without being powered off.	
22.	The Data protection mechanism should be part of the HCI solution with/without need to deploy a dedicated tool for data protection. It shall include features such as snapshots	

	(crash/application consistent), replication. All licenses required should be incorporated as part of the proposal.	
23.	The solution should have ability to create copies of Data at multiple sites i.e Local, Remote and cloud and should support one to one, one to many and many to one replication strategy. VM replication should be integral part of the HCI software.	
24.	The Protection Software must protect Virtual machines within the cluster. RPO should be 15 minutes or lesser.	
25.	The Software should use replication bandwidth efficiently i.e compress and dedupe data sent on link.	
Hypervisor		
26.	HCI Solution should provide a purpose built hypervisor that installs directly on the bare metal x86 server hardware with no dependence on general purpose OS for greater reliability and security.	
27.	Support for heterogeneous guest OS – Server OS such as Windows (Desktop & Server) and Linux flavors (Red Hat, SUSE, Ubuntu, CentOS). Bidder should do the migration of physical Windows and virtual workloads to proposed Hypervisor platform on best effort basis.	
28.	Proposed hypervisor should provide standard features like VM Migration, HA, DRS/ADS/PRO, Replication, Snapshots, Cloning of VMs & Load Balancing.	
29.	The solution shall support HA for VMs with a pass-through PCIe device or NVIDIA GPU.	
30.	Solution should provide abstraction of GPU pool to allocate to VMs for GPU intensive workloads.	
31.	Hypervisor shall provide the ability to hot add CPU and memory , hot-plug disks and NICs (provided the same is supported by guest OS)	
32.	The solution should have memory overprovisioning without impacting VM performance using memory management techniques such as Memory Ballooning and Memory Swapping.	
33.	The solution shall provide automated encrypted live migrations for initial placement and balancing of available resources with rules to define host affinity and anti-affinity for workloads (eg. 2 VMs providing availability for each other should all be placed on different hosts)	
34.	Integration of 3rd party endpoint security to secure the virtual machines with offloaded antivirus, antimalware, firewall solutions with/without the need for agents inside the virtual machines.	
35.	The solution should provide secure boot for protection for both the hypervisor and guest operating system by ensuring images have not been tampered with and preventing loading of unauthorized components	
36.	Hypervisor should support integrating external storage through FC, iSCSI and NFS.	
37.	Hypervisor shall have I/O prioritization for virtual workloads to ensure business critical VM's are not affected due to congestion of other VM's on the same host.	
38.	Hypervisor solution should provide VM & data encryption protection to protect unauthorized data access both at rest and in motion. Any licenses, if required (including licensing for any	

	KMS server, if required) should be included as part of proposal.	
39.	In-built enhanced host-level packet capture tool which will provide functionalities like SPAN, RSPAN, ERSPAN and will capture traffic at uplink, virtual switch port and virtual NIC level. It should also be able to capture dropped packets and trace the path of a packet with time stamp details.	
40.	The solution should support integrating Kubernetes with hypervisor for unified control of compute, network and storage resources to run both containers and virtual machines on the same platform from day-1.	
41.	Virtual machine performance reports generation for performance and utilization of virtual machines.	
Security & Network Virtualization Features		
42.	The solution should offer software-defined simplified, programmable, application of network & security policy to deploy virtualized network functions (like micro-segmentation, switching, routing, firewalling, VPN, DHCP and load-balancing).	
43.	The platform should have tight integration with the chosen hypervisor and HCI solution and should offer converged visibility and analytics that tie together compute, storage, network and security.	
44.	The solution should support basic routing methods such as OSPF and BGP at the logical level.	
45.	The solution should offer VXLAN (or similar) based logical virtual switching.	
46.	The solution should support port-mirroring capabilities to mirror traffic from one virtual port to another across the physical hosts and networks.	
47.	The Solution should offer Centrally managed distributed L2-L7 stateful firewall that is integrated into the virtualized host architecture and should protect every VM. Minimum firewall throughput across the cluster shall be 100 Gbps (HTTP 64 Kbyte). It should offer, virtualized workload at the vNIC level, to be protected at a granular level based on MAC, IP, Ports, security groups.	
48.	The solution should provide the ability to provide native application isolation for providing zero trust security for the application and should allow for on-demand creation of security groups and policies.	
49.	The solution should enable creation of security groups and security policies/ rules based on constructs like machine name, OS type, IP address, Logical Switches, Security Tags and other layer 7 application information.	
50.	The solution should provide the NAT function for multi-tenant deployment and automate network provisioning for tenants while enabling complete customization and isolation.	
51.	The solution should provide creation of per application server virtual load balancer with SSL offload capability which can be integrated with management platform. The solution should provide L4-L7 load balancer with <ul style="list-style-type: none"> • SSL throughput greater than 5 Gbps, • minimum SSL (RSA 2K) connections of 2000 • minimum SSL (ECC) connections of 2000. • GSLB between atleast 2 sites.& • WAF with minimum throughput of 1 Gbps. 	

52.	The Distributed/logical firewall at virtualization layer should have integration with Active Directory groups to provide Identity base firewall for different users, offer distributed Firewall and filter traffic based on logical groupings and also provides protection against MAC Address/ IP Address changes with spoof guard capability.	
53.	The solution should be capable to provide agent/agentless guest introspection services like Anti-Malware, Anti-Virus.	
54.	The solution should provide network introspection services like IPS, IDS with a minimum throughput of 15 Gbps across the cluster scalable upto 50 Gbps.	
55.	The solution should provide NetFlow assessment, Packet capture, Performance statistics granularity, flow monitoring granularity, all upto VM level. It should also have syslog support, activity (apps/users) monitoring support and network snapshot support.	
56.	The proposed solution must offer Micro segmentation for VM-level security (at the vNIC).	
57.	It must provide full network traffic visibility (VM-VM traffic flow) and visualization of communication between virtual machines. It should automatically analyze and recommend security policies to be applied to the VMs for secure traffic flow/microsegmentation.	
58.	The solution should offer visibility of all the virtual as well as physical hops on the path between two machines in a single view and should be able to generate report that includes amount of traffic that's East-West, Internet, VM to VM, VM to Physical, and Unprotected.	
59.	The solution should also offer threshold based / behavior based analytics for network and security for identifying any VMs exceeding its normal threshold limits or baselines calculated based on historical data.	
60.	The virtual solution should offer extending Layer-2 network across DC & DR, without re-architecture or any configuration on physical network.	
61.	The network and security virtualization solution also should work in high availability mode and redundant manner to avoid any single point of failure.	
62.	The HCI vendor/OEM may integrate/collaborate with a commercially supported third party solution with direct OEM support to achieve the Network & Security Virtualization requirements given above, if the above functionality is not available as integral part of the HCI solution. Vendor to ensure tight integration of the Network & Security Virtualization component with the proposed hypervisor.	
63.	Any hardware/software & corresponding licenses required for the above functionality should be incorporated as part of the proposal.	
Orchestration & Management Features		
64.	The solution should provide unified and centralized software defined datacenter platform that brings together compute, storage, networking and security virtualization in an integrated stack and is independent of the underlying hardware components.	
65.	The solution should support integration with the proposed HCI solution, hypervisor and the network & security virtualization components to automate delivery of virtual compute, virtual storage, virtual networking & security services.	

66.	Solution should provide automation and orchestration solution with unified multi-tenant service catalogue for automated delivery of IaaS, PaaS, XaaS/ SaaS services so that when VM/app is created it should automatically get the required virtualized compute, switching, routing, firewall, load balancing and security services without any manual intervention.	
67.	The solution shall provide predictive analytics capabilities to understand baselines and model capacity and demand for accurate forecasting of infrastructure requirements.	
68.	Solution should monitor utilization of running VMs and should reclaim resources from idle VMs and allocate to other VMs in automated fashion.	
69.	The solution should provide proactive monitoring and management of the physical/logical topology and the overall infrastructure of the software defined data center to monitor and provide real-time insight into the infrastructure behavior, upcoming problems/risks/failures and opportunities for efficiency improvements as part of operations management.	
70.	The solution should include unique lifecycle management services that automate day 0 to day 2 operations, from bringing up to configuration, resources provisioning and patching/upgrades.	
71.	The solution should support integration of container technologies such as Docker and container management tools such as kubernetes, etc	
72.	The solution should have the self-service capabilities for provisioning the services (IaaS, PaaS, etc.) through the available catalogue or create customized templates. The users must be able to access and control the resources of the services allocated through the web-portal.	
73.	The solution should have the pre-defined workflows or create customized ones to automate the service process, right from requesting the resources, obtaining approvals and the deployment of VM. It should have the facility for email notifications for the same.	
74.	The solution should support automation and orchestration via both portal and API. It should have the ability to create customized workflows through SOAP, REST and Powershell scripts.	
75.	The solution must provide a comprehensive set of REST APIs and integrate with service automation deployment and configuration management tools to facilitate provisioning, maintaining and decommissioning resources through REST APIs	
76.	The solution should have the facility to enable the users to request new IT services and extend the operational capabilities of the service/VM to the owner/requestor through the self-service portals and defined workflows and access the machine through RDP/SSH with/without secure VPN based channel.	
77.	The solution should have the facility to define the validity (service end date/time) of the service granted so as to automatically reclaim the granted resources back.	
78.	The solution should have the auto-scaling feature which allows to adapt to the workloads by automatically scaling the resources.	

79.	The solution should provide capacity analytics and provide infrastructure and operations log analytics to eliminate time-consuming processes through root-cause analysis.	
80.	The private cloud orchestration & management solution also should work in high availability mode and redundant manner to avoid any single point of failure.	
81.	The HCI vendor/OEM may integrate/collaborate with a commercially supported third party solution with direct OEM support to achieve the private cloud orchestration & management requirements given above, if the above functionality is not available as part of the HCI solution. Vendor to ensure tight integration of the private cloud orchestration & management component with the proposed hypervisor.	
82.	Any hardware/software & corresponding licenses required for the above functionality should be incorporated as part of the proposal.	
Log Management, Monitoring and Reporting		
83.	The solution should also have the log-management, monitoring and reporting capabilities including customization of reports and dashboards, web-based dashboard for managing the private cloud and ability to provide time period based reports.	
84.	The solution should tightly integrate with the proposed hypervisor, HCI solution, network and security virtualization and the cloud management solution, to deliver heterogeneous and highly scalable log management with intuitive, actionable dashboards, sophisticated analytics and broad third-party extensibility.	
85.	Solution should provide deep operational visibility and faster troubleshooting and root cause analysis across physical, virtual environments.	
86.	Solution should be able to collect and analyze all types of machine-generated log data and able to connect it to everything in the environment—operating systems (including Linux and Windows), applications, servers, storage, firewalls, network devices etc.—for enterprise-wide visibility via log analytics. Solution should be able to preserve logs for a duration of at least one year without over-writing.	
87.	Solution should have the ability to archive logs to a remote storage/location.	
88.	The log management, monitoring and reporting solution should work in high availability mode and redundant manner to avoid any single point of failure.	
89.	The HCI vendor/OEM may integrate/collaborate with a commercially supported third party solution with direct OEM support to achieve the log management, monitoring and reporting requirements given above, if the above functionality is not available as part of the HCI solution. Vendor to ensure tight integration of the log management, monitoring and reporting component with the proposed hypervisor.	
90.	Any hardware/software & corresponding licenses required for the above functionality should be incorporated as part of the proposal.	

4.1.1. Specific Requirements for HCI Solution (One Time Procurement) – Unit

Quantity – 1 No.

1.	Hyper-converged solution must provide desired capacity using All-Flash (SSD/NVMe) drives. Vendor should provide Enterprise class SSD/NVMe with high endurance, greater than or equal to 1 DWPD drives for 5 years for all drives.	
2.	HCI solution should provide minimum 4 X 25G or more SFP28 ports per node. All ports must be prepopulated with transceiver modules.	
3.	Solution should provide minimum 2 x 32 G FC-HBA cards.	
4.	HCI solution should provide 1 x 1G or more out of band management port per node.	
5.	<p>HCI should provide minimum: Usable 600 Cores or more of Compute with 5th or latest generation of Intel Xeon Gold/Platinum processor with 2.1 GHz or higher clock speed per CPU and usable 10 TB or more RAM. It should include 400 TB or more Usable storage capacity without any Deduplication, Compression.</p> <ul style="list-style-type: none"> • The solution shall be able to sustain atleast 1 node failure. • The above-mentioned compute, RAM and usable storage capacity shall be made available even after 1 node failure and shall spread evenly across multiple nodes. • The solution should be designed with FTT=1/RF=2, RAID-1. • Any overheads must be factored over and above the usable capacity. • Node sizing shall be such that each node has minimum of 64 or more cores (32 cores/socket) and 1024 GB or more RAM. • Each node shall have minimum of 16 drive bays for accommodating SSD/NVMe. 	
6.	The proposed HCI solution must provide Data Compression and Deduplication natively and licenses, if any, the same should be incorporated as part of the proposal.	
7.	The solution should support adding nodes with GPU cards. It should enable native 2D and 3D graphics performance for virtual machines and should support multiple vGPUs per VM with capability to suspend and resume capabilities of vGPUs. The solution should support latest NVIDIA GPU cards such as H100/A40/A16 for running compute & graphic intensive applications.	
8.	The solution should support GPU Passthrough for VMs.	
9.	The solution should provide 4 no. NVIDIA H100 80 GB GPU (one per node). All nodes in the solution should have the provision to accommodate at-least 2 NVIDIA cards per node	

	with the latest PCIe cards available for future scalability. Any licenses required for using GPU as such or as vGPU shall be included as part of the proposal.	
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------	--

4.2. Specification for Microsoft Operating System

Product Name	Product Description	Quantity	Compliance by Vendor (Yes/No)
Microsoft server license	Microsoft Windows Server Datacenter edition (latest available version)	Vendor to ensure to provide core based license to license at least 4 nodes provided as part of the solution referred in 4.1, 4.1.1	

4.3. Specifications for Red-Hat Operating System

Product Name	Product Description	Quantity	Compliance by Vendor (Yes/No)
Red-Hat Operating System	Red-Hat Enterprise Linux For Virtual Datacentres, Standard (Latest Version with Updates) with 5 years of standard support & subscription for 2 socket servers	4	

Note: SAC will provide the remaining licenses from the available licenses, Vendor should support installations and activation of these licenses. Linux Guest OS will be provided by SAC.

5.0 System Architecture

In this section, vendor should provide architecture document providing complete technical details covering architecture, design, deployment, interfaces with components, data flow, event flow, installation and commissioning model, integration, data migration etc. for realizing the solution.

6.0 Installation and Commissioning for Overall Solution

Sr. No.	Statement	Compliance by Vendor (Yes/No)
1	Vendor should provide turnkey solution that includes installation, configuration and integration of Servers, storage, HCI solution (compute & storage virtualization), Network & Security Virtualization solution, cloud management solution, log management solution, and OS	

	<p>with all required components and accessories etc. at SAC Ahmedabad with no single point of failure. Vendor should take responsibility that all the quoted items are compatible and interoperable with each other and perform the required functions as demanded in the RFP.</p> <p>Having a particular required feature in the component/product and not performing its intended function, when integrated with the overall solution may lead to rejection of the offer.</p>	
2	<p>The Bidder shall be responsible for installation and commissioning of the Systems including cabling and other related activities such as unpacking, inspection etc. for which SAC shall provide the required space. While unpacking and installation the Bidder shall check physical availability of items as per the packing list. Delivery of goods or products shall be deemed to have been made when the contents are installed and components are witnessed together by SAC and the Bidder or their representatives, to be identical to those listed in the packing list included therein. Delivery is considered complete once items are accepted by SAC. However, this proof of delivery to the final destination shall in no way absolve/release the Bidder from the performance of his warranty obligations under the agreement/ contract.</p>	
3	<p>The planning and installation shall be done by the respective subject experts from OEM.</p>	
4	<p>Vendor should also convert our existing physical machines to virtual machines on proposed solution, which are compatible, on best efforts basis.</p>	
5	<p>Vendor should make the complete system operational.</p>	
6	<p>Vendor should deliver the solution within 16 weeks from date of purchase order, Installation and commissioning should be carried out within 1 month or earlier from date of delivery. After installation, configuration, data migration and self-test by the vendor, ATP will be done. Vendor to prepare and submit mutually agreed upon ATP document for acceptance testing. Any shortcoming in delivery, configuration etc. found during acceptance planning has to be addressed by the vendor, any time involved in this will be accounted as part of installation time.</p> <p>Complete ATP should be completed within 30 days after successful installation and commissioning of the solution. Installation & commissioning to be certified by the identified nodal person from SAC.</p>	
7	<p>Upgrades to new versions released should be implemented during Warranty.</p>	
8	<p>Notification about the new compatible released final versions must be intimated to SAC immediately after release date.</p>	
9	<p>New compatible version should be operationalized at SAC preferably within 10 days and maximum of 30 days from an operationally stable release.</p>	
10	<p>If SAC desires to relocate the data centre for SAC Private Cloud to any other location within Ahmedabad, during the implementation/post implementation and within the contract period, the vendor shall assist in de-installation and reinstallation of entire solution. However, this exercise may</p>	

	be on chargeable basis. Charges for the same shall be quoted as part of Annexure-3.	
--	-------------------------------------------------------------------------------------	--

7.0 Warranty

Sr. No.	Statement	Compliance by Vendor (Yes/No)
1	Vendor should provide 5 years, 24 X 7 comprehensive onsite warranty, support & subscription with advance part replacement & direct principal back lined support for all the supplied hardware and software items. The warranty, support & subscription will start from the date of successful Acceptance Testing and operationalization of the supplied solution at SAC. During the warranty period, vendor is required to install upgrades, new releases and handle the faults/problems at no extra cost.	
2	In case of disk failure, vendor should replace it without any cost implication to SAC. Faulty Disk will be retained by SAC.	
3	Supplied hardware and software warranty should have back to back OEM support. Bidder should submit the required documents from respective OEM.	
4	Penalty Clause: In case operational support found unsatisfactory (issue not resolved within 6 hours from the time of reporting), penalty will be recovered from the vendor at 0.5% of the quarterly onsite operational support & maintenance cost upto a maximum of 10% of the quarterly payment due against onsite operational support & maintenance, per 24 hours after expiration of 6 hours of reporting. Recovery will be done from onsite operational support & maintenance charges.	

8.0 Operational Support during Warranty, support & subscription period

Sr. No.	Statement	Compliance by Vendor (Yes/No)
1	Onsite operational, maintenance and administration support should be provided by a OEM certified expert engineer from OEM/Vendor during warranty, support & subscription for all the products factored in the solution.	
2	During warranty, support & subscription period, any Operational issue related to the proposed solution should be resolved within 6 hours from the time of reporting.	
3	Along with the onsite operational support, <u>all</u> the components of the Private Cloud Infrastructure should have unlimited critical/emergency (highest) incident support with L1, L2, L3 level technical support (Email, Web & Telephonic) directly from respective OEM. The support should be available 24x7x365 with unlimited software updates and upgrades during the complete tenure of the agreement without any additional cost, during the validity of the agreement.	
4	As per ISRO policy, remote access over internet of any device (hardware or software) connected on intranet (i.e.	

	SACNET) network is not permitted. To address the same, vendor authorized, qualified person must visit SAC campus for required operational support.	
5	The bidder should deploy at-least 2 no. on-site manpower as part of the onsite operations and maintenance. The deployed manpower shall be Graduate Engineer (B.E/B.Tech(IT/CS)/MCA) and have OEM certification for the required components of Private Cloud which are part of this RFP. The deployed manpower shall be able to manage the infrastructure from day-1.	
6	Uninformed or un-approved absence from duty (i.e. without approval from the focal person at SAC) may result in penalty being levied at Rs. 500 per manpower per day which may be deducted from the operational support cost or PBG due to the bidder.	
7	Statutory Compliance: Vendor is expected to abide by the laws of the land including prevailing labour laws with respect to the personnel deployed at SAC. SAC will not be responsible of any liability in this regard.	

9.0 Terms and Conditions

Sr. No.	Statement	Compliance by Vendor (Yes/No)
1	Vendor must troubleshoot and resolve any problem arising in their offered solution, hardware and software during the warranty period without any cost implications to SAC.	
2	Vendor must not quote items which are declared 'End of Support' by OEM in next 5 years from the date of tender. Vendor must not quote items which are declared 'End of Sale' by OEM in next 1 years from the date of tender.	
3	Technical and commercial offer should contain make and model/version of all the components of the solution offered.	
4	SAC may ask the vendor/OEM to host/implement minimal setup required of the proposed solution at SAC, Ahmedabad to carry out the integrated PoC for the private cloud solution. The vendor is expected to have respective subject/matter experts available to answer any queries pertaining to the solution. Necessary arrangements for the PoC to be made by the vendor/OEM at SAC. SAC will arrange the entry gate passes for the material and personnel. The PoC has to be carried out during the technical evaluation stage. Exact time slots and duration for the same shall be intimated to vendor at later stage. The vendor must start the PoC within 15 days of the intimation from SAC and complete the same within 15 days of starting the PoC. During the PoC, the vendor shall demonstrate the specifications/features/requirements as per the RFP, in detail and SAC will verify the same.	

	SAC reserves the right to disqualify the bidder and respective proposal in case of failure to demonstrate any of the required capabilities.	
5	Offer should be complete along with compliance as required. SAC reserves rights to reject incomplete or partial offer without asking for any clarification.	
6	No optional item(s) should be quoted. Offers with optional items will be straight forward rejected.	
7	The bidder on awarding the PO, is understood to have automatically entered a Confidentiality and Non-Disclosure agreement as an undertaking that they shall not disclose any information acquired while dealing with the project which may be confidential in nature. Signing of any formal undertaking/agreement regarding the same is at the discretion of SAC and the bidder may be asked to formally enter the Non-Disclosure agreement while awarding the PO.	
8	In case the Supplier / Contractor does not fulfill their obligations as required in accordance with the terms and conditions of the same, including the execution of rate contract requirements, provisions for default on the part of Contractor shall be invoked. The Purchaser reserves its rights to forfeit securities submitted by the Contractor against the contract in addition to recovery and impositions of any other penalties provided for including re-appraisal of the Supplier's performance and their qualification for future tenders.	

10.0 Training and Documents

Sr. No.	Statement	Compliance by Vendor (Yes/No)
1	Training should be provided to Administrator, IT team and Operators for day to day system administration and operations for supplied solution for minimum 5 days including hands on practice at SAC. The training should necessarily cover the products supplied to meet the functional and technical specifications mentioned in the RFP.	
2	Pre-Implementation: Training should be provided to SAC IT team on the product architecture, functionality and the design for each solution under the scope of this RFP. Post-Implementation: Training should be provided to SAC IT team on operations, alert monitoring, security orchestration, policy configuration for all in-scope solutions, routine operations, management, monitoring, etc. The Bidder shall train SAC's IT Team for independent operation, creation of policies/rules, generation of reports, and analysis of the reports, troubleshooting and familiarization of features and functionalities, policy configuration, alert monitoring.	
3	Offline softcopy of all manuals must be made available to Administrator, IT Team and operators.	
4	Architecture document as already specified in Section 5.0 of this RFP shall be provided by the bidder/OEM.	

11.0 Payment Terms

Sr. No.	Statement	Compliance by Vendor (Yes/No)
1	50% of payment of supplied material (hardware and software) shall be paid against delivery and inspection of supplied material. Remaining payment will be paid within 30 days after successful completion of Final Acceptance Test. Any software component will be considered delivered only after the delivery of complete hardware for the solution.	
2	Onsite operational support payment will be made on quarterly basis post facto after submission of satisfactory certificate from identified nodal person.	

12.0 Bidding Model

Vendor should submit the offer in two parts

(a) Technical and Commercial offer with terms and conditions

a. Technical offer should cover

- Compliance (Yes/No) by OEM for respective products in their letter head, with sign of authorized signatory and seal on each page of the offer along with supporting datasheets/documents.
- Compliance by vendor with signature & stamp of vendor's designated personnel on each and every page of the offer.
- Complete masked Bill of material (Annexure-2) (un-priced).
- Complete masked Rate Contract for 3 years (Annexure-3) (un-priced BoM).
- Vendor should submit Technical & commercial terms and conditions, if any, in the technical offer only.
- **Vendor shall not disclose any prices with the technical bid/details. Disclosing any prices will lead to rejection of offer.**

(b) Price Bid

- a. Price Bid should contain Bill of Material (Annexure-2) & Rate Contract (Annexure-3) with price. Commercial Bill of Material should be identical to un-priced BoM. Any terms and conditions mentioned in commercial offer will not be considered.
- b. Total Price (T_{total}) mentioned in Annexure-4 will be considered for calculating L1 for the allotment of contract.

Annexure-1: Experience of Installation, Commissioning and Operational Support of HCI Solution

Sr. No.	Installation Site Name	Size	Location	Contact Person Name, Telephone and email address

Note:

1. Vendor should support Documentary Proof to support this.
2. These criteria will be used in the final decision making without any further clarifications.

Annexure – 2: Bill of Material (BoM)

Sr. No.	Item	Unit Price	Quantity	Tax (%)	Total Price
1.	Hyper Converged Infrastructure solution-(as specified in Ref. 4.1 & 4.1.1)				
2.	Microsoft Windows Server 2022 Datacenter edition (as specified in Ref. 4.2)				
3.	Red-Hat Enterprise Linux For Virtual Datacentres, Standard (Latest Version with Updates) with 5 years of standard support & subscription for 2 socket servers (as specified in Ref. 4.3)				
4.	Installation and Commissioning (as specified in Ref. 6.0)				
5.	Onsite Operational Support during Warranty period on 9X6 basis (as specified in Ref. 8.0)				
6.	Any additional item (if required for offered solution)*				
Total (T_{BoM})					

*Add separate row for each item.

- Vendor is requested to fill appropriate value in each field. No field should be left blank or filled with “-” or “N/A”.
- **Vendor shall not disclose any prices with the technical bid/details. Disclosing any prices will lead to rejection of offer.**
- Un-Priced BoM shall be same as priced BoM.

Annexure – 3: Rate Contract for 3 years after acceptance of the solution

- Unit price should include respective items, delivery, installation, commissioning and any associated accessories required for installation and commissioning and making the unit operational. The item(s) procured as part of Rate contract may / may-not be (at SAC discretion) integrated with the existing private cloud solution procured as part of this RFP.
- Any items which is not present below and is required to build the private cloud solution (as specified in section 4.1 – 4.4) should be added below by the vendor in the other items row(s). Additional row shall be added for each item.
- Each component procured during rate contract shall have warranty/support & subscription for 5 years from the date of its procurement.

For Hyper Converged Infrastructure Solution (section 4.1)

Sr. No.	Item	Quantity Required to build the proposed solution* (Qi)	Unit Price during 1 st year of RC (Uia)	Unit Price during 2 nd year of RC (Uib)	Unit Price during 3 rd year of RC (Uic)	Unit Price (Ui _(avg)) [(Uia+Uib+Uic)/3]	Total Rate Contract Cost for L1 evaluation (Ti = QiUi _(avg))
1.	HCI Node (with same node configuration as proposed for 4.1.1) with all the required software & hardware licenses to achieve the technical specifications and other hardware specifications for HCI Solution as mentioned in Section 4.1 and 4.1.1 respectively (Without NVIDIA GPU Card).						
2.	HCI Node (with same node configuration as proposed for 4.1.2) with all the required software & hardware licenses to achieve the technical specifications and other hardware specifications for HCI Solution as mentioned in Section 4.1 and 4.1.2 respectively (With NVIDIA GPU Card).						
4.	NVIDIA H100 80 GB GPU. (This shall include any component/accessory/s oftware/license required to install the GPU card in the HCI node already						

	procured or may be procured from Rate Contract)						
For Microsoft Windows Server 2022 Datacenter Edition							
6.	Microsoft Windows Server 2022 Datacenter edition – 16 core License						
For Red-Hat Enterprise Linux for Virtual Datacentres							
7.	Red-Hat Enterprise Linux For Virtual Datacentres, Standard (Latest Version with Updates) with 5 years of standard support & subscription for 2 socket servers						
Any Other Item							
8.	De-installation & Re-installation charges (Ref. Sr. No. 10 of Section 6.0)	1					
Any Other Item							
n.	Other items ...*						

* as proposed in Annexure -2

Annexure – 4: L1 evaluation methodology

1. Total Price of Rate Contract component for L1 evaluation will be calculated based on values in Annexure 3 as per the following. However, it is upto SAC discretion to procure any, all or none of the items as per the quoted prices from the Rate Contract.

$$T_{RC} = \sum_{i=1}^n T_i = T_1 + T_2 + \dots + T_n$$

where n is total number of items quoted in rate contract

2. Total Price (T_{total}) which will be used for determining L1 during commercial evaluation, will be based on T_{BOM} mentioned in Annexure-2 and T_{RC} calculated above, and is defined as per the following

$$T_{total} = 4 \times T_{RC} + T_{BOM}$$

This Page is deliberately left blank.