Purchase of HCI

Additional Eligibility Evaluation Criteria:

S/N	Eligibility Criteria	Attachments
1.	The bidder would be a company registered/incorporated under Indian company Act. and must have 5 years of existence in India. **AND** Bidder should be an established IT System Integrator and should have been engaged in similar IT projects/solutions business for a period of at least five years as on the bid issuance date.	Copy of certificate of Incorporation, PAN and GST registration Certificate. Work Orders / Client Certificates confirming year and area of activity should be enclosed.
2.	The bidder should have a total sum of turnover of Rs. 20 Crore (Minimum) in the last three financial years as on 31st March 2021.	The copies of Audited Annual Accounts/Balance Sheet along with Profit & Loss Account and CA Certified Statement for last three financial years as on 31st March 2021 shall be attached along with the bid.
3.	The OEM of the proposed product should have a total sum of turnover of Rs. 1000 Crore (Minimum) in the last three financial years as on 31st March 2022.	The copies of Audited Annual Accounts/Balance Sheet along with Profit & Loss Account and CA Certified Statement for last three financial years as on 31st March 2022 shall be attached along with the bid.
4.	The bidder should have experience in Supply, Installation, Testing and Commissioning (SITC) of Data Centre IT Infrastructure i.e. Server, Storage, Virtualization, Network and Security. Bidder Should have executed on premises Data Center IT Infrastructure related work order of minimum one work order value of 10 Cr or two order of value 7 Cr in the last Five financial years as on bid submission. All work orders / contracts should be in the name of the bidder	Details of such projects undertaken along with work order/purchase order copy/clients' on-going or completion certification/letter signed by authorized signatory or company secretary with the details w.r.t to the clause should be enclosed.
5.	OEM of Proposed solution (Hardware & Virtualization stack) should have existence in India for the last Five years as on bid submission date.	OEM Undertaking confirming the existence along with copies of work completion certificate or work order/purchase order.
6.	HCI solution must have been implemented at Minimum two locations/Projects for Central / State Gov, PSU, BFSI in India during the last five years as on Bid submission date.	Relevant Work order copy / client satisfactory letter regarding successful implementation HCI in the name of the bidder is to be submitted. The PO/Workorder/contracts / letter should be in the name of the bidder and clearly mention the scope of work.
7.	Bidder and OEM should not be blacklisted by any Ministry of Government of India or by any State Government of India or any of the Government PSUs at the time of bidding.	Self-Declaration/Certificate/affidavit mentioning that the Bidder is not blacklisted as per the clause.

8.	The bidder should be authorized by the OEMs of the proposed equipment/devices to bid for this tender	MAF for Authorized partner. Self-declaration if the bidder is an OEM.
9.	The Bidder should have at least one office in Gujarat If the Bidder is not having any office in Gujarat, then bidder should submit a letter of undertaking to open the office in Gujarat within 45 days from the date of award.	The copy of Property tax bill/Electricity Bill/Telephone Bill/GST/CST should be enclosed. Registration/Lease agreement should be submitted as proof Or Undertaking Letter should be enclosed.

Note:

1. All the details and the supportive documents for the above-mentioned items should be uploaded in the bid.
2. Bidder's experience, bidder's turn over criteria will not be considered of GeM bid, however bidder must match eligibility criteria, experience, bidder's turn over criteria, as mentioned in this document and will be considered for evaluation.
3. Bidder should be authorized by the OEM to quote this bid. MAF of Server, Storage, Network Switch, Firewall, Software should be submitted.

Pre-bid Meeting

Date and Time :- 10-11-2022 : 13:00, At Gujarat Informatics Limited, Block No. 2, 2nd Floor, C & D Wing, Karmayogi Bhavan, Sector - 10 A, Gandhinagar - 382010 Gujarat.

Queries to be submitted: Dy Director (IT), Gujarat Informatics Limited, Block No. 2, 2nd Floor, Karmayogi Bhavan, Sector-10A, Gandhinagar 382 010

E-mail: ddict-gil@gujarat.gov.in, mgrhninfra-gil@gujarat.gov.in, rajesh_patel@emri.in

Scope of Work:

1. The scope is to supply install, configure, test and commission Hyper Converged Infrastructure as per specification mentioned in this document along with Network, Security, Software and required hardware, software (including all active and passive components and sub-components) and necessary licenses, if any along with the 5 years of Comprehensive warranty and OEM Support at GVK Emergency Management and Research Institute 108 Emergency Management Centre .
2. Bidder is required to supply, install, configure, test and commission the required Hardware and software compute (inclusive of all active & passive components and sub components, accessories) as per the technical and functional specification mentioned in the RFP document.
3. The OEM support credentials should in name of GVK / Health Department and handed over to GVK/Health Department.
4. The bidder is responsible for physical connectivity of the proposed solution.
5. The Bidder shall configure the proposed solution in such a way that it should comply with all the policies of the GVK.
6. The bidder is required to submit the certification from the OEM of the proposed solution confirming successful implementation, testing, commissioning and satisfactory deployment of the proposed solution based on the industry best practices as a part of FAT.
7. The bidder shall have to provide various documents like technical document of delivered product, Standard Operating Procedures Templates, Troubleshooting guide, "How-To" knowledge base, Escalation matrix etc.
8. Successful bidder in coordination with the representatives from the GVK/GIL is required to conduct FAT of the solution.
9. The successful bidder shall be responsible for obtaining installation, commissioning and FAT certificate (Sign-off) on completion of the work as per the scope of work, functional and technical requirements.
10. The Successful bidder shall be responsible for rectification of discrepancies identified by the GVK/any other authorized representative while conducting FAT. Further on rectification of all the discrepancies identified during the FAT, GVK/GIL representative will re-conduct the FAT or if agreed FAT will be signed.
11. After FAT, successful bidder has to handover to GVK for O&M.

12. **Warranty Support:** As part of the warranty services bidder shall provide:
    1.1. Bidder shall provide a comprehensive on-site free warranty for 5 years from the date of FAT for proposed solution.
    1.2. Bidder shall also obtain the five year OEM premium support (ATS/AMC) on all licensed software, hardware and other equipment for providing OEM support during the warranty period.
    1.3. Bidder shall provide the comprehensive manufacturer's warranty and support in respect of proper design, quality and workmanship of all hardware, equipment, accessories etc. covered by the bid. Bidder must warrant all hardware, equipment, accessories, spare parts, software etc. procured and implemented as per this bid against any manufacturing defects during the warranty period.
    1.4. Bidder shall provide the performance warranty in respect of performance of the installed hardware and software to meet the performance requirements and service levels in the bid.
    1.5. Bidder is responsible for sizing and procuring the necessary hardware and software licenses as per the performance requirements provided in the bid. During the warranty period bidder, shall replace or augment or procure higher-level new equipment or additional licenses at no additional cost in case the procured hardware or software is not adequate to meet the service levels.
    1.6. Mean Time between Failures (MTBF): If during contract period, any equipment has a hardware failure on four or more occasions in a period of less than three months, it shall be replaced by equivalent or higher-level new equipment by the bidder at no cost. For any delay in making available the replacement and repaired equipment's for inspection, delivery of equipment's or for commissioning of the systems or for acceptance tests / checks on per site basis, DST/GIL reserves the right to charge a penalty.
    1.7. During the warranty period bidder, shall maintain the systems and repair / replace at the installed site, at no charge, all defective components that are brought to the bidder notice.
    1.8. The bidder shall as far as possible repair/ replace the equipment at site.
    1.9. Warranty should not become void, if GVK/GIL buys, any other supplemental hardware from a third party and installs it within these machines under intimation to the bidder. However, the warranty will not apply to such supplemental hardware items installed.
    1.10. The bidder shall carry out Preventive Maintenance (PM), including cleaning of interior and exterior, of all hardware and testing for virus, if any, and should maintain proper records at each site for such PM. Failure to carry out such PM will be a breach of warranty and the warranty period will be extended by the period of delay in PM.
    1.11. Bidder shall monitor warranties to check adherence to preventive and repair maintenance terms and conditions.
    1.12. Bidder shall ensure that the warranty complies with the agreed Technical Standards, Security Requirements, Operating Procedures, and Recovery Procedures.
    1.13. Bidder shall have to stock and provide adequate onsite and offsite spare parts and spare component to ensure that the uptime commitment as per SLA is met.
    1.14. Any component that is reported to be down on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame indicated in the Service Level Agreement (SLA).
    1.15. Bidder shall develop and maintain an inventory database to include the registered hardware warranties.

Minimum Specification

Specification of Hyper Converged Infrastructure & other Hardware		
Hyper Converged Infrastructure		
Sr.No.	Component	Description
1	Hyper Converged Appliance	Proposed HCI Solution must be hardware OEM Agnostic and must support all the major OEM for the future investment protection. And the license must be portable to the other hardware OEM procured in future.
		Fully Software Defined Hyperconverged Infrastructure Appliance/Technology (Compute, Storage and Management). Technology must be software defined, so that the technology is all integrated and cannot be broken out into separate components of Server and functional Storage on its own.
		Appliance/Technology should NOT have any hardware dependency to enable Hyper Converged Solution.
		~~Solution should also have capability to use Software Defined Networking, must propose the Logical FW Solution from day-1 considering the GVK Security.~~
	Config	*The cluster should be configured with minimum 5 All Flash Node : *280 physical usable cores, 1.5TB ram, 60TB usable storage capacity (W/O Deduplication Compression and Erasure Coadding) across the 5 node cluster. (w/O HCI & Management Overhead, Bidder need to consider the HCI & Management overhead Separately) *Each Node must be populated with minimum 2*1.6TB SSD or more per node for caching and full capacity of the SSD must be available to server caching and capacity requirement, Caching must be redundant in nature and failure of single SSD must not consider as a node failure *Each node should be Configured with 4*10/25Gbps LAN ports.
		HCI Appliance/Technology should be listed on OEM website and analyst reports
	Redundancy & Business Continuity	Solution should have No Single Point of Failure with complete redundancy at all levels considering FTTR=1 with RAID- 1(Mirroring) Performance or RF=2 and solution should be sized to support data & cluster availability in event of one Node Failure (N+1). The proposed HCI solution must support Data Compression, Deduplication and Erasure Coding natively and licenses, if any, the same should be incorporated as part of the proposal.
		Solution must support Asynchronous / Synchronous replication and also be
		capable of providing zero data loss, minimum downtime of VMs from day one within the same cluster
		Storage must have capability to integrate within the Hypervisor kernel itself or should be using virtual storage controller architecture.
	Storage Feature	The solution support for automated non-disruptive upgrades of SDS through management GUI with no downtime and major impact on production
		Storage availability and performance service level objectives should be managed from VM and changed non-disruptively at any point in time
		Storage policies should be enforced directly from hypervisor and managed directly from hypervisor.
		Single Web Interface Central Management for Compute, Network, Storage and Clustering.
		Single Click Upgrade/Update for all components of compute (including network adapter, BIOS), hypervisor and SDS
		The Solution should be able to monitor end to end session of the user including giving the insight of the underlying infrastructure like server and Storage
		HCI monitoring console should display up-to-date hypervisor usage statistics like CPU, memory, IOPS across cluster and for a particular vm and should match corresponding statistics as per hypervisor element manager for real time monitoring and diagnostics. Stats should be collected directly through hypervisor

		element manager only. it must also have a operation Management portal for reporting, alerting and monitoring.
		On demand single click upgrade for the complete HCI infrastructure including, hypervisor element manager, sds, bios, drive/nic firmware, hypervisor, etc
		The HCI management GUI should have capability to display hypervisor performance and usage statistics for real time monitoring and diagnostics. HCI solution must analyse capacity trends and operations analytics. It should also provide performance bottleneck detection, performance behaviours, detects anomalies, and enable automated remediation. The solution should provide customized dashboard functionality with advanced reporting features including capacity analytics which can identify over-provisioned resources so they can be right_sized for most efficient use of virtualized resources.
		Platform must support monitoring via SNMPv3 and email alerting via SMTP.
		HCI Solution should be able to provide Quality of Service measures on Storage and Network Operations. This is to ensure minimum IOPS (performance) to critical applications
	Scalability	Proposed solution should be able to scale 64 nodes of similar types within the same HCI cluster.
		Proposed solution must support automated cluster deployment, configuration and non-disruptive updates and migration
	Form factor	Proposed Appliance/Technology should be rack mountable and all accessories needed should be provided from OEM/bidder. Proposed solution should be based on rack servers not blade/chassis architecture
	OS / Virtualization Cloud	The Hypervisors are to be preinstalled in the nodes along with Virtualization Management. The management node (if not virtual) requirements, if any should be included by default.
	Warranty	24 X 7, NBD onsite for five years fulfilled directly by OEM of appliance. Single number support for all components of appliance (compute, hypervisor, software defined storage)
	Orchestration	HCI Appliance should have built in automation for installation and operations & hardware lifecycle management
	~~Security features~~	~~The Solution should have out of the box security compliance methodology in HCI Solution to ensure highly secure environment it should have industry standard certifications NIST and FIPS140-2.~~ ~~The HCI Appliance/Technology should Support Security Features~~ ~~1. Proposed solution must provide VM-VM isolation to protect against cyber attack and in the event of attack, it should be possible to quarantine the VM to prevent other VMs.~~ ~~2. Should protect against hardware firmware attacks which executes before OS Boot~~ ~~3. Hardware should support hardware root of trust~~ ~~4. The solution should have the ability to provide native application isolation and on-demand creation of security groups based on existing security policies.~~
	Top of rack networking	Solution Should have no dependency proprietary interconnect i.e. should have Capability to Connect 3rd Party network switch well and proposed HCI solution should not have any dependency on underlying networking switches
	HCI licenses	HCI Should be proposed with preconfigured with Enterprise class features such as Vmotion/Live migration, HA, DRS/ADS, Encryption using Industry leading virtualization OEM solutions

Server Rack - 2 nos.		
Sr.No.	Component	Description

2	Server Rack with KVM Switch	Server Racks (42U) with TWO additional power strip, Trays (2), and Exhaust Fan, 16 Port KVM Switch, 16-Port VGA Switch Kit. 1U Rack Mount Supports, Console Monitor (19" or Higher) with Keyboard and Mouse for All Servers with 5 Years Warranty. Proposed hardware should be compatible with each other. Bidder need to propose adequate power sockets and power strips as per requirement. Bidder will have to quote servers and standard Networks Racks (42U) to meet the requirement.

Network Rack (42U) - 2 nos.		
Sr.No.	Component	Description
3	Network Rack	Network Racks (42U) with TWO additional power strip and Exhaust Fan with 5 Years Warranty.Proposed hardware should be compatible with each other.Bidder need to propose adequate power sockets and power strips as per requirement. Bidder will have to quote servers and standard Networks Racks (42U) to meet the requirement.

Network Rack (12U) - 38 nos.		
Sr.No.	Component	Description
4	Network Rack	Wall mounted Network Racks (12U) with TWO additional power strip and Exhaust Fan with 5 Years Warranty. Proposed hardware should be compatible with each other. Bidder need to propose adequate power sockets and power strips as per requirement. Bidder will have to quote servers and standard Networks Racks (12U) to meet the requirement.

Network Switch (48-port 10G L3 fully managed) - 2 nos.		
Sr.No.	Component	Description
5	Hardware features	48x 10/25GbE SFP28, 6 x QSFP28 Datacenter class advance Layer-3, standard rack mountable switch.
		Proposed network device must be 19'' rack mountable
		Network Infrastructure equipment must use 240V AC power.
		The switch should support Dual hot swappable Power supply and Fan supporting to control the switch temperature.
		The switch should support minimum 8 Gbps Flash
		The switch should support minimum 4 Gbps DRAM/Processing memory
		The switch should support minimum 12 Mbps Buffer memory
		The switch should support minimum 2 switches in stack or equivalent feature offering Active - Active control plane switch configuration.
		48x 10/25GbE SFP28, 6 x QSFP28 Datacenter class advance Layer-3 Open Network, standard rack mountable switch.
		The switch should support minimum 3.6Tbps of Switching Performance with 1200Mpps of Forwarding rate less than five microsecond latency.
	Layer 2 and Layer 3 Features	All Optic and modules offered should be hot swappable and fully populated.
		Must support port channeling or equivalent across multiple switches using the IEEE standard LAG features.
		Software based standards for Network Device
		Must support IEEE 802.1d – Spanning-Tree Protocol,
		IEEE 802.1w – Rapid Spanning Tree,

		IEEE 802.1s – Multiple Spanning Tree Protocol,
		IEEE 802.1q – VLAN encapsulation,
		IEEE 802.3ad – Link Aggregation Control Protocol (LACP),
		IEEE 802.1ab – Link Layer Discovery Protocol (LLDP),
		IEEE 802.3x Flow Control
		Routing protocol support; Static IP routing, OSPF, BGPv4, BGP Route , appropriate L2/L3 advance Licenses to be included from day one
		Should support Bidirectional Forwarding Detection (BFD) for OSPF/IS-IS appropriate L2/L3 advance Licenses to be included from day one
		The switch should support Ipv4 and Ipv6 features and function in hardware with minimum Layer-3 routing capacity of 32K table for Ipv4 and 8K table for Ipv6 in hardware. Any license or hardware required to enable all feature to be incorporated in the offer.
		The network infrastructure must allow for multiple equal metric/cost routes to be utilized at the same time
		The switch should support minimum 98K MAC address and 4K Vlan ID and 802.1Q vlans
		Switch must have the ability to offer complete hitless software upgrades with zero interruption to services or data forwarding. Functionality offering the same to be offered to address Switch firmware upgrades major/minor OS releases and patch upgrades.
		Should support 802.1, Layer-2 Vlans, Layer-3 Vlans, Private Vlan, Protocol etc
		IEEE 802.3ad Link Aggregation or equivalent capabilities
		The switch hardware shall be designed to run both Ipv4 & Ipv6 simultaneously (Dual Stack).
		IP Version 6 (Ipv6) must be supported in hardware
		Must support Static Ipv6 routing, OSPFv3/Ipv6 IS-IS
		Should support ECMP for all routing protocols
		Should support Ipv4 and Ipv6 routing
		Supported Ipv6 features should include: DHCPv6/ICMPv6/Ipv6 Multicast support/ Ipv6 PIM Sparse Mode
		Device must support multicast in hardware supporting feature SSM/DM, MLD
	Security features	Must support multiple privilege levels for remote access (e.g. console or telnet access)
		Must support Remote Authentication Dial-In User Service (RADIUS) and/or Terminal Access Controller Access Control System Plus (TACACS+)
		The switch should support ACL Standard, Extended ACL OR Time-based ACL.
		The ACL should be configurable using combination of IP protocol number, Source and Destination address, Source and destination TCP/UDP port number
		The ACL should be able to configure and Manage Access control, Define Filters and re-sequence data flow, Traffic management, Route Distribution, Qos, Cos, Policy Maps, Policy based routing
	QoS features	Must support IEEE 802.1p class-of-service (CoS) prioritization, with 8 queues per port.
		Must support rate limiting (to configurable levels) based on source/destination IP/MAC, L4 TCP/UDP
		Must have the ability to complete traffic shaping to configurable levels based on source/destination IP/MAC and Layer 4 (TCP/UDP) protocols
		There should not be any impact to performance or data forwarding when QoS features
		Must support a “Priority” queuing mechanism to guarantee delivery of highest priority (broadcast critical/delay-sensitive traffic) packets ahead of all other traffic

		Should support Network monitoring features like NetFlow/sFlow, SPAN, RSPAN / GRE SPAN , Streaming Telemetry or similar technologies
	High Availability Features	The switch should support STP/RSTP/MSTP/PVST+, VRRP/HSRP, clustering two switches using OEM or standard based technology.
	Management features	Must support SNMP V1,V2, V3
		Must support SNMP traps (alarms/alerts) and send it to destinations
		Network switch should support Remote Monitoring on every port covering the following four groups (Statistics, Alarm, Event, History).
		Must support Network Timing Protocol and support SDN using Open flow or REST API or similar technologies
		The switch should support dedicated Out of band management port – 10/100/1000baseT, USB port to support additional flash drive expansion, copy/backup/restore switch firmware and configuration, and serial console port via an RJ45 and or USB-B port or serial interface.
	Warranty	5 year 24x7 NBD onsite OEM support.
	Product Support	The system should not be declared as end of life / end of service/support by the OEM for at least next 1Year

Network Switch (48-port 1G L3 fully managed) – 4 nos.		
Sr.No.	Component	Description
6	Hardware features	48x 1GbE RJ45, 2 x SFP+ with Enterprise class advance Layer-3, stackable, standard rack mountable switch.
		Proposed network device must be 19'' rack mountable
		Network Infrastructure equipment must use 240V AC power.
		The switch should come with Dual hotswappable Power supply and Fan supporting to control the switch temperature.
		The switch should support minimum 512MB Flash or Higher.
		The switch should support minimum 1 Gbps DRAM/Processing memory
		The switch should support minimum 4 Mbps Buffer memory
		The switch should support minimum 212GBPS of Switching Performance with 158Mpps of Forwarding rate
		The switch should support minimum 4 Stacking/MLAG of switches using Stacking or MLAG Ports.
		Must support port channelling or equivalent across multiple switches using the IEEE standard LAG features.
		Software based standards for Network Device
		Must support IEEE 802.1d – Spanning-Tree Protocol,
		IEEE 802.1w – Rapid Spanning Tree,
		IEEE 802.1s – Multiple Spanning Tree Protocol,
		IEEE 802.1q – VLAN encapsulation,
		IEEE 802.3ad – Link Aggregation Control Protocol (LACP),
		IEEE 802.1ab – Link Layer Discovery Protocol (LLDP),
		IEEE 802.3x Flow Control
		Must support auto-sensing and auto-negotiation (Link Speed/Duplex)
		Routing protocol support; Static IP routing, OSPF, BGPv4, BGP Route , appropriate L2/L3 advance Licenses to be included from day one
		Should support Bidirectional Forwarding Detection (BFD) for OSPF/IS-IS appropriate L2/L3 advance Licenses to be included from day one
		The switch should support minimum 32K MAC address and 4K Vlan ID and 802.1Q vlans

		Should support 802.1, Layer-2 Vlans, Layer-3 Vlans, Private Vlan, MVRP etc
		IEEE 802.3ad Link Aggregation or equivalent capabilities
		The switch hardware shall be designed to run both Ipv4 & Ipv6 simultaneously (Dual Stack).
		IP Version 6 (Ipv6) must be supported in hardware
		Must support Static Ipv6 routing, OSPFv3 / Ipv6 IS-IS
		Should support ECMP for all routing protocols
		Should support Ipv4 and Ipv6 routing
		Supported Ipv6 features should include: DHCPv6/ICMPv6/Ipv6 Multicast support/ Ipv6 PIMv2 Sparse Mode
		Device must support multicast in hardware supporting feature SSM/DM, MLD
	Security features	Must support multiple privilege levels for remote access (e.g. console or telnet or SSH access)
		Must support Remote Authentication Dial-In User Service (RADIUS) and/or Terminal Access Controller Access Control System Plus (TACACS+)
		The switch should support ACL Standard, Extended ACL OR Time-based ACL.
		The ACL should be configurable using combination of IP protocol number, Source and Destination address, Source and destination TCP/UDP port number
		The ACL should be able to configure and Manage Access control, Define Filters and re-sequence data flow, Traffic management, Route Distribution, Qos, Cos, Policy Maps, Policy based routing
		The ACL should be able to configure and Manage Access control, Define Filters and re-sequence data flow and patterns, Traffic management, Route Distribution, Qos, Cos, Policy Maps, Policy based routing, Logging and flow-based monitoring for Ipv4 and Ipv6 packets.
	QoS features	Must support IEEE 802.1p class-of-service (CoS) prioritization, with 8 queues per port.
		Must have the ability to complete traffic shaping to configurable levels based on source/destination IP/MAC and Layer 4 (TCP/UDP) protocols
		There should not be any impact to performance or data forwarding when QoS features
		Must support a “Priority” queuing mechanism to guarantee delivery of highest priority (broadcast critical/delay-sensitive traffic) packets ahead of all other traffic
		Should support Network monitoring features like NetFlow/sFlow, SPAN, RSPAN / GRE SPAN , Streaming Telemetry/sflor/REST or similar technologies
	High Availability Features	The switch should support STP/RSTP/MSTP/PVST+, VRRP/HSRP, clustering multiple switches using OEM or standard based technology.
	Management features	Must support SNMP V1,V2, V3
		Must support SNMP traps (alarms/alerts) for a minimum of four destinations
		Network switch should support Remote Monitoring on every port covering the following four groups (Statistics, Alarm, Event, History).
		Must support Network Timing Protocol and support SDN using Open flow or REST API or similar technologies
		The switch should support dedicated Out of band management port – 10/100/1000baseT, USB port to support additional flash drive expansion, copy/backup/restore switch firmware and configuration, and serial console port via an RJ45 and or USB-B port or serial interface.
	Warranty	5 year 24x7 NBD onsite OEM support.
	Product Support	The system should not be declared as end of life / end of service/support by the OEM for at least next 1Year

Network Switch (24-port 1G L2 managed) – 48 nos.		
Sr.No.	Component	Description
7	Hardware features	24x 1GbE RJ45, 2 x SFP+ with Enterprise class Image, stackable/MLAG, standard rack mountable switch
		Proposed network device must be 19'' rack mountable
		Network Infrastructure equipment must use 240V AC power.
		Switch should support External Redundant Power supply and Fan supporting to control the switch temperature.
		Switch should support minimum 256 Mb Flash or higher
		The switch should support minimum 1 Gbps DRAM/Processing memory or More
		The switch should support minimum 1 MB Buffer memory or more.
		The switch should support minimum 128 Gbps or higher of Switching Performance with 95 Mpps or higher of Forwarding rate
		The switch should support Minimum 2 Stacking/MLAG ports of switches using dedicated/Open 10G SFP+ ports
	Layer 2 and Layer 3 Features	All Optic and modules offered should be hot swappable and fully populated.
		Must support port channeling or equivalent across multiple switches using the IEEE standard LAG features.
		Software based standards for Network Device
		Must support IEEE 802.1d – Spanning-Tree Protocol,
		IEEE 802.1w – Rapid Spanning Tree,
		IEEE 802.1s – Multiple Spanning Tree Protocol,
		IEEE 802.1q – VLAN encapsulation,
		IEEE 802.3ad – Link Aggregation Control Protocol (LACP),
		IEEE 802.1ab – Link Layer Discovery Protocol (LLDP),
		IEEE 802.3x Flow Control
		Must support auto-sensing and auto-negotiation (Link Speed/Duplex)
		Routing protocol support; Static IP routing, Intervlan Routing. Appropriate L2/L3 advance Licenses to be included from day one
		The switch should support minimum 16K MAC address or higher and 4K Vlan ID and 1000 Active VLAN
		Should support 802.1, Layer-2 Vlans, Private Vlan, MVRP etc
		IEEE 802.3ad Link Aggregation or equivalent capabilities
		IP Version 6 (Ipv6) must be supported in hardware
		Device must support multicast in hardware supporting feature IGMP V2/V3.
	Security features	Must support multiple privilege levels for remote access (e.g. console or telnet or SSH access)
		Must support Remote Authentication Dial-In User Service (RADIUS) and/or Terminal Access Controller Access Control System Plus (TACACS+)
		The switch should support ACL Standard, Extended ACL OR Time-based ACL.
		The ACL should be configurable using combination of IP protocol number, Source and Destination address, Source and destination TCP/UDP port number
		The ACL should be able to configure and Manage Access control, Define Filters and re-sequence data flow and patterns, Qos, Cos.
	QoS features	Must support IEEE 802.1p class-of-service (CoS) prioritization, with 8 queues per port.
		Must support rate limiting (to configurable levels) based on source/destination IP/MAC, L2 TCP/UDP
		There should not be any impact to performance or data forwarding when QoS features
		Must support a "Priority" queuing mechanism to guarantee delivery of highest priority (broadcast critical/delay-sensitive traffic) packets ahead of all other traffic

		Should support Network monitoring features like NetFlow/sFlow, SPAN, RSPAN / GRE SPAN or similar technologies
	Management features	Must support SNMP V1,V2, V3
		Must support SNMP traps (alarms/alerts) for a minimum of four destinations
		Network switch should support Remote Monitoring on every port covering the following four groups (Statistics, Alarm, Event, History).
		Must support Network Timing Protocol and support SDN using Open flow or REST API or similar technologies
	Warranty	5 year 24x7 NBD onsite OEM support.
	Product Support	The system should not be declared as end of life / end of service/support by the OEM for at least next 1Year

Firewall - 2 No.	
Sr.No.	**Description**
	Hardware Specification
1	Firewall appliance atleast have 4x 10GE SFP+, 4x GE SFP, 12x GE RJ45 interfaces from day one. All these interfaces should be available simultaneously.
2	Firewall Throughput should be at least 78 Gbps.
3	Threat Prevention (including FW, IPS, Application Control & Antivirus) throughput must be at least 8 Gbps with real-world / enterprise MIX traffic
4	NGFW (including FW, IPS, Application Control) throughput must be at least 9 Gbps with real-world / enterprise MIX traffic
5	NGFW should have IPsec VPN throughput of at least 50 Gbps
6	The proposed firewall must support at least 8 Gbps of SSL Inspection throughput along with IPS feature enabled.
7	NGFW should support 2000 site-to-site VPN Tunnels.
8	NGFW should support more than 500000 new sessions per second
9	NGFW should support atleast 7.7 Million concurrent sessions
10	NGFW should not introduce more than 5 microsecond latency. Vendor's claim must be available in publicly availabe documents like datasheet, admin guide etc.
	Security Features
11	The Firewall should be Hardware based, Reliable, purpose-built security appliance with hardened operating system supporting State full policy inspection technology.
12	The NGFW solution should support NAT64, NAT46, DNSv6 & DHCPv6
13	The proposed system should be able to operate in Transparent (Access) mode and NAT/Route mode simultaneously without creating virutal context or virtual firewall
14	The physical interface should be capable of link aggregation as per IEEE 802.3ad standard, allowing the grouping of interfaces into a larger bandwidth 'trunk'. It should also allow for high availability (HA) by automatically redirecting traffic from a failed link in a trunk to the remaining links in that trunk.
15	The NGFW should support WAN links load balancing and fail-over for at least 2 links.
16	The NGFW should support internet links load balancing and fail-over based parameters such as Latency, Jitter, Packet-Loss,
17	The proposed system should have integrated Traffic Shaping functionality for both inbound and outbound traffic.
18	The NGFW should have both SSL and SSH Inspection capabilities
19	The system should support 2 forms of site-to-site VPN configurations:
	a) Route based IPsec tunnel
	b) Policy based IPsec tunnel
20	The system should support IPSEC site-to-site VPN and remote user IPSec VPN in transparent mode.
21	The system should provide IPv6 IPsec feature to support for secure IPv6 traffic in an IPsec VPN.

22	Proposed NGFW must not require reboot to push security policies or any signature (IPS, Anti-malware etc.) update.
23	The NGFW shall be able to support various form of user Authentication methods simultaneously, including: Local Database, LDAP, RADIUS, TACACS+, Windows AD, Citrix & Terminal Server Agent support for Single Sign On
24	The NGFW should readily available integration with SDN platforms like - Kubernetes, Vmware ESXi and NSX, OpenStack, Cisco ACI, Nuage Networks and Nutanix
Intrusion Prevention System	
25	IPS throughput should be at leat 12 Gbps or better for Enterprise MIX traffic
26	The IPS should be able to inspect SSL sessions by decrypting the traffic
27	The IPS system should have at least 10K+ signatures
28	In event if IPS should cease to function, it should fail open by default and be configurable so that crucial network traffic should not be blocked and NGFW should continue to operate while the IPS problem is being resolved.
29	IPS solution should have capability to protect against Denial of Service (DOS) and DDOS attacks. Should have flexibility to configure threshold values for each of the Anomaly. DOS and DDOS protection should be applied and attacks stopped before firewall policy look-ups.
30	Signatures should have severity level defined to it so that the administrator can understand and decide which signatures to enable for what traffic (e.g. for severity level: high medium low)
31	NGFW should have capabilities to limit number of parameters in URL, number of cookies in request, number of headers lines in request, total URL and Body parameters in length to block advanced HTTP layer attacks.
	Application Control Features:
32	The appliance should have at least 4000 application signatures database
33	The proposed Firewall must have 25 Gbps of Application Control Throughput.
Anti-Malware & Advanced Persistent Threat	
34	Should be able to block, allow or monitor only using AV signatures and file blocking based on per firewall policy based or based on firewall authenticated user groups with configurable selection of the following services and their equivalent encrypted versions, wherever applicable: HTTP, SMTP, POP3, IMAP, FTP, CIFS, NNTP, SSH, MAPI.
35	NGFW must include Anti-bot capability using IP reputation DB, terminates botnet communication to C&C servers also. Vendor needs to add additional license if it is required.
36	NGFW should have functionality of Content Disarm and Reconstruction (CDR) to remove all active content from attachment in real-time before passing it to user.
37	NGFW should have cloud sandbox functionality to protect organization from Adance Persistence Threats. In case any additional license is required, bidder has to include it in proposal from day one.
38	The proposed solution should utilize a state-full attack analysis to detect the entire infection lifecycle, and trace the stage-by-stage analysis of an advanced attack, from system exploitation to outbound malware communication protocols leading to data exfiltration.
39	NGFW should be able to monitor encrypted traffic to detect APTs hidden in SSL traffic.
40	Buyer should be able to view file-analysis status details including file submission time, source IP, destination IP, File name, URL, File size, File type, Suspicious Act etc.
Web & DNS Security Functionalities	
41	The NGFW must have in-built Web Filtering Functionality.
42	The NGFW shall allow administrators to override Web Filtering database ratings with local settings.
43	The NGFW should be capable to identify and prevent in-progress phishing attacks by controlling sites to which users can submit corporate credentials based on the site's URL category thus blocking users from submitting credentials to untrusted sites while allowing users to continue to submit credentials to corporate and sanctioned sites.
44	NGFW should have 40000+ botnet definitions in its database and should be updated on regular basis to protect from new definitions

45	The NGFW must have advanced URL filtering categories to block access to Newly Registered Domains, Newly Observed Domains, Dynamic DNS based websites.
46	The NGFW must have option to rate web resource based on their DNS rating.
47	The proposed solution shall support DNS-based signatures to detect specific DNS lookups for hostnames that have been associated with malware.
48	The NGFW must block Botnet C&C domains request at DNS level itself.
49	The NGFW must have DNS Sinkhole functionality from day one to block and redirect malicious request to custom defined web portal.
Data Leakage Prevention	
50	NGFW should have in-built DLP functionality without requiring any additional hardware or software license
51	NGFW should allow administrator to prevent sensitive data from leaving the network. Administrator should be able to define sensitive data patterns, and data matching these patterns that should be blocked and/or logged when passing through the unit.
52	NGFW must detect, protect and log sensitive data travelling through protocols - HTTP, FTP, SMTP, IMAP, POP3, NNTP, MAPI, CIFS, SFTP, SCP
53	DLP feature must offer watermarking functionality which allows organizers to apply document marking for DLP.
54	DLP actions should be : Log only, block, quarantine user/IP/Interface.
55	It should have DLP fingerprinting feature which generates a checksum fingerprint from intercepted files and compare it to those in the fingerprint database.
SSL VPN	
56	The Firewall should be integrated solution and there should be no user based licensing for SSL VPN
57	SSL VPN must have atleast throughput of 3.5 Gbps or higher
58	Solution must support at least 5000 concurrent SSL VPN.
59	The Firewall should support for TWO modes of SSL VPN:1.Web mode,2.Tunnel mode
IPSEC VPN Requirements:	
60	The proposed system shall support industry standards ofIPSEC, and SSL VPN without additional cost for license or solution for VPN client
61	Firewall must have atleast 10000 IPSec VPN client in Route mode from the day 1
62	IPSEC (DES, 3DES, AES) encryption/decryption and SSL encryption/decryption
63	The system shall support IPSEC site-to-site VPN and remote user VPN in transparent mode without any additional cost for VPN clients
High Availability	
64	The proposed NGFW shall have built-in high availability (HA) features without extra cost/license or hardware component
65	The NGFW shall support stateful session maintenance in the event of a fail-over to a standby unit.
66	High Availability feature must be supported for either NAT/Route, Transparent or Hybrid mode
67	The NGFW must support both Active-Passive and Active-Active High Availability options.
68	The NGFW must provide Load sharing mode along with redundancy
69	The NGFW shall support interface link monitoring failover
70	The NGFW shall support external device ping probe failover
71	The HA solutions should support silient firmware upgrade process that ensures minimum downtime
72	The NGFW must have provision of fail-over in case of high memory utilisation on primary appliance.
73	The NGFW must have capability to perform security inspection in networks where forward traffic and return traffic follow different paths.
Logging & Reporting	
74	Solution should offer in-house centralized reporting to store logs with 1year retention.
75	Solution should offer Centralized NOC/SOC Visibility for the Attack Surface.
76	Solution should offer Real-time notifications, reports, predefined or customized dashboards deliver single-pane visibility and actionable results.

Installation, Configuration & Warranty	
77	The bidder should install & Configure the NGFW as per requirement of department. Onsite support will be provided by Bidder along with Remote (24*7) remote support from OEM.
78	The device should be delivered with 5 Years OEM warranty & 24*7 support along with NBD for RMA.

NMS Software - 150 nos.		
Sr.No.	Component	Description
9	Deep Discovery, Inventory, CMDB	NMS should have the capability to discover chassis, PIC/card, ports. It should also have the capability to discover logical interfaces.
	Fault Management and Notification.	NMS should have the capability to monitor for health-affecting conditions of multi-vendor platforms. Notification mechanisms such as an Alarm Viewer, email, SMS and API should be supported.
	Configuration File Management	NMS should back-up configuration of devices on an automated, scheduled or ad hoc basis.
	Change and Compliance Management	NMS should have the capability to detect and report on changes. NMS should ensure only permitted operators are allowed to apply changes.
	Automated Network Topology	NMS should have the capability to automatically build the physical and logical topology.
	Firmware/OS Management & Deployment	NMS should download and maintain various versions of firmware for all your devices.
	Customer Self-Care (multi-tenancy)	NMS should support multi-tenancy. It should be capable of providing role-based access to users in an multi-tenant environment.
	User Security Management	NMS should manage user/user group security settings and their functional permissions within the application.
	Comprehensive Solution Auditing & Logging	NMS should retains all transactions with devices. It should let the users easily revisit these transactions making troubleshooting easier.
	Multi-Technology/Vendor Support	NMS should support devices from multiple vendors like DellEMC, Cisco, Ruckus, Aerohive, Brocade, Juniper, Netgear, Extreme, Foundry, HPE, F5, Sonicwall, Sonus, Aperi, Avaya, Ericsson, Siemens, Enterasys, Nortel, Alcatel, 3Com and many more. NMS should support single pane-of-glass management of your hybrid cloud and network infrastructure including servers, Routers, Switches, Security Devices, Storage, Appliances/
	3rd-Party Integration	NMS should integrate seamlessly with other systems using various methods like web services, SNMP traps, email notifications, and scripts.
	Network Operations Collaboration	NMS should build network operational communities across management systems silos so work groups can share information instantly, solve problems quickly, and deliver services faster.
	Real-time network monitoring	Real-time Interface Traffic, Real-time Server Performance
	Physical and virtual server monitoring	Monitor CPU, memory, and disk utilization of Windows and Linux servers. Also monitor the performance of Hosts and VMs of VMware, Hyper-V, Xen and Nutanix server virtualization platforms.
	Multi-level thresholds	Proactively monitor network performance with multi-level thresholds. For every critical performance monitor, set multiple thresholds and get instant alerts for violation.
	Customizable dashboards	Assess default dashboards or create your own dashboards by making use of over 200 performance widgets available and view performance of your network at-a-glance.

	Network Devices & WAN Link monitoring	Monitor key metrics such as latency, jitter, RTT, and packet loss to eliminate network issues. View hop-by-hop performance to find what's causing latency and fix it quickly

Uptime: It is required to maintain uptime of 99.741%. Further, bidder is responsible for providing comprehensive warranty and support (24x7x365) for the period of five years from the date of successful completion FAT**.**

MIS Reports:

#	Types of Reports	Periodicity
1	• System performance report, which includes CPU, memory, Cache, disks, etc. • All type of event reports • SLA Compliance report • Reports as directed by the State for SLA calculation • Summary of system reboot • Summary of issues / complaints logged with the OEMs. • Patch update status as notified by the OEM	Weekly, Monthly, Quarterly
2	• Log of preventive / scheduled maintenance undertaken • Details of Patch, updates, Vulnerability fixes released and implementation status of same • Details of break-fix maintenance undertaken	Monthly, Quarterly

SERVICE LEVEL AGREEMENT:

#	Target	Penalty
1	Priority Level 1 Incident - Within 1 hr. Priority Level 2 Incident - Within 6 hr. Priority Level 3 Incident - Within 12 hr.	• Level 1 Incident 0.25% of QP for every 2-hr. delay in resolution; • Level 2 Incident 0.25% of QP for every 3-hr. delay in resolution; • Level 3 Incident 0.25% of QP for every 6 hrs. delay in resolution

- Priority Level 1: Complete System failure or not in working condition or not accessible.
- Priority Level 2: Solution is not functioning properly due to failure of any hardware/software/part(s)/ component(s) or performance of the solution is down (in terms of latency and response time)
- Priority Level 3: Any other issues except Priority 1 & 2 above

IMPLEMENTATION TIMELINES & PENALTIES:

S/N	Measurement	Target	Penalty for Delay
Applicable for overall contract			
1	Kick-off meeting	1 week from issuance of LoI/WO	Rs 50,000/week or part thereof. Delay Beyond 4 weeks, DST/GIL may terminate the contract and Forfeit the PBG.
Applicable for each storage separately			
2	Delivery of Components (Hardware, Software, License, etc.)	T1 = T + 12 weeks	A penalty of 0.5% of **Contract Value** per week or part thereof. Delay beyond T + 14 weeks GVK/GIL may terminate the contract and Forfeit the PBG
3	Installation and Commissioning	T2 = T1 + 4 weeks	A penalty of 0.5% of **Contract Value** per week or part thereof. Delay beyond T1 + 6 weeks DST/GIL may terminate the contract and Forfeit the PBG
4	Final Acceptance Test (FAT)	T3 = T2 + 2 weeks	A penalty of 0.5% of **Contract Value** per week or part thereof.
5	Training	T4 = T3 + 2 weeks	A penalty of 0.5% of **Contract Value** per week or part thereof.

FINAL ACCEPTANCE TEST: To be carried out based on followings but not limited to:

- Verification of installation and commissioning (Hardware, software and licenses)
- OEM Certifications
- All Functional and Technical requirements

MILESTONE BASED PAYMENT TERMS:

S/N	Activity	Payment (%)
Table 1: Schedule-I		
1	Delivery of all components (Hardware, Software, Licenses, etc.)	70% of the sum total of schedule I of financial bid
2	Successful installation, Testing, Integration, Commissioning	10% of the sum total of schedule I of financial bid
3	Successful completion of training & Final Acceptance test of entire solution	20% of the sum total of schedule I of financial bid
Table 2:		
1	5 Years AMC/warranty and Back to Back OEM support for the entire Infrastructure (hardware & Software)	Will be divided and paid in 20 equated Quarters. Five years will start from the date of successfully completion of FAT.

PRICE BID SCHEDULE:

Sr. #	Device Description	Unit	Item Quantity	Unit Rate Inc. GST	Total Rate
1	Hyper Converged Infrastructure	Lot	1		
2	Network Switch (48-port 10G L3 fully managed)	Nos	2		
3	Network Switch (48-port 1G L3 fully managed)	Nos	4		
4	Network Switch (24-port 1G L2 managed)	Nos	48		
5	Firewall	Nos	2		
6	Server Rack	Nos	2		
7	Network Rack (42U)	Nos	2		
8	Network Rack (12U)	Nos	38		
9	NMS Software 150 Nos	Lot	1		

10	Cost for 5 year CAMC & Warranty Support	Nos	1		

Note:

1. L1 will be the lowest sum total of rates of all line items including GST as per GeM GTC
2. Sum Total of CAMC & Warranty would be paid in 20 equated Quarters from the date of successfully completion of FAT.
3. RA has been enabled in the GEM Bid.

ADDITIONAL DOCUMENT TO BE SUBMITTED:

In the technical bid section of GeM, the bidder is required to upload following documents;

1. Brochure and OEM Compliance of the Offered product on OEM letterhead.
2. BoQ with part-code on OEM letterhead for software and/or hardware components required to complete the solution.
3. Compliance of the SoW, SLA and Payment terms etc as uploaded as part of the GeM Bid on bidder's letterhead.
4. Undertaking as per guidelines published by Ministry of Finance, Dept. of Expenditure, Public Procurement division dated 23.07.2020 in the given format by Bidder as well as OEM.
5. RA has been enabled in the GEM Bid.
6. Sum Total of AMC & Warranty would be paid in 20 equated Quarters from the date of successfully completion of FAT.
7. After completion of 5 years warranty/CAMC period, if required, GVK may extend the warranty/AMC support for further period of 2 years (6th year and 7th year) on the derived rates of average cost of 5 years warranty/CAMC cost quoted for Hardware and Software. Bidder is required to provide the undertaking for the same mentioning that they will provide 6th year and 7th year warranty/ CAMC support.

On letterhead of Bidder

Sub : Undertaking as per Office Memorandum No.: F. No.6/18/2019-PPD dated 23.07.2020 published by Ministry of Finance, Dept. of Expenditure, Public Procurement division

Ref: Bid Number: _____

I have read the clause regarding restriction on procurement from a bidder of a country which shares a land border with India. I certify that we as a bidder and quoted product from following OEMs are not from such a country or, if from such a country, these quoted products OEM has been registered with competent authority. I hereby certify that these quoted product & its OEM fulfills all requirements in this regard and is eligible to be considered for procurement for Bid number_____.

No.	Item Category	Quoted Make & Model

In case I'm supplying material from a country which shares a land border with India, I will provide evidence for valid registration by the competent authority, otherwise GIL/End user Dept. reserves the right to take legal action on us.

(Signature)

Authorized Signatory of **M/s <<Name of Company>>**

On letterhead of OEM

Sub : Undertaking as per Office Memorandum No.: F. No.6/18/2019-PPD dated 23.07.2020 published by Ministry of Finance, Dept. of Expenditure, Public Procurement division

Ref: Bid Number: _____

Dear Sir,

I have read the clause regarding restriction on procurement from a bidder of a country which shares a land border with India. I certify that our quoted product and our company are not from such a country, or if from such a country, our quoted product and our company have been registered with competent authority. I hereby certify that these quoted product and our company fulfills all requirements in this regard and is eligible to be considered for procurement for Bid number_____.

No.	Item Category	Quoted Make & Model

In case I'm supplying material from a country which shares a land border with India, I will provide evidence for valid registration by the competent authority; otherwise GIL/End user Dept. reserves the right to take legal action on us.

(Signature)

Authorized Signatory of **M/s <<Name of Company>>**

Answer to Pre-Bid Queries

Combined Bidder's Request For Clarification for Purchase of HCI for GVK EMRI for Dial 112 Project. (Bid Number: GEM/2022/B/2659623 Dated: 02-11-2022)						
S.No.	**Bidding Document Reference (Clause /page)**		**Content of RFP requiring clarification**	**Points of Clarification required**	**Remarks of Organization submitting Request**	**GIL / GVK Remarks**
1	Minimum Specification NMS Software - 150 nos. pg no14		Additional clause for NMS software	In order to select NMS solution from Make In India company (as per Govt. of India guidelines) along with long term existence and offering proven solution in industry, we would request you to add following clause in the NMS specification. "The proposed NMS solution OEM should be Make in India and must have atleast 3 deployments (in state/central Government/ PSU) in India with 1000 devices being monitored in each of these deployments in last five years. Reference PO copy and completion/ sign-off document need to be submitted at the time of submission."		No Change, As per RFP. Make In India product is Allowed.
2	Minimum Specification NMS Software - 150 nos. pg no14		Additional clause for NMS software	In order to select established NMS OEM with strong financial background in the industry, we request the authority to incorporate the below clause: "NMS OEM must have average annual turnover of atleast INR 20 Cr. or above in last 3 financial years Excluding the current financial year with positive net worth. CA certificate need to be submitted at time of bid submission."		No Change, As per RFP
3	Minimum Specification NMS Software - 150 nos. pg no14		Additional clause for NMS software	In order to provide complete visibility of IT infrastructure including servers with micro level monitoring (on need basis) through which granular level details can be captured along with flexibility of monitoring through agent and agentless approach. Hence, we request the authority to add the following clause in the NMS specification: "The proposed NMS solution must provide agentless as well as agent based monitoring for server infrastructure. The agents should be able to set polling interval as low as 1 second with low overhead on target server infrastructure."		No Change, As per RFP
4	Additional Eligibility Evaluation Criteria: Page No 1 of 19		Relevant Work order copy / client satisfactory letter regarding successful implementation on-premise cloud solution in the name of the bidder is to be submitted. The PO/Workorder/contracts / letter should be in the name of the bidder and clearly mention the scope of work.	**Modification :** Relevant Work order copy / client satisfactory letter regarding successful implementation on-premise cloud solution in the name of the bidder**/OEM** is to be submitted. The PO/Workorder/contracts / letter should be in the name of the bidder and clearly mention the scope of work. **Justification:-** Request you to please consider bidder/OEM in eligibility criteria, amending this clause will help in wider participation from bidders/OEM.		Please See Corrigendum

5	Minimum Specification: Hyper Converged Appliance. Page 3		Solution should also have capability to use Software Defined Networking, must propose the Logical FW Solution from day-1 considering the GVK Security.	**Modification** : Request you to please deleate this clause or please elaborate on GVK Security so all OEMs can offer a standard solution. Any OEM cant guarantee compatibility, unless the application is certifed by developer on compatible OS, VM environment, also Software defined networking is supported but no license's are proposed.		Please See Corrigendum. Requirement of "Logical FW solution from day-1 removed as Physical firewall is being procured." is removed.
6	Minimum Specification: Security Feature. Page 3		The Solution should have out of the box security compliance methodology in HCI Solution to ensure highly secure environment it should have industry standard certifications NIST and FIPS140-2. The HCI Appliance/Technology should Support Security Features 1. Proposed solution must provide VM-VM isolation to protect against cyber attack and in the event of attack, it should be possible to quarantine the VM to prevent other VMs. 2. Should protect against hardware firmware attacks which executes before OS Boot 3. Hardware should support hardware root of trust 4. **The solution should have the ability to provide native application isolation and on-demand creation of security groups based on existing security policies.**	**We reqeust GIL to claify on point 4, as this means the Guest VM isiloation that works in conjuction with VM-VM isolation to protect intra VM attachs or any kind of VM image corruption.**		Please See Corrigendum. Requirement is removed.
7	Minimum Specification: Hyper Converged Appliance. Page 3		Solution should also have capability to use Software Defined Networking, must propose the Logical FW Solution from day-1 considering the GVK Security.	**Additional Clause :** Logical Routing capabilities to avoid traffic Hairpinning **Justification:-** In a traditional scenario, all inter-VLAN traffic initiates from VM (in one VLAN) to TOR – CORE Switch where the routing is checked and the traffic is sent back to TOR and to Destination VM (in another VLAN). Due to this VM to VM traffic moves all the way from Virtual – Physical – Virtual environment which causes utilization to the uplinks and increases utilization on Core Switches everytime. Adding Logical routing capabilities helps achieve Inter-VLAN traffic from VM to VM at the virtual layer itself, as all the routing is done at the virtual layer. This eliminates the utilization on the Uplink links and further utilization on the Core Switches as well. Hence, we request to consider this capability in the current RFP. Any OEM/Bidder who cannot offer this functionality within their solution, can		Please See Corrigendum. Requirement of "Logical FW solution from day-1 removed as Physical firewall is being procured." is removed.

				stitch their solution with 3rd party component.		
8	Firewall			The firewall connectivity port also according to it, creates proprietorship/monopoly of that product		Please see Firewall spec sheet
9	Firewall			The IPS VPN Thruput is unnecessarily higher than the same category of product, which points also creates a monopoly in this bid.		
10	Firewall			A few network/connectivity port are unique supplies of 'SOPHOS' and those are not useful to the client but have an impact on other OEMs.		
11	**Eligibility Criteria : Point No. 4**		The OEM of the proposed product should have a total sum of turnover of Rs. 1000 Crore (Minimum) in the last three financial years as on 31st March 2022.	As per Government PPP guidelines, the buyer has to consider MSE Exemption from the local vendor for bid qualification.		No Change, As per RFP
12	Firewall		Firewall "IPsec VPN throughput" - 17000 Mbps	**Request you to Amend With : 6000 Mbps**		Please see Firewall spec sheet
13	Firewall		Firewall "Flexi Port Modules" - 8 x Port GbE Copper 4 x Port 10 GbE SFP+ Fiber	**Request you to Amend With : 8x 1G Copper and 4*10G SFP+ ports, that will also complete the requirement. (As 10G SFP+ ports can also work as 1G sfp ports)**		Please see Firewall spec sheet
14	Firewall		Firewall "Management Port" - 1 x MICO USB (cable Incl.)	To comply this, we will provide USB to Micro-USB converter		Please see Firewall spec sheet
15	Firewall		Firewall "Other IO Port" - 1 x MICO USB (cable Incl.)	2 x USB 3.0 are enough for connectivity. Kindly remove extra 1 USB ports as it is restricting other suppliers to comply.		Please see Firewall spec sheet
16	Firewall (2 pieces), Technical Specifications Page No. 5			Referring to the bid specification, this tender is made to support British product SOPHOS, MODEL XGS3100 Product, please refer to the attached data sheet of it. You will really feel that the bid specification and criteria is copy pasted from SOPHOS's datasheet. This is the third time the same kind favors to foreign-made products. which is against GFR & Govt's Procurement Guidelines. THESE PROPRIETARY SPECIFICATIONS OF 'SOPHOS XGS 3100' CREATE MONOPOLY CONDITIONS AGAINST OTHER BIDDERS. Please find the attached data sheet for your checking.		Please see Firewall spec sheet
17	**Eligibility Criteria**		HCI solution must have been implemented at Minimum two locations/Projects for Central / State Gov, PSU, BFSI in India during the last five years as on Bid submission date	Relevant Work order copy / client satisfactory letter regarding successful implementation on-premise cloud solution in the name of the **bidder/OEM** is to be submitted. The PO/Workorder/contracts / letter should be in the name of the **bidder/OEM** and clearly mention the scope of work.		Please See Corrigendum.
18	Scope of Work		The Bidder shall configure the proposed solution in such a way that it should comply with all the policies of the GVK.	Requesting you to kindly share the GVK policy.		Details will be shared with Selected Bidder

19	Scope of Work		Bidder is responsible for sizing and procuring the necessary hardware and software licenses as per the performance requirements provided in the bid. During the warranty period bidder, shall replace or augment or procure higher-level new equipment or additional licenses at no additional cost in case the procured hardware or software is not adequate to meet the service levels.	Requesting you to kindly help share performance requirement.		No Change, As per RFP
20	Specification of Hyper Converged Infrastructure & other Hardware	Config	*The cluster should be configured with minimum 5 Node : *280 physical usable cores, 1.5TB ram, 60TB usable storage capacity (W/O Deduplication Compression and Erasure Coadding) across the 5 node cluster. (w/O HCI & Management Overhead, Bidder need to consider the HCI & Management overhead Separately) *Each Node must be populated with minimum 2*1.6TB SSD or more per node for caching and full capacity of the SSD must be available to server caching and capacity requirement, Caching must be redundant in nature and failure of single SSD must not consider as a node failure *Each node should be Configured with 4*10/25Gbps LAN ports.	*The cluster should be configured with minimum 5 **All Flash Node** : *280 physical usable cores, 1.5TB ram, 60TB usable storage capacity (W/O Deduplication Compression and Erasure Coadding) across the 5 node cluster. (w/O HCI & Management Overhead, Bidder need to consider the HCI & Management overhead Separately) *Each Node must be populated with minimum 2*1.6TB SSD or more per node for caching and full capacity of the SSD must be available to server caching and capacity requirement, Caching must be redundant in nature and failure of single SSD must not consider as a node failure *Each node should be Configured with 4*10/25Gbps LAN ports.		Please See Corrigendum.
21	Specification of Hyper Converged Infrastructure & other Hardware	Minimum Specification : Security Feature. Page 3	The Solution should have out of the box security compliance methodology in HCI Solution to ensure highly secure environment it should have industry standard certifications NIST and FIPS140-2. The HCI Appliance/Technology should Support Security Features 1. Proposed solution must provide VM-VM isolation to protect against cyber attack and in the event of attack, it should be possible to quarantine the VM to prevent other VMs. 2. Should protect against hardware firmware attacks which executes before OS Boot 3. Hardware should support hardware root of	**We request GIL to claify on point 4, as this means the Guest VM isiloation that works in conjuction with VM-VM isolation to protect intra VM attachs or any kind of VM image corruption.**		Please See Corrigendum. Requirement is removed.

			trust 4. **The solution should have the ability to provide native application isolation and on-demand creation of security groups based on existing security policies.**			
22	Server Rack with KVM Switch	Config for KVM	Server Racks (42U) with TWO additional power strip, Trays (2), and Exhaust Fan, 16 Port KVM Switch, 16-Port VGA Switch Kit. 1U Rack Mount Supports, Console Monitor (20") with Keyboard and Mouse for All Servers with 5 Years Warranty. Servers with 5 Years Warranty. Proposed hardware should be compatible with each other. Bidder need to propose adequate power sockets and power strips as per requirement. Bidder will have to quote servers and standard Networks Racks (42U) to meet the requiremen	Server Racks (42U) with TWO additional power strip, Trays (2), and Exhaust Fan, 16 Port KVM Switch, 16-Port VGA Switch Kit. 1U Rack Mount Supports, Console Monitor (19") with Keyboard and Mouse for All Servers with 5 Years Warranty. Servers with 5 Years Warranty. Proposed hardware should be compatible with each other. Bidder need to propose adequate power sockets and power strips as per requirement. Bidder will have to quote servers and standard Networks Racks (42U) to meet the requiremen		Please See Corrigendum.
23	Eligibility Criteria : Point No. 4		**Eligibility Criteria : Point No. 4** The bidder should have experience in Supply, Installation, Testing and Commissioning (SITC) of Data Centre IT Infrastructure i.e. Server, Storage, Virtualization, Network and Security. Bidder Should have executed on premises Data Center IT Infrastructure related work order of minimum one work order value of 10 Cr or two order of value 7 Cr in the last three financial years as on bid submission. All work orders / contracts should be in the name of the bidder	**Request you Amend With :** Bidder Should have executed on premises Data Center IT Infrastructure related work order of minimum one work order value of 10 Cr or two order of value 7 Cr in the **last five financial years** as on bid submission.		Please See Corrigendum.
24	Eligibility Criteria : Point No. 6		HCI solution must have been implemented at Minimum two locations/Projects for Central / State Gov, PSU, BFSI in India during the last five years as on Bid submission date.	**Request you Amend With :** HCI solution must have been implemented **by Bidder/OEM** at Minimum two locations/Projects for Central / State Gov, PSU, BFSI in India during the last five years as on Bid submission date.		Please See Corrigendum.
25			Solution should also have capability to use Software Defined Networking, must propose the Logical FW Solution from day-1 considering the GVK Security.	Request to elaborate on GIL Security so all OEMs can offer a standard solution. AS standard OEM cant guarantee compatibility, unless the application is certifed by developer on compatible OS, VM environment. Software defined		Please See Corrigendum. Requirement of "Logical FW solution from day-1 removed as Physical

				networking is supported but no license are proposed.		firewall is being procured." is removed.
26			The Solution should have out of the box security compliance methodology in HCI Solution to ensure highly secure environment it should have industry standard certifications NIST and FIPS140-2. The HCI Appliance/Technology should Support Security Features 1. Proposed solution must provide VM-VM isolation to protect against cyber attack and in the event of attack, it should be possible to quarantine the VM to prevent other VMs. 2. Should protect against hardware firmware attacks which executes before OS Boot 3. Hardware should support hardware root of trust **4. The solution should have the ability to provide native application isolation and on-demand creation of security groups based on existing security policies.**	We reqeust GIL to claify on point 4, as this means the Guest VM isiloation that works in conjuction with VM-VM isolation to protect intra VM attachs or any kind of VM image corruption.		Please See Corrigendum. Requirement is removed.
27			Minimum Specification NMS Software - 150 nos.	**Addtional clause for NMS software :** In order to avoid tempering with SLA calculation, we recommend authority to select solution with in-built database for ensuring better control and flexibility along with lower TCO, we request the authority to incorporate the below clause: "The monitoring module of proposed solution must not use any third party database (including RDBMS and open source) to store data in order to provide full flexibility and control on collected data as well as avoiding tempering with SLA calculations."		No Change, As per RFP
28			Minimum Specification NMS Software - 150 nos.	**Addtional clause for NMS software :** In order to select NMS solution from Make In India company (as per Govt. of India guidelines) along with long term existence and offering proven solution in industry, we would request you to add following clause in the NMS specification. "The proposed NMS solution OEM should be Make in India and must have atleast 3 deployments (in state/central Government/ PSU) in India with 1000 devices being monitored in each of these deployments in last five years. Reference PO copy and completion/		No Change, As per RFP. Make In India product is Allowed.

				sign-off document need to be submitted at the time of submission."		
29			Minimum Specification NMS Software - 150 nos.	**Addtional clause for NMS software :** In order to select established NMS OEM with strong financial background in the industry, we request the authority to incorporate the below clause: "NMS OEM must have average annual turnover of atleast INR 20 Cr. or above in last 3 financial years Excluding the current financial year with positive net worth. CA certificate need to be submitted at time of bid submission."		No Change, As per RFP
30			Minimum Specification NMS Software - 150 nos.	**Addtional clause for NMS software :** In order to provide complete visibility of IT infrastructure including servers with micro level monitoring (on need basis) through which granular level details can be captured along with flexibility of monitoring through agent and agentless approach. Hence, we request the authority to add the following clause in the NMS specification: "The proposed NMS solution must provide agentless as well as agent based monitoring for server infrastructure. The agents should be able to set polling interval as low as 1 second with low overhead on target server infrastructure."		No Change, As per RFP
31			**Eligibility Criteria : Point No. 4** The OEM of the proposed product should have a total sum of turnover of Rs. 1000 Crore (Minimum) in the last three financial years as on 31st March 2022.			No Change, As per RFP
32			Firewall "IPsec VPN throughput" - 17000 Mbps	**Request you to Amend With :** 6000 Mbps		Please see Firewall spec sheet
33			Firewall "Flexi Port Modules" - 8 x Port GbE Copper 8 x Port GbE SFP Fiber 4 x Port 10 GbE SFP+ Fiber	**Request you to Amend With :** 8x 1G Copper and 4*10G SFP+ ports, that will also complete the requirement. (As 10G SFP+ ports can also work as 1G sfp ports)		Please see Firewall spec sheet
34			Firewall "Management Port" - 1 x MICO USB (cable Incl.)	To comply this, we will provide USB to Micro-USB converter		Please see Firewall spec sheet
35			Firewall "Other IO Port" - 1 x MICO USB (cable Incl.)	2 x USB 3.0 are enough for connectivity. Kindly remove extra 1 USB ports as it is restricting other suppliers to comply.		Please see Firewall spec sheet

36	HCI Solution		Solution should also have capability to use Software Defined Networking, must propose the Logical FW Solution from day-1 considering the GVK Security.	Request you also add : Logical Routing capabilities to avoid traffic Hairpinning, In a traditional scenario, all inter-VLAN traffic initiates from VM (in one VLAN) to TOR – CORE Switch where the routing is checked and the traffic is sent back to TOR and to Destination VM (in another VLAN). Due to this VM to VM traffic moves all the way from Virtual – Physical – Virtual environment which causes utilization to the uplinks and increases utilization on Core Switches everytime. Adding Logical routing capabilities helps achieve Inter-VLAN traffic from VM to VM at the virtual layer itself, as all the routing is done at the virtual layer. This eliminates the utilization on the Uplink links and further utilization on the Core Switches as well. Hence, we request to consider this capability in the current RFP. Any OEM/Bidder who cannot offer this functionality within their solution, can stitch their solution with 3rd party component.		Please See Corrigendum. Requirement of "Logical FW solution from day-1 removed as Physical firewall is being procured." is removed.
37			Bidder should have executed on premises Data Center IT related one work order value of 10Cr or 2 Order of value 7 Cr in the last 3 financial years as on bid submission.	Please consider to change two orders of value 3 Crore in the atleast 3 financial years on bid submission. As the turnover asked in 20Cr. So reference order asked can be maximum 3 CR. This would enable more bidders to participate and inturn more competition would help bring aggressive commercials price for this bid.		No Change, As per RFP
38	HCI Solution		Solution should also have capability to use Software Defined Networking, must propose the Logical FW Solution from day-1 considering the GVK Security.	Request you also add : Logical Routing capabilities to avoid traffic Hairpinning, In a traditional scenario, all inter-VLAN traffic initiates from VM (in one VLAN) to TOR – CORE Switch where the routing is checked and the traffic is sent back to TOR and to Destination VM (in another VLAN). Due to this VM to VM traffic moves all the way from Virtual – Physical – Virtual environment which causes utilization to the uplinks and increases utilization on Core Switches everytime. Adding Logical routing capabilities helps achieve Inter-VLAN traffic from VM to VM at the virtual layer itself, as all the routing is done at the virtual layer. This eliminates the utilization on the Uplink links and further utilization on the Core Switches as well. Hence, we request to consider this capability in the current RFP. Any OEM/Bidder who cannot offer this functionality within their solution, can stitch their solution with 3rd party component.		Please See Corrigendum. Requirement of "Logical FW solution from day-1 removed as Physical firewall is being procured." is removed.

39	Firewall		Firewall Throughput	38,000 Mbps	75,000 Mbps	Please see Firewall spec sheet
40			IPS Throughput	9820 Mbps	11500 Mbps	Please see Firewall spec sheet
41			Threat protection Throughput	2000 Mbps	9 GBPS	Please see Firewall spec sheet
42			IPsec VPN throughput	17000 Mbps	55 GBPS	Please see Firewall spec sheet
43		Features : Web Policy	~~Client Authentication Agent for dedicated per-user tracking~~	Kindly Remove		Please see Firewall spec sheet
44		Web Application Firewall Protection	~~URL hardening engine with deep-linking and directory traversal prevention~~	Kindly Remove		Please see Firewall spec sheet
45			~~Form hardening engine~~	Kindly Remove		Please see Firewall spec sheet
46			~~Dual Antivirus engines~~	Kindly Remove		Please see Firewall spec sheet
47			Cookie signing with digital signatures	Kindly Remove		Please see Firewall spec sheet
48			~~Path-based routing~~	Kindly Remove		Please see Firewall spec sheet
49			~~Outlook anywhere protocol support~~	Kindly Remove		Please see Firewall spec sheet
50			Reverse authentication (offloading) for form-based and basic authentication for server access	Kindly Remove		Please see Firewall spec sheet
51			Virtual server and physical server abstraction	Kindly Remove		Please see Firewall spec sheet
52			Integrated load balancer spreads visitors across multiple servers	Kindly Remove		Please see Firewall spec sheet
53			~~Skip individual checks in a granular fashion~~	Kindly Remove		Please see Firewall spec sheet
54			~~Support for logical and/or operators~~	Kindly Remove		Please see Firewall spec sheet
55			~~Wildcard support for server paths~~	Kindly Remove		Please see Firewall spec sheet
56			~~Automatically append a prefix/suffix for authentication~~	Kindly Remove		Please see Firewall spec sheet
57			~~On-box reporting: Packet filter, intrusion protection, bandwidth and day/week/month/year scales~~	Kindly Remove		Please see Firewall spec sheet
58			Identity-based reporting	Kindly Remove		Please see Firewall spec sheet
59			~~URL filter override report~~	Kindly Remove		Please see Firewall spec sheet

60			Per-user tracking and auditing	Kindly Remove		Please see Firewall spec sheet
61			Anonymization of reporting data to enforce privacy policy	Kindly Remove		Please see Firewall spec sheet
62		Email Protection	~~Recipient Verification against Active Directory account~~	Kindly Remove		Please see Firewall spec sheet
63			~~Dual antivirus engines~~	Kindly Remove		Please see Firewall spec sheet
64		Network Switch (48-port 10G L3 fully managed) - 2 nos.	The switch should support minimum 3.6Tbps of Switching Performance with 1320Mpps of Forwarding rate less than five microsecond latency.	The switch should support minimum 3.6Tbps of Switching Performance with 1200Mpps of Forwarding rate less than five microsecond latency.		No Change, As per RFP
65		Network Switch (48-port 10G L3 fully managed) - 2 nos.	All Optic and modules offered should be hot swappable and fully populated.	Transceiver type & speed required to be mentioned		No Change, As per RFP
66		Network Switch (48-port 1G L3 fully managed) – 4 nos.	The switch should support minimum 212GBPS of Switching Performance with 158Mpps of Forwarding rate	The switch should support minimum 136GBPS of Switching Performance with 102Mpps of Forwarding rate		No Change, As per RFP
67		Network Switch (24-port 1G L2 managed) – 48 nos.	The switch should support minimum 128 Gbps or higher of Switching Performance with 95 Mpps or higher of Forwarding rate	The switch should support minimum 88GBPS of Switching Performance with 65Mpps of Forwarding rate		No Change, As per RFP
68		Network Switch (24-port 1G L2 managed) – 48 nos.	All Optic and modules offered should be hot swappable and fully populated.	Transceiver type & speed required to be mentioned		No Change, As per RFP
69	Firewall Throughput	38,000 Mbps	NGFW throughput : 17 Gbps	Requested feature set are from next gen firewall , hence request to consider Throughput with NGFW feature		Please see Firewall spec sheet
70	IPsec VPN throughput	17000 Mbps	Ipsec Vpn Throughput : 8	Ipsec vpn throughput is very high		Please see Firewall spec sheet
71	Flexi Port Modules	8 x Port GbE Copper	8 x Port GbE SFP Fiber 8 x Port 10 GbE SFP+ Fiber	OEM specific point		Please see Firewall spec sheet
72		8 x Port GbE SFP Fiber				Please see Firewall spec sheet
73		4 x Port 10 GbE SFP+ Fiber				Please see Firewall spec sheet
74		4 x Port GbE Copper Bypass (2 Pairs)				Please see Firewall spec sheet
75		4 x Port GbE Copper PoE+4 Port 2.5 GbE Copper PoE				Please see Firewall spec sheet
76		2 x Port GbE Fiber(LC) Bypass+4				Please see Firewall spec sheet

		Port GbE SFP Fiber				
77	Firewall	UTM/Firewall Security with all the features and 5 years subscription	UTM/NGFW Security with all the features and 5 years subscription			Please see Firewall spec sheet
78	Features : Web Protection	View traffic in real-time, choose to block or shape Malware scanning: HTTP/S, FTP and web-based email via dual independent antivirus engines to block all forms of viruses, web malware, Trojans and spyware	View traffic in real-time, choose to block or shape Malware scanning: HTTP/S, FTP HTTP, SMTP, IMAP, POP3, FTP,	For protecting organisation against unknown and zero-day threats, different OEM use different approach like AV or APT and hence requesting change		Please see Firewall spec sheet
79		Active content filter: File extension, MIME type, JavaScript, ActiveX, Java and Flash	To be removed	Functionality of Web proxy solution or WAF		Please see Firewall spec sheet
80	Features : Web Policy	Proxy Modes: Standard, (Fully) Transparent, Authenticated, Single sign-on and Transparent with AD SSO	To be removed	Functionality of Web proxy solution		Please see Firewall spec sheet
81		Browsing quota time policies and quota reset option	Browsing quota time policies	Functionality of Web proxy solution		Please see Firewall spec sheet
82		Client Authentication Agent for dedicated per-user tracking	To be removed	Functionality of Web proxy solution		Please see Firewall spec sheet
83		Cloning of security profiles Customizable user-messages for events in local languages	To be removed	OEM specific point		Please see Firewall spec sheet
84		Setup wizard and context	To be removed	OEM specific point		Please see Firewall spec sheet

		sensitive online help				
85	Management	Self-service user portal for VPN setup	To be removed			Please see Firewall spec sheet
86	Features : Network Routing and Services	Bridging with STP support and ARP broadcast forwarding	To be removed			Please see Firewall spec sheet
87		WAN link balancing: multiple Internet connections, auto-link health check, automatic failover, automatic and weighted balancing and granular multipath rules	The solution should support ISP load sharing/balancing with failover based on defined SLA	asked wan balancing requires a dedicated link load balancer solution		Please see Firewall spec sheet
88		QoS with full control over bandwidth pools and download throttling using Stochastic Fairness Queuing and Random Early Detection on inbound traffic	QoS with full control over bandwidth pools and upload/download throttling	OEM specific point		Please see Firewall spec sheet
89		Server load balancing	To be removed	Not functionality of firewall.		Please see Firewall spec sheet
90	Features : Network Protection	Connection tracking helpers: FTP, IRC, PPTP, TFTP	The system can generate logs of the connections. Should support troubleshooting techniques like Packet tracer and capture	OEM specific point		Please see Firewall spec sheet
91	Features : Authentication	Transparent, proxy NTLM authentication or client authentication	To be removed	Functionality of Web proxy solution		Please see Firewall spec sheet
92		Authentication via: Active Directory, eDirectory RADIUS, LDAP and TACACS+	Authentication via: Active Directory, eDirectory RADIUS, LDAP	Tacacs is used for device admin.		Please see Firewall spec sheet

93		Automatic user creation	To be removed	Feature set of AAA or NAC		Please see Firewall spec sheet
94		Complex password enforcement	To be removed	Feature set of AAA or NAC		Please see Firewall spec sheet
95	Web Applicatio n Firewall	Reverse proxy	To be removed	OEM specific point and Requested feature set is functionality of WAF not NGFW		Please see Firewall spec sheet
96	Protection	URL hardening engine with deep-linking and directory traversal prevention				Please see Firewall spec sheet
97		Form hardening engine				Please see Firewall spec sheet
98		SQL injection protection				Please see Firewall spec sheet
99		Cross-site scripting protection				Please see Firewall spec sheet
100		Dual Antivirus engines				Please see Firewall spec sheet
101		HTTPS (SSL) encryption offloading				Please see Firewall spec sheet
102		Cookie signing with digital signatures				Please see Firewall spec sheet
103		Path-based routing				Please see Firewall spec sheet
104		Outlook anywhere protocol support				Please see Firewall spec sheet
105		Reverse authenticati on (offloading) for form-based and basic authenticati on for server access				Please see Firewall spec sheet
106		Virtual server and physical server abstraction				Please see Firewall spec sheet
107		Integrated load balancer spreads visitors across multiple servers				Please see Firewall spec sheet
108		Skip individual checks in a				Please see Firewall spec sheet

		granular fashion				
109		Match requests from source networks or specified target URLs				Please see Firewall spec sheet
110		Support for logical and/or operators				Please see Firewall spec sheet
111		Options to change WAF performance parameters				Please see Firewall spec sheet
112		Scan size limit option				Please see Firewall spec sheet
113		Allow/Block IP ranges				Please see Firewall spec sheet
114		Wildcard support for server paths				Please see Firewall spec sheet
115		Automatically append a prefix/suffix for authentication				Please see Firewall spec sheet
116		Logging and Reporting :				Please see Firewall spec sheet
117		Logging: Remote syslog				Please see Firewall spec sheet
118		On-box reporting: Packet filter, intrusion protection, bandwidth and day/week/month/year scales				Please see Firewall spec sheet
119		Identity-based reporting				Please see Firewall spec sheet
120		PDF report exporting				Please see Firewall spec sheet
121		Executive report scheduling and archiving				Please see Firewall spec sheet
122		Daily activity reporting				Please see Firewall spec sheet
123		URL filter override report				Please see Firewall spec sheet
124		Per-user tracking and auditing				Please see Firewall spec sheet

125		Anonymization of reporting data to enforce privacy policy				Please see Firewall spec sheet
126		Full transaction log of all activity in human-readable format				Please see Firewall spec sheet
127		Web log searching parameters per user, URL or action				Please see Firewall spec sheet
128	Email Protection	Block spam and malware during the SMTP transaction	To be removed	For protection of email traffic a dedicated email security solution is required which is inline and accepts taffic as MTA and then take decision.		Please see Firewall spec sheet
129		Detects phishing URLs within e-mails				Please see Firewall spec sheet
130		Global & per-user domain and address black/white lists				Please see Firewall spec sheet
131		Recipient Verification against Active Directory account				Please see Firewall spec sheet
132		E-mail scanning with SMTP and POP3 support				Please see Firewall spec sheet
133		Dual antivirus engines				Please see Firewall spec sheet
134		True-File-Type detection/scan within archive files				Please see Firewall spec sheet
135		Scan embedded mail formats: Block malicious and unwanted files with				Please see Firewall spec sheet
136		MIME type checking				Please see Firewall spec sheet
137		Quarantine unscannable or over-sized messages				Please see Firewall spec sheet

138		Filter mail for unlimited domains and mailboxes				Please see Firewall spec sheet
139		Automatic signature and pattern updates				Please see Firewall spec sheet
140		Should support more than 25,000 (excluding custom signatures) IPS signatures or more	to be added as suggestion	Since IPS leverages signature to match against pattern, hence it is critical that solution should have high number of signature or extreme database		Please see Firewall spec sheet
141		Should support more than 4000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness	to be added as suggestion	Help organization for enforcing granular application control		Please see Firewall spec sheet
142		Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.	to be added as suggestion	Automatic tuning feature help maximize protection and sensor performance and significantly reduce, or virtually eliminate, the manual effort required to tune IPS sensors		Please see Firewall spec sheet
143		Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 280 million of URLs in more than	to be added as suggestion	More granular catergories help organization define precise list of websites which their users are permitted to access		Please see Firewall spec sheet

		80 categories.				
144		Should have the capability of passively gathering information about virtual machine traffic, network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.	to be added as suggestion			Please see Firewall spec sheet
145		Solution should support feature Policy Based Routing with match condition like port, address, protocol, applications	to be added as suggestion			Please see Firewall spec sheet
146		Make/Brand	Hyper Converged infrastructure OEM shall be in Leaders Quadrant of latest Gartner Magic Quadrant for Hyper Converged infrastructure software respectively	**Change Request:** Please rephrase the clause for wider participation of OEM: "Proposed solution must be “Hyper Converged Infrastructure” listed in the leaders’ quadrant of latest Gartner’s Magic Quadrant/Leaders or in latest Forrestor report for Hyper Converged Infrastructure."		No Change, As per RFP

147		Hyper Converged Appliance	Proposed HCI Solution must be hardware OEM Agnostic and must support all the major OEM for the future investment protection. And the license must be portable to the other hardware OEM procured in future.	**Change request:** This point is OEM specific. Request to remove this clause for wider participation of OEMs. **Justification:** Cisco's HCI solution is engineered to run on Cisco's UCS hardware platform only. Cisco's solution is factory shipped engineered & integrated appliance. All the components of HCI in our solution such as compute nodes, hypervisor OS, storage disks, management software are factory installed and shipped ready for fast deployment. This approach alleviates problems like: 1) Introducing another silo of stand-alone hardware with custom management and deployment 2) Lacking integrated networking fabric resulting in longer deployment and configuration time 3) Software only model adds support complexity. As hardware support will be from different OEM.		No Change, As per RFP
148		HCI	Sotution should also have capability to use Software Defined Networking, must propose the Logical FW Solution from day-1 considering the GVK Security.	**Change Request:** To be removed **Justification:** Cisco does not support micro-segmentation as part of the HCI solution. We support micro-segmentation through our SDN (software defined networking) solution called as ACI (Application centric Infrastructure) that is based on Nexus 9K switch deployed in Spine-leaf topology. Asking micro-segmentation as part of the HCI solution will restrict our participation. Note: Hypervisor based SDN solution that provides micro-segmentation is only supported by few vendors and will have following limitations: 1) Micro-segmentation support only for virtual workloads; limited or no support for bare metal or physical workloads 2) Are not hypervisor agnostic (for e.g.: VMware NSX supports only VMware ESXi) 3) They cannot automate the underlay and the physical network		Please See Corrigendum. Requirement of "Logical FW solution from day-1 removed as Physical firewall is being procured." is removed.

149		Config	*The cluster should be configured with minimum 5 Node : *280 physical usable cores, 1.5TB ram, 60TB usable storage capacity across the 5 node cluster. (w/O HCI Overhead, Bidder need to consider the HCI overhead Separately) *Each Node must be populated with minimum 2*1.6TB SSD or more per node for caching and full capacity of the SSD must be available to server caching and capacity requirement, Caching must be redundant in nature and failure of single SSD must not consider as a node failure *Each node should be Configured with 4*10/25Gbps LAN ports.	**Change Request** *The cluster should be configured with minimum 5 Node : *280 physical usable cores, 1.5TB ram, 60TB usable storage capacity across the 5 node cluster. (w/O HCI Overhead, Bidder need to consider the HCI overhead Separately) The Proposed HCI nodes should have Cache Drives for Caching. Failure in cache drive should not fail the entire node. *Each node should be Configured with 4*10/25Gbps LAN ports. **Justification:** Cisco's HCI data platform implements a distributed, log-structured file system. It uses the node's memory and SSD drives as part of a distributed caching layer (creates a cache pool of SSDs), and it uses the node's HDDs (in case of hybrid node), SSD drives (in case of All flash nodes), NVMe drives (in case of NVMe nodes) as a distributed capacity layer. We do not store VM data on the cache drives. For write operations, data is written to the local SSD or NVMe cache, and the replicas are written to remote caches in parallel before the write operation is acknowledged. Writes are later synchronously flushed to the capacity layer HDDs (for hybrid nodes) or SSD drives (for all-flash nodes) or NVMe storage (for NVMe nodes). If the cache SSD fails, the cluster remains highly available. The VMs will keep on running since Cisco's HCI storage controller VM is still running and will get the data from and to the HCI Data Platform in conjunction with the other nodes and the residing Hyperflex storage controller VMs on those nodes. Data will always be accessible. Our approach of data distribution stripes data evenly across all nodes and prevents both network and storage hot spots and maintains the I/O performance regardless of virtual machine location; in contrast to other solutions that are built on node-local affinity and can easily cause data hotspots/performance issues Note: This clause is proprietary to Nutanix. Both Cisco and VMware do not support this.		Please See Corrigendum.
150		Top of rack networking	Solution Should have no dependency proprietary interconnect i.e. should have Capability to Connect 3rd Party network switch well and proposed HCI solution should not have any dependency on underlying networking switches	Change request: Request to rephrase clause as per below for wider participations. Solution should have Capability to Connect 3rd Party network switch or fabric interconnect as well and proposed HCI solution should not have any dependency on underlying networking switches		No Change, As per RFP