Annexure 1

Tender Enquiry No: RFP/NCIIPC/Open/01
Addendum 1

Delivery of Hardware, Software & Operations for Creation of IT Infrastructure

(Design, Build, Installation, Testing Commissioning, Integration, and Operations & Maintenance of IT Infrastructure for AI Grand challenge)

Foundation For Innovation and Technology Transfer New Delhi, India

Part - A

Key Points:

1. **All revisions to the document are clearly shown. Struck-out text indicates the removed original wording, and text highlighted in yellow indicates the new, added wording)**
2. [Deleted in Addendum 1] means that there been no change done in the clause from RFP hence it has been deleted from the Addendum.
3. Numbering of all paras has been retained as was given in RFP for ease of reference
4. Key Points Discussed
    a) **AMD Processors**: Committee members evaluated the request and amended the Processor for Non-GPU server and Workstations to be Intel or AMD. The details are in the attached Addendum 1
    b) **VMware VCF/vSAN hosting platform services** the project is to be established in a running Tier 3 data center and large number of services are already on VMware VCF/vSAN ESA. Hence the requirement of the application is not being changed
    c) **Open-Source Scheduler** Flexibility Bidders may propose any open-source or equivalent commercial scheduler. The RFP remains flexible and does not restrict OEMs.
    d) **Cybersecurity Suite** EDR and storage-security components are excluded. Vendors may offer any OEM or open-source SIEM + HIDS solution per Clause 10.4.3 (No license cost implementation included).
    e) **Storage configuration** The same has been revised from 20% NVME to 100 % NVMe-based
    f) **Switches** No where is the Make specified. Vendors can provide switches as per the Technical Specifications given in the Addendum 1
    g) Certifications: ISO-27001is required
    h) EMD is required to be deposited as mentioned in RFP

****

PART – A

Tender Document

1. Fact Sheet [Deleted in Addendum 1]
2. Project Profile & Background [Deleted in Addendum 1]
3. Invitation for Bid [Deleted in Addendum 1]
4. Brief Scope of Work [Deleted in Addendum 1]
5. Pre-Qualification / Eligibility Criteria

S#	Criteria	Criteria Description	Documents / Proof to be submitted
1.	**Legal Entity**	(A) A company registered in India under Indian Companies Act, 1956 OR (B) A partnership firm registered under Indian Partnership Act, 1932. OR (C) Limited liability partnership company (LLP) under Indian LLP act 2008.	- Copy of valid Registration Certificates - Copy of Certificates of incorporation - Partnership deed And any other relevant document to satisfy legal entity condition. ***Prime Bidder and the Consortium partner to comply the above separately.***
2.	**Financial Turnover**	The average annual turnover of the Prime Bidder and/or its consortium partner jointly during the last 3 financial years ending with year 2024-25 should not be less than INR 35 Crores from Govt./ PSU/ BFSI/ telecom/ Enterprise Infrastructure Projects (as per the last published audited balance sheets	- Audited Balance Sheets - CA Certificate with CA's Registration Number & Seal.
3.	**Financial: Net Worth**	The net worth of the Prime Bidder and its consortium partner in the last three financial year (asper the last published audited balance sheets), should be 'Positive' in each financial year.	- CA Certificate with CA's Registration Number & Seal ***Prime Bidder and the Consortium partner to comply the above separately.***

S#	Criteria	Criteria Description	Documents / Proof to be submitted
4.	**Technical Capability**	During the last Five years, the Prime bidder should have implemented and completed similar project (Similar work means handled Creation of datacenter, storage, compute , NW security…) along with Information technology products supply installation for a reputed Govt./ PSU/ BFSI/ telecom/ Enterprise / Integrated Command Control Centre/ Data Centre (DC) / Network Operation center (NOC) with A. Single order of value 15 Crore or more, OR B. Two orders each having value of 8 Crores or more, OR C. Three orders each having value of 6 Crores or more.	Work Completion Certificates from the client. OR Work Order + Self Certificate of Completion (CA Certificate with CA's Registration Number and Seal) OR Work Order + Phase Completion Certificate from the client showing acceptance of completion of supply and installation. ***Prime Bidder and the Consortium partner to comply the above jointly or separately***
5.	**Certifications**	The Prime bidder and/or its consortium partner should have followed certification: 1. Valid ISO 9001:2015 or latest 2. Valid ISO 27001:2013 or latest	Copy of valid certificate ***Prime Bidder and the Consortium partner to comply the above jointly or separately***
6.	**Market Share and Ranking Clause**	The Original Equipment Manufacturer (OEM) for servers, GPUs, network switches, or any other hardware being bid must be a globally recognized leading vendor in the respective product category, having been ranked among the top five vendors in **market share** or appear in the magic quadrant for at least one of the last four quarters, as per the latest available industry tracker reports from an independent and reputed market research firm (e.g., IDC, Gartner, or equivalent."	Copy of valid certificate ***Prime Bidder and the Consortium partner to comply the above jointly or separately***
7.	**Mandatory Undertaking**	Bidder should: a) not be insolvent, in receivership, bankrupt or being wound up, not	A Self Certified letter - Self-Declaration

S#	Criteria	Criteria Description	Documents / Proof to be submitted
		have its affairs administered by a court or a judicial officer, not have its business activities suspended and must not be the subject of legal proceedings for any of the foregoing reasons; b) not have, and their directors and officers not have, been convicted of any criminal offence related to their professional conduct or the making of false statements or misrepresentations as to their qualifications to enter into a procurement contract within a period of three years preceding the commencement of the procurement process, or not have been otherwise disqualified pursuant to debarment proceedings; c) Not have a conflict of interest in the procurement in question as specified in the bidding document. d) Comply with the code of integrity as specified in the bidding document.	***Prime Bidder and the Consortium partner to comply the above separately.***
8.	**Manpower Strength**	The Prime Bidder and its consortium partner should have at least 10 IT professionals on its rolls as on 31st March 2025.	Letter from HR of the firm duly signed and sealed of the firm.
9.	**Local Presence**	Prime Bidder must have a functional office in Delhi operating since last 5 years.	GST and PAN details should be furnished. ***Prime Bidder and the Consortium partner to comply the above jointly or separately***

7. Instruction to Bidders (ITB) [Deleted in Addendum 1]

8. General Conditions of Contract [Deleted in Addendum 1]

9. Design Consideration [Deleted in Addendum 1]

10. Scope of Work (SANCT) [Deleted in Addendum 1]

10.1. Overview HW and SW

e) **Storage 1**00TB storage (PFS/NAS/object storage/ any others storage) for the GPU cluster which shall provide at least ~~200~~ 160 Gbps or 20 ~~25~~GBps throughput with NVMe disks (~~20% of100TB)~~ Low latency and Scalable

10.2. Summary BoM (Quantities) [Deleted in Addendum 1]

10.3. Detailed Hardware BoM

b) VCF/vSAN ESA Servers (Platform Cluster)

- ~~Intel based **CPU:** 2× latest 4th -gen or higher server CPUs (≥ 32 cores each)~~

Minimum of two (2) x86-architecture server processors. Each processor must be equipped with thirty-two (32) or more physical cores. Eligible processor families include the Intel 4th Generation Xeon Scalable series (or newer) or the AMD 4th Generation EPYC 9004 series (or newer)

- **NVMe for vSAN ESA:** capacity to achieve **≥ 100 TB usable** (FTT=1) across 8 nodes; recommend ≥ **20-24 TB raw per node** using 6–8× 3.84–7.68 TB NVMe devices

  Equivalent configurations from **any OEM meeting the performance, endurance, and compatibility requirements of VCF/ vSAN ESA** shall be acceptable.

c) Storage

- Minimum ~~**200**~~ **160 Gbps (~~25~~ 20 GB/s)** sustained read/write throughput
- Minimum usable **100 TB** (scalable beyond ~~1 PB~~ 500 TB without major re-architecture)

~~At least **20% of capacity (~20 TB)** on~~ NVMe SSDs (tier-0) for hot data, balance may be HDD or other SSD tier

d) Switch & Firewalls

18.2 Proforma 2: Declaration of Acceptance of Terms & Conditions of RFP [Deleted in Addendum 1]

18.3 Proforma 3: Format of Technical Proposal Document [Deleted in Addendum 1]

18.4 Proforma 4: Format for furnishing Earnest Money Deposit [Deleted in Addendum 1]

18.5 Proforma 5: Undertaking on Not Being Black-Listed [Deleted in Addendum 1]

18.6 Proforma 6: Undertaking of Service Level Compliance [Deleted in Addendum 1]

18.7 Proforma 7: Authorization Letters from OEMs [Deleted in Addendum 1]

18.8 Proforma 8: Technical specification compliance by OEM/Bidder. [Deleted in Addendum 1]

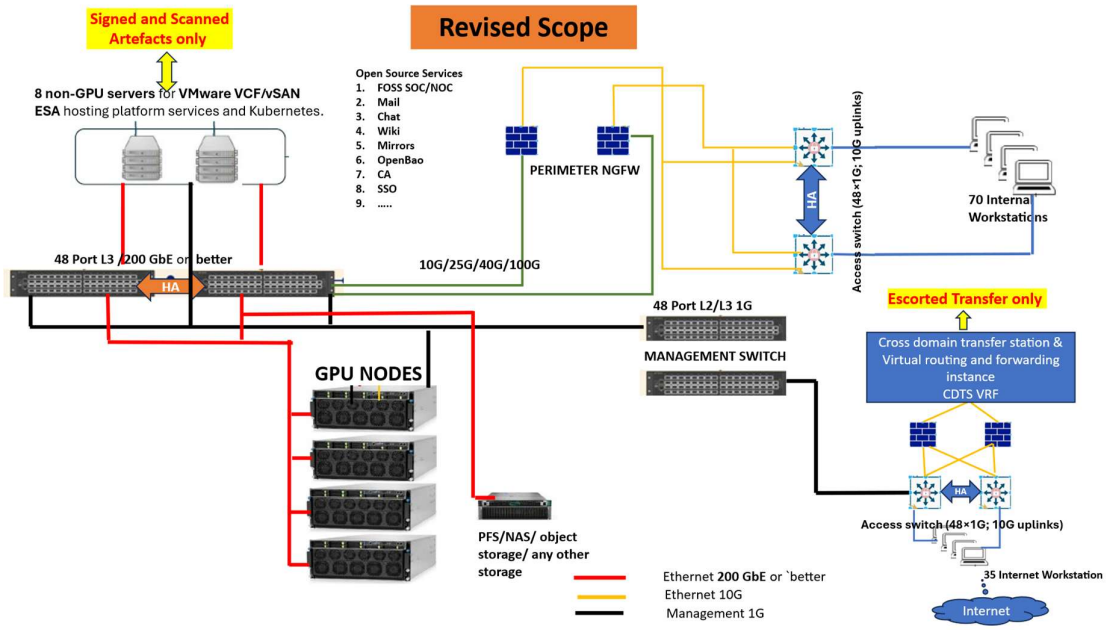
18.9 Proforma 9: Project Credentials Format [Deleted in Addendum 1]

18.10 Proforma 10: Format for Performance for Bank Guarantee (PBG)

PART B

TECHNICAL SPECIFICATION HARDWARE, PROJECT GOVERNANCE and SECURITY

1. Technical Specification and compliances



NOTE: Separate management Switch 16 Port for CDTS enclave

2. Hardware

2.1. GPU Server

Sl NO	Components	Specifications	Compliance Yes/No
1	CPU	Min Two or more Intel based x86 Architecture based server Processors*,Each CPU with at least 56 Cores,2.1GHz Base or higher with 105MB Cache or more.	
2	RAM	2048 GB using Dual Rank x4 DDR5-5600 Registered Standard Memory or better Registered ECC RAM installed from day one. Total 24 DIMM Slots or higher.	
3	Storage for OS	Each Node must have the provision to be configured with minimum 2 (or More)x 480 GB SATA SSD/NVME M.2 Drives for OS	
4	Local Storage	6–8× U.2/U.3 NVMe (≥ 3.84 TB each) for OS/scratch	
5	Networking	2× **200 GbE** (QSFP56/112G-ready)	

6	Networking GPU	Embedded dual port 1/10GbE Copper for Management	
		The proposed system must have a PCI-5 slots as per industry standards if proposed	
		Minimum 2 USB ports per node	
		Each Node must be configured with 8 x H200 141GB GPUs connected connected with 4-way NVIDIA NVLink bridge bidirectional communication bandwidth The GPU card should be able to logically slice during the submission of jobs; that is a job can be submitted in all or any of the GPU card through the Workload Manager The quoted model at time of application of EoI should be available in the market place of NVIDIA.	
7	GPU Memory	The total aggregate memory per node from the GPUs should be at least 1128 GB.	
8	Multi Instance GPU	The deployed system must utilize the full capabilities of **Multi-Instance GPU (MIG)** technology, enabling a single GPU to be securely partitioned into a maximum of seven (7) isolated instances. • **NVIDIA AI Enterprise Requirement:** Since the H200 GPU often includes a bundled **NVIDIA AI Enterprise** software subscription , this subscription **must be supplied, activated, and fully transferable** to the organization upon project handover. • **Supplementary Software:** All additional software required to provide the slicing, fair-share scheduling, and resource management functionality within the operating environment (e.g., in a virtualized or Kubernetes-based cluster) must be included in the supply.	
9	Power Supply	6x 2800-Watt capacity or similar high wattage per server system providing N+1	

		or better redundant hot-swap Power Supplies	
10	Industry Standard Compliance	1. ~~ACPI 6.3 or above complaint~~	
11	Industry Standard Compliance	2. PCIe Base Specification Rev. 4.0 or above Compliant	
		~~3.WOL Support~~	
		4.PXE Support	
		5.VGA/Display Port	
		6.USB Specification 2.7 or above Compliant	
		7. 80 Plus compliant	
		~~8.SMBIOS 2.7 or above complaint~~	
		9.Redfish API	
		10.IPMI 2.0	
		~~11.Advanced Encryption Standard (AES) support~~	
		~~12.SNMP v3~~	
12	Embedded Remote Management System management and system security	Integrated management controller should support: OEM's server management software should be provided. Hardware and management software should be from the same OEM.	
		a. Monitoring fan, power supply, memory, CPU, RAID, NIC for failures.	
		b. Silicon root of trust/Hardware root of trust, authenticated BIOS, signed firmware updates	
		c. Real-time power meter, temperature monitoring, Policy based administration and management of System Temperature and Cooling Sub-System	
		Secure Boot that enables the system firmware, option card firmware, operating systems, and software collaborate to enhance platform security	
13	Operating System Operating Environment Latest Versions	a) Red Hat Enterprise Linux (RHEL)	
		b) Ubuntu	
		Quoted OS should be under enterprise support from the OEM/SI	
		Air cooled with support up to 30 degrees C inlet	
14	Installation	Installation, Testing, Training, and Implementation costs for all above	

		mentioned solution must be included from day one.	
15	Form Factor	6U rack mountable or lower	
16	Warranty	3 years + 2 years EoL(End of Life) support	

2.2. Non GPU Server VCF/vSAN ESA Servers (Platform Cluster)

Item	Description of Requirement	Compliance Yes/No
Chassis	1U/2U Rack Mountable	
CPU	~~Min Two or more Intel based x86 Architecture based server Processors*, Each CPU with at (≥ 32 Cores 4th Gen or Higher)~~ Minimum of two (2) x86-architecture server processors. Each processor must be equipped with thirty-two (32) or more physical cores. Eligible processor families include the Intel 4th Generation Xeon Scalable series (or newer) or the AMD 4th Generation EPYC 9004 series (or newer)."	
Chipset	Compatible with C741-class chipsets or equivalent, supporting processors with equivalent or higher specifications to meet the required performance, scalability, and operational efficiency	
Memory	- ≥ **512 GB RAM** per server -1TB DIMMS scalable up to 8.0 TB using DDR5 Registered DIMM (RDIMM) operating at 4800 MT/s	
Bus Slot	Server should support up to six PCI-Express Slots 4.0/5.0 X16 slots (Can be a mix of 4.0 or 5.0 OR only 5.0) Additional two x8 or higher OCP 3.0 slots or Higher	
HDD Bays	Capacity to achieve **≥ 100 TB usable** (FTT=1) across 8 nodes; recommend ≥ **20-24 TB raw per node** using 6–8× 3.84–7.68 **TB** NVMe devices OR Equivalent configurations from **any OEM meeting the performance, endurance, and compatibility requirements of VCF/vSAN ESA** shall be acceptable.	
~~Controller~~	~~Server should support below controllers, must support Mixed Mode which combines RAID and HBA mode operation simultaneously : Embedded / PCIe based RAID controller with 4GB Flash backed write cache supporting RAID 0, 1, 5, 6, 10, 50, 60. Must support mix-and-match SAS,~~	

	~~SATA, and NVMe drives to the same controller.~~ ~~Controller must support 6G SATA, 12G SAS, 16G NVMe/24 G SSD.~~ ~~Above mentioned controller must support following :~~ ~~1. Hardware root of trust and secure encryption and decryption of critical drive data~~ ~~2. Online Capacity Expansion (OCE)~~ ~~3. Configurable stripe size up to 1 MB~~ ~~4. Global and dedicated Hot Spare with Revertible Hot~~ ~~5. Instant Secure Erase~~ ~~6. Migrate RAID/Stripe Size~~ ~~7. Modifying Cache Write Policy~~ ~~8. Move Logical Drive~~ ~~9. Re-enable Failed Logical Drive~~	
Networking features	25/100 GbE as per leaf uplinks (at least 2×25 GbE per node)	
Interfaces	Serial - 1 (Optional) USB support with Up to 4 total or higher. 1GbE Dedicated management port	
Power Supply	~~Should support hot plug redundant low halogen power supplies with minimum 94% efficiency~~ Should support hot plug redundant platinum rated power supply	
Fans	Redundant hot-plug system fans	
Industry Standard Compliance	~~ACPI 6.3 or above Compliant~~ PCIe 4.0 or above ~~5.0~~ Compliant ~~WOL Support~~ Microsoft® Logo certifications PXE Support Energy Star UEFI 2.7 Redfish API IPMI 2.0 ~~Advanced Encryption Standard (AES) support~~ ~~SNMP v3~~ Active Directory v1.0 ASHRAE A3/A4	
System Security	UEFI Secure Boot and Secure Start support Tamper-free updates - components digitally signed and verified ~~Immutable Silicon Root of Trust~~ Ability to rollback firmware ~~FIPS 140-2 validation~~ Secure erase of NAND/User data	

	~~Common Criteria certification~~ TPM (Trusted Platform Module) 2.0 option Advanced Encryption Standard (AES) on browser Bezel Locking Kit option Support for Commercial National Security Algorithms (CNSA) Chassis Intrusion detection option Secure Recovery - recover critical firmware to known good state on detection of compromised firmware	
Operating Systems and Virtualization Software Support	Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) VMware ESXi. Canonical Ubuntu OpenSource	
Provisioning	1. Should support tool to provision server using RESTful API to discover and deploy servers at scale 2, Provision one to many servers using own scripts to discover and deploy with Scripting Tool (STK) for Windows and Linux or Scripting Tools for Windows PowerShell	
Firmware security	1. For firmware security, system should support remote management chip creating a fingerprint in the silicon, preventing servers from booting up unless the firmware matches the fingerprint. This feature should be immutable 2. Should maintain repository for firmware and drivers recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware 3. End-to-end supply chain controls to ensure component integrity, security, and vendor responsibility 4. One-Button Secure Erase - Making server retirement and redeployment simpler. 5. Security Dashboard for Server to detect possible security vulnerabilities.	
Embedded Remote Management and firmware security	1. System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication 2. Server should have dedicated 1G remote management port 3. Remote management port should have storage space earmarked to be used as a repository for	

	firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware 4. Server should support agentless management using the out-of-band remote management port 5. The server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur 6. Two factor Authentication and Local or Directory-based user accounts with Role based access control 7. Remote console sharing up to 6 users simultaneously during pre-OS and OS runtime operation, 128 bit SSL encryption and Secure Shell Version 2 support. Should provide support for AES on browser. Should provide remote firmware update functionality. Should provide support for Java free graphical remote console. 8. Should support RESTful API integration 9. System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support 10. Should support managing multiple servers as one via : Group Power Control Group Power Capping Group Firmware Update Group Configuration Group Virtual Media/Encrypted Virtual Media Group License Activation	
Server Management	OEM server management Software should be provided. The Hardware and software should be from the same OEM	
	Software should support dashboard view to quickly scan the managed resources to assess the overall health of the data center. It should provide an at-a-glance visual health summary of the resources user is authorized to view.	
	The Dashboard minimum should display a health summary of the following: • Server Profiles • Server Hardware • Appliance alerts	
	The Systems Management software should provide Role-based access control	
	Zero Touch Provisioning (ZTP) using SSDP with remote access or equivalent	

	Management software should support integration with popular virtualization platform management software like Vmware vCenter & vRealize Operations, and Microsoft System Center & Admin Center	
	Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD.	
	Should provide an online portal that can be accessible from anywhere. The portal should provide one stop, online access to the product, support information and provide information to track warranties, support contracts and status. The Portal should also provide a personalized dashboard to monitor device heath, hardware events, contract and warranty status. Should provide a visual status of individual devices and device groups. The Portal should be available on premise (at our location - console based) or off premise (in the cloud).	
	Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.	
	Should have dashboard for firmware baselines while performing minimum required firmware checks and highlighting out-of-compliance devices for updates with the selected firmware baseline	
	The Server Management Software should be of the same brand as of the server supplier.	
Warranty	3 years + 3 years support	

2.3. Storage

Category	**Specification Requirement**	**Compliance Yes/No**
Storage Type	Parallel File System (PFS) / NAS / Object Storage (vendor choice, must meet performance criteria). More than 2 controllers/nodes for HA. Minimum 1.5TB DRAM based cache for ability to cache training datasets	
Primary Use Case	High-throughput data access for GPU clusters (AI/ML, HPC workloads)	
Connectivity	100/200/400 Gbps Ethernet (RoCEv2 or TCP/IP supported); must integrate with GPU servers via Ethernet fabric	
Aggregate Throughput	With NVME Disk Minimum **160 Gbps (20 GB/s)** ~~**or 200 Gbps (25 GB/s)**~~ **more** sustained throughput at 100%	

	read, minimum ~~100~~ 32 Gbps (~~12.5~~ 4GB/s) sustained throughput at 100% write or higher	
Latency	Low-latency design, ≤ 5 **ms** (end-to-end for I/O, 128-512K KB I/O size)	
Storage Capacity	Minimum usable **100 TB** (scalable beyond ~~1 PB~~ 500 TB without major re-architecture)	
Performance Tier	On NVMe SSDs ~~At least **20% of capacity (~20 TB)** on NVMe SSDs~~ (tier-0) for hot data, ~~balance may be HDD or other SSD tier Bidder can provide >20% NVME also~~	
Scalability	Must support linear scaling of throughput and capacity (scale-out architecture)	
Data Protection	Erasure coding or RAID equivalent, ensuring fault tolerance with minimal overhead	
File / Object Protocols	Must support at least **NFSv4.1**, **SMB3**, and/or **S3 API**; POSIX-compliance for Storage solutions	
Security	End-to-end encryption (in-transit TLS 1.2+ and at-rest AES-256) Should not be possible to turn off data at rest encryption; **or should have Encrypted Drives;** Role-Based Access Control (RBAC) / LDAP / AD integration ~~Offered storage must provide autonomous ransomware protection to detect, protect and restore data in case of ransomware attack.~~ ~~Storage must offer following features for protecting critical data-~~ ~~1. Immutable snapshots~~ ~~2. Multi Admin Validation~~ ~~3. Multi Factor Authentication~~ ~~4. Data at rest and in flight encryption~~ ~~5. Synchronous and Asynchronous Replication~~	
Management Interface	Web-based GUI and REST API for monitoring, provisioning, and alerting	
High Availability	No single point of failure; redundant controllers, network paths, and power supplies	
Compatibility	Certified to interoperate with leading GPU server platforms (NVIDIA HGX/DGX or equivalent). Documentation from Nvidia website, on interoperability of offered family of storage to be provided ~~Offered storage OEM must be certified from Nvidia for both BasePOD / SuperPOD architecture.~~	

	~~Documentation from NVIDIA website/Storage OEM, on interoperability of offered family of storage to be provided~~	
Monitoring & Telemetry	Real-time performance metrics, SNMP/Prometheus export	
Rack Space & Power	Vendor to specify; must fit standard 19" racks	
Support	24x7 vendor support, with SLA for critical failures ≤6 hours	

2.4. Switching & Firewalls

2.4.1. DC leaf/L3 Switch (Upto 400G capable)

Sr. No	Specifications	Compliance (Yes/No)
1	**Architecture**	
	The switch should have 32 x 100G/200G/400G QSFP-DD and 2 x 10G SFP+ Ports from day one.	
	The proposed switch should have switching performance of ~~2.5~~ 25 Tbps throughput. All switching and routing are wire-speed to meet the demands of bandwidth-intensive applications today and in the future.	
	The switch should have 128GB SSD RAM/ 32GB Flash and ~~132MB~~ min 16 GB RAM and 120 MB or greater Packet buffer	
	The proposed switch should support High-speed fully distributed architecture	
	The proposed shwich should have High availability with redundancy, and redundant power supplies and fans	
	Switch shall 1RU 19" rack mountable.	
2	**Management**	
	The proposed switch should support automation and programmability using REST APIs or equivalent and Python scripts fine-grained programmability of network tasks	
	The proposed switch should support access to all network state information to allow unique visibility and analytics	
	The proposed switch should support centralized configuration with validation for consistency and compliance	
	The proposed switch should support simultaneous viewing and editing of multiple configurations	
	The proposed switch should support Network health and topology visibility	
	The proposed switch should support Flexible active-active network designs at Layers 2 and Layer 3	
	The proposed switch should support High availability by design during upgrades,Live Upgrade with LACP traffic.	

	The proposed switch should support real-time state and resiliency and allowing individual software modules to be independently upgraded for higher availability	
	The proposed switch should support Industry-standard CLI with a hierarchical structure	
	The proposed switch should able to restricts access to critical configuration commands to offers multiple privilege levels with password protection, ACLs provide SNMP access, local and remote Syslog capabilities to allow logging of all access	
	The proposed switch should support IPSLA or equivalanrt to monitor the network for degradation of various services, including monitoring voice. Monitoring is enabled via the NAE (Network Analytic engine) for history and for automated gathering of additional information when anomalies are detected.	
	The proposed switch should support SNMP v2c/v3	
	The proposed switch should support sFlow (RFC 3176) to Provides scalable ASIC-based wire speed network monitoring and accounting with no impact on network performance and gather a variety of sophisticated network statistics and information for capacity planning and real-time network monitoring purposes.	
	The Proposed switch shall support RMON/Streaming Telemetery/ TFTP/SFTP, IPv4 and IPv6 traceroute and ping, NTP	
	The proposed switch should support IEEE 802.1AB Link Layer Discovery Protocol (LLDP)	
	The proposed switch should support Dual flash images to provide independent primary and secondary operating system files for backup while upgrading	
3	**Quality of Service (QoS)**	
	The proposed switch should support congestion actions	
	The proposed switch should support Strict priority (SP) queuing and Deficit Weighted Round Robin (DWRR)	
	The proposed switch should support Data Center Bridging (DCB)	
	The proposed switch should support lossless Ethernet networking standard PFC, ETS and DCBX.	
	Storage Solution Support, iSCSI, Lossless iSCSI, RDMA over Converged Ethernet version 2 (RoCE v1 and v2) OR ~~and~~ Non-Volatile Memory Express (NVMeOF)	
4	**Resiliency and high availability**	
	The proposed switch should support distributed and redundant architecture by deploying two switches with each switch maintaining independent control and synchronized during upgrades or failover and should support upgrades during live operation.	
	The proposed switch should support Virtual Router Redundancy Protocol (VRRP)	

	The proposed switch should support Ethernet Ring Protection Switching (ERPS) to supports rapid protection and recovery in a ring topology OR loop free setup, like EVPN-Multihoming or MC-LAG with STP enabled for any loop protection	
	The proposed switch should support Unidirectional Link Detection (UDLD)	
	The proposed switch should support IEEE 802.3ad LACP with 128 link aggregation groups (LAGs), each with 16 links per group, with a user-selectable hashing algorithm	
	The proposed switch should support N+1 high reliability with hot swappable, redundant power supplies	
	The proposed switch should support Redundant, Hotswappable and load-sharing fans and power supplies	
	The proposed switch should support Separates control from services and keeps service processing isolated to increases security and performance	
5	**Layer 2 switching**	
	The switch should have 32 K or more ~~64K~~ MAC address table size	
	The proposed switch should support up to 4000 port-based or IEEE 802.1Q-based VLANs	
	The proposed switch should support VLAN Translation	
	~~The proposed switch should support Static VXLAN to manually connect two or more VXLAN tunnel endpoints (VTEP).~~ The switch must support Loop-Free Resiliency and High Availability suitable for a Layer 3 ECMP Data Center Leaf/Spine architecture. Mandatory support includes: 1. Multi-Path/Fast Convergence: Support for large-scale ECMP (≥64-way) for intelligent load-balancing and sub-second convergence upon link or neighbour failure (via BFD or similar mechanism). 2. Server-Facing HA: Support for Multichassis Link Aggregation Group (MC-LAG) or EVPN Multihoming (EVPN-MH) to allow servers to connect to two separate Leaf switches for active-active redundancy without relying on STP. 3. Routing Protocol HA: Support for Graceful Restart for the deployed routing protocol (e.g., BGP) to ensure non-disruptive neighbor transitions during control plane failure.	
	The proposed switch should support Dynamic VXLAN with BGP-EVPN to Deep segmentation for campus networks or Layer 3 designs	
	The proposed switch should support Port mirroring to duplicates port traffic (ingress and egress) to a local or remote monitoring port andsupport minimum 4 mirroring groups with an unlimited number of ports per group	

	The proposed switch should support IEEE 802.1D ~~STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)~~ for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)	
	The proposed switch should support Rapid Per-VLAN spanning tree plus (RPVST+) to allow each VLAN to build a separate spanning tree to improve link bandwidth usage in network environments with multiple VLANs	
6	**Layer 3 routing**	
	The switch should support 60K IPv4 and 30KIPv6 Unicast Routes	
	The proposed switch should support Static IPv4 routing, ~~RIPv2, RIPng,~~ Policy Based Routing (PBR), Border Gateway Protocol 4 (BGP-4)	
	The proposed switch should support Open shortest path first (OSPF) with support of ECMP, NSSA, and MD5 authentication for increased security and graceful restart for faster failure recovery	
	The proposed switch should support Multiprotocol BGP (MP-BGP) with IPv6 Address Family	
	The proposed switch should support 6in4 tunnels to tunnell of IPv6 traffic in an IPv4 network.	
	The proposed switch should support Advanced Layer 2/3 feature set includes BGP, OSPF, VRF-lite, and IPv6	
	The proposed switch should support IP performance optimization to Provides a set of tools to improve the performance of IPv4 networks which include directed broadcasts, customization of TCP parameters, support of ICMP error packets and extensive display capabilities	
	The proposed switch should support Dual IP stack	
	The proposed switch should support Equal-Cost Multipath (ECMP)	
	The proposed switch should support Generic Routing Encapsulation (GRE) Or VxLAN encapsulation with BGP-EVPN.	
7	**Security**	
	The proposed switch should support Access control list (ACL) Feature for both IPv4 and IPv6 and ACLs should also protect control plane services such as SSH, SNMP, NTP or web servers.	
	The proposed switch should support Remote Authentication Dial-In User Service (RADIUS)	
	The proposed switch should support Terminal Access Controller Access-Control System (TACACS+)	
	The proposed switch should support Management access security	
	The proposed switch should support Secure shell (SSHv2)	
8	**Multicast**	
	The switch should support 7000 IPv4 and IPv6 Multicast Routes	
	The proposed switch should support Internet Group Management Protocol (IGMPv1, v2, and v3)	

	~~The proposed switch should support Anycast RP~~ The switch must support Anycast RP to provide redundancy and load-sharing for the Rendezvous Point function	
	~~The proposed switch should support MSDP Mesh Groups to provide redundancy and load-sharing capabilities.~~	
	The proposed switch should support FastLeave (FL) and Forced-FastLeave (FFL)	
	~~The proposed switch should support Multicast Listener Discovery (MLD)~~ The switch must support both Internet Group Management Protocol (IGMP) (for IPv4) and Multicast Listener Discovery (MLD) (for IPv6) Snooping and Querier functions for efficient multicast group management at Layer 2 and Layer 3.	
	~~The proposed switch should support Multicast Service Delivery Protocol (MSDP)~~	
	The proposed switch should support IGMP/MLD Snooping	
	The proposed switch should support Protocol Independent Multicast (PIM)	
	The proposed switch should support PIM for IPv4 and IPv6 supports one-to-many and many-to-many and support for PIM Sparse Mode/Source Specific mode (PIM-SM/ SSM IPv4 and IPv6).~~The proposed switch should support PIM-Dense Mode~~	
9	~~**Environmental Features**~~	
	~~The proposed switch should support for RoHS (EN 50581:2012) regulations~~	
	~~The Switch shall have common criteria NDPP certified~~	
	~~Compliant with DoDIN, APL, NDcPP, FIPS, and USGv6 requirements for federal certifications.~~	
	~~The switch support Operating temperature of 0°C to 45°C~~	
	~~Immunity~~ ~~EN55024:2015 / CISPR 24:2015, ESD: EN 61000-4-2,~~ ~~Radiated: EN61000-4-3, EFT/Burst: EN 61000-4-4, Surge: EN 61000-4-5~~ ~~Conducted: EN 61000-4-6~~ ~~Power frequency magnetic field: IEC 61000-4-8~~ ~~Voltage dips and interruptions: EN 61000-4-11~~ ~~Harmonics: EN 61000-3-2, IEC 61000-3-2~~ ~~Flicker: EN 61000-3-3, IEC 61000-3-3~~ ~~Emissions~~ ~~EN 55032:2015 / CISPR 32:2015, Class A, VCCI-32:2016~~ ~~Class A, CNS 13483, AS/NZS, ICES-003 Issue 5 FCC CFR 47 Part 15:2010, Class A~~ ~~RoHS-6 Compliant (EN 50581:2012)~~	
10	**Warranty and Support**	
	The switch shall be offered with minimum three years hardware warranty with NBD Shipment and software updates/upgrades from OEM directly and 3 Years EoL support	

	Software upgrades/updates shall be included as part of the warranty	

2.4.2. ~~Enclave Access and Internet LAN Access: 2× switches(Each) , 48×1G copper with 4×10 or 25G uplinks to leafs/L3~~ 48×1G/10G SFP+ Ports and 4 x 40G/100G uplinks to leafs/L3

Sr.No	Minimum Technical Specification	Compliance (Yes/No)
1	**General Features:**	
	The switch should be Gigabit Layer 2 and Layer 3 switch with console/auxiliary ports along with all accessories.	
	Switch should have hot swappable redundant Power Supply and fan tray from day-1.	
	Switch should have non-blocking throughput capability on all ports from day 1	
	Software upgrades, updates shall be included as part of the warranty	
	The switch should be based on programmable ASICs purpose-built to allow for a tighter integration of switch hardware and software or Open Networking Install Environment capabilities to have 3rd party Network OS installed to optimize performance and capacity	
	Switch should have integrated trusted platform module (TPM) or equivalent for platform integrity to ensure the boot process is from trusted source OR The Switch should support image pre-check. The firmware installation is performed only if the result of the pre-check]successful.	
	Switch shall support cloud-based and on-premises management.	
	Operating temperature of 0°C to 45°C	
	All mentioned features (above & below) should be available from day 1. Any license required to be factored from day 1.	
2	**Performance:**	
	Should have 8GB DRAM and 32GB Flash.	
	The switch will have at up to 880 Gbps or higher switching capacity.	
	Forwarding rates: The switch should have 650Mpps or higher forwarding rates.	
	IPv4 Routing entry support : ~~60K~~ 24K or more.	
	IPv6 Routing entry support : ~~60K~~ 12 K or more.	
	IPv4 and IPv6 Multicast Routes : 4K or more. And 1K VLAN simultaneously	
	MAC addresses support: ~~32K~~ 8K or more.	
	VLANs ID: 4K or more and 4K VLANs simultaneously.	
	ACL /QOS entry support : 4K or more.	
	Packet buffer : 8 MB or more	
	The device should be IPv6 ready from day one. Should support the ability to configure backup of the previous configuration automatically.	
3	**Functionality:**	
	The switch should support MC-LAG / vPC / MLAG to allow two switches to form a virtual chassis or have front plane stacking on uplink port or Backplane stacking and should have 200 Gbps of Virtual Chassis	

	performance or Stacking Performance of minimum 160 Gbps. ~~The switch should suppot minimum 10 switch in stack~~	
	The Switch should support long distance across the Rack and Floor Switch virtual-chassis or Stacking..	
	Must support EVPN, VRF, VXLAN, EVPN,OSPFv2 and v3 Routed Access, Policy-Based Routing (PBR), PIM-SM / PIM-DM / PIM-SSM and Virtual Router Redundancy Protocol (VRRP) from Day 1	
	The switch should support IEEE 802.3ad link-aggregation control protocol (LACP) and port trunking.	
	The switch should support IEEE 802.1s Multiple Spanning Tree	
	The switch should support STP, Trunking, Private VLAN (PVLAN) / VLAN autostate / NAT, Q-in-Q, Shaped Round Robin (SRR)/Deficit Weighted Round-Robin (DWRR) scheduling, Committed Information Rate (CIR)/Equivalent and or eight egress queues per port	
	Switch shall support rolled back to the previous successful configuration	
	The switch should support SNMPv1, v2, and v3, SSL, SSHv2, Telnet, ping, traceroute	
	The switch should support TPM & Zero-Touch Provisioning (ZTP). The switch shall support IP SLA for Voice monitors quality of voice traffic using the UDP Jitter and UDP Jitter for VoIP tests	
	Switch should have Data Center Bridging (DCB), Supports lossless Ethernet networking standards to eliminate packet loss due to queue overflow, Priority Flow Control (PFC) 2 priorities per port, Enhanced Transmission Service (ETS) ~~DCB Exchange Protocol (Pre-standard LLDP DCBX IEEE 1.01 version)~~	
	Switch should have SCSI, Lossless iSCSI, RDMA over Converged Ethernet version 2 (RoCE v1 and v2) OR ~~and~~ Non-Volatile Memory Express (NVMe over Fabrics)	
	The switch should be manageable from cloud OR On-premises or Both solution.	
	The switch should support IEEE 802.1X or MAC filtering	
	The switch should support Port-based authentication, if solution is based on 802.1x	
	The switch should support MAC-based authentication, if solution is based on 802.1x	
	The switch should provide IP Layer 3 filtering based on source/destination IP address/subnet and source/destination TCP/UDP port number	
	The switch should support Source-port filtering or IP and Layer-4 port filtering	
	The switch should support RADIUS/TACACS+, Dynamic ARP protection or MAC filterting, Port Security, STP route guard, BPDU guard.	
	OS should have support for Management automation via Netconf/Yang/REST-API, Python or equivalent technology	
	Should support Netflow/Sflow/Jflow, Port mirroring or equivalent technology	
4	**Interface Requirement:**	
	i) 48nos. of 1G/10G SFP+ ports	
	ii) 4 nos. of 100G SFP28 uplink ports.	
5	**Regulatory Compliance:**	
	Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or equivalent Indian Standard like IS-13252:2010 or better for Safety requirements of Information Technology Equipment.	
	Switch shall conform to EN 55022/55032 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B or equivalent Indian Standard like IS 6873 (Part 7): 2012 or better for EMC (Electro Magnetic Compatibility) requirements.	

6	**OEM qualification criteria, Warranty and Support**	
	The switch shall be offered with minimum 3 Years hardware warranty with NBD Shipment and software updates/upgrades from OEM directly and 3 years of Support	
	Switch or Switch's Operating System on different hardware platform should be tested for EAL 2/NDPP or above under Common Criteria Certification OR FIPS Certified	
	The OEM shall be in Leaders Quadrant of Gartner report for DC/Wired & Wireless LAN Infrastructure for minimum 5 Consecutive Years. Or "The OEM shall be in Part of the magic Quadrant of Gartner report for Datacenter Networking/Switching in any of the last 3 years	

2.4.3. A Management/OOB: 2× switches, 48 nos. of 1000 Base-T Ports and 4 x 1G/10G SFP+." OOB-only (BMC/iLO/iDRAC, management ports)

Sr.No	Minimum Technical Specification	Compliance (Yes/No)
1	**General Features:**	
	Access Switch "48 nos. of 1000 Base-T Ports and 4 x 1G/10G SFP+."	
	Access switch should be Gigabit Layer 2/Layer 3 switch with console/auxiliary ports along with all accessories.	
	Switch should have non-blocking throughput capability on all ports from day1.	
	Software upgrades, updates shall be included as part of the warranty.	
	The switch should be based on programmable ASICs purpose-built to allow for a tighter integration of switch hardware and software or Open Networking Install Environment capabilities to have 3rd party Network OS installed to optimize performance and capacity.	
	Switch should have integrated trusted platform module (TPM) or equivalent for platform integrity to ensure the boot process is from trusted source OR The Switch should support image pre-check. The firmware installation is performed only if the result of the pre-check successful.	
	Operating temperature of 0°C to 40°C.	
	All mentioned features (above & below) should be available from day 1. Any license required to be factored from day 1.	
2	**Performance:**	
	Should have 8 GB DRAM and 16 GB Flash.	
	The switch will have at up to 128 or higher Gbps switching capacity.	
	Forwarding rates: The switch should have 95Mpps or Higher forwarding rates.	
	IPv4 Routing entry support : 2K ~~24~~K or more.	
	IPv6 Routing entry support : 1K ~~12K~~ or more.	
	IGMP Groups ~~and~~ OR MLD Group : 1K or more.	
	MAC addresses support: ~~32K~~ 8K or more.	
	VLANs ID: 4K or more and 1K VLANs simultaneously.	
	ACL /QOS entry support : 1K or more.	
	Packet buffer : 8 MB or more	
	The device should be IPv6 ready from day one.	
	Should support the ability to configure backup of the previous configuration automatically.	
3	**Functionality:**	

	The switch should support front plane stacking on uplink port or Backplane stacking or equivalent technology and should have Stacking Performance of minimum 40 Gbps. The switch should support minimum 8 switch in stack."	
	The Switch should support long distance across the Rack and Floor virtual chassis or Switch Stacking.	
	Must support , VXLAN, SPFv2 and v3 Routed Access, Policy-Based Routing (PBR), PIM SM/PIM-SSM/ PIM-DM, and Virtual Router Redundancy Protocol (VRRP) from Day 1.	
	The switch should support IEEE 802.3ad link-aggregation control protocol (LACP) and port trunking.	
	The switch should support IEEE 802.1s Multiple Spanning Tree.	
	The switch should support STP, Trunking, Private VLAN (PVLAN) / VLAN autostate / NAT, Q-in-Q, Shaped Round Robin (SRR)~~STP, Trunking, Private VLAN (PVLAN), VLAN tagging, Q-in- Q,~~ Deficit Weighted Round-Robin(DWRR) or equivalent scheduling, Committed Information Rate (CIR)/Equivalent and eight egress queues per port"	
	Switch shall support rolled back to the previous successful configuration	
	The switch should support SNMPv1, v2, and v3, SSL, SSHv2, Telnet, ping, traceroute	
	The switch should support Zero-Touch Provisioning (ZTP). The switch shall support IP SLA for Voice monitors quality of voice traffic using the UDP Jitter and UDP Jitter for VoIP tests.	
	The switch should be manageable from cloud NMS or On-premises NMS solution offered.	
	The switch should support IEEE 802.1X and MAC filtering	
	The switch should support Port-based authentication,	
	The switch should support MAC-based authentication,	
	The switch should provide IP Layer 3 filtering based on source/destination IP address/subnet and source/destination TCP/UDP port number	
	The switch should support Source-port filtering or IP and Layer-4 port filtering	
	The switch should support RADIUS/TACACS+, Dynamic ARP protection or MAC filterting, Port Security, STP route guard, BPDU guard.	
	OS should have support for Management automation via Netconf/Yang/REST-API, Python or equivalent technology.	
	Should support Netflow/Sflow/Jflow, Port mirroring or equivalent technology.	
4	**Interface Requirement:**	
	48 nos. of 1000 Base-T Ports and 4 x 1G/10G SFP+."	
5	**Regulatory Compliance:**	
	Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or equivalent Indian Standard like IS-13252:2010 or better for Safety requirements of Information Technology Equipment.	
	Switch shall conform to EN 55022/55032 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B or equivalent Indian Standard like IS 6873 (Part 7): 2012 or better for EMC (Electro Magnetic Compatibility) requirements.	
6	**OEM qualification criteria, Warranty and Support**	
	The switch shall be offered with minimum 3 Years hardware warranty with NBD Shipment and software updates/upgrades from OEM directly and 3 years of Support	

	Switch or Switch's Operating System on different hardware platform should be tested for EAL 2/NDPP or above under Common Criteria Certification. OR FIPS Certified	

2.4.4. A Management/OOB: 1× switches,16 nos. of 1000 Base-T Ports and 2 x 1G/10G SFP+." OOB-only (BMC/iLO/iDRAC, management ports)

Sr.No	Minimum Technical Specification	Compliance (Yes/No)
1	**General Features:**	
	Access Switch "16 nos. of 1000 Base-T Ports and 4 x 1G/10G SFP+."	
	Access switch should be Gigabit Layer 2/Layer 3 switch with console/auxiliary ports along with all accessories.	
	Switch should have non-blocking throughput capability on all ports from day1.	
	Software upgrades, updates shall be included as part of the warranty.	
	The switch should be based on programmable ASICs purpose-built to allow for a tighter integration of switch hardware and software or Open Networking Install Environment capabilities to have 3rd party Network OS installed to optimize performance and capacity.	
	Switch should have integrated trusted platform module (TPM) or equivalent for platform integrity to ensure the boot process is from trusted source OR The Switch should support image pre-check. The firmware installation is performed only if the result of the pre-check successful.	
	Operating temperature of 0°C to 40°C.	
	All mentioned features (above & below) should be available from day 1. Any license required to be factored from day 1.	
2	**Performance:**	
	Should have 8 GB DRAM and 16 GB Flash.	
	The switch will have at up to 128 or higher Gbps switching capacity.	
	Forwarding rates: The switch should have24 Mpps or Higher forwarding rates.	
	IPv4 Routing entry support : 2K ~~24~~K or more.	
	IPv6 Routing entry support : 1K ~~12K~~ or more.	
	IGMP Groups and MLD Group : 1K or more.	
	MAC addresses support: ~~32K~~ 8K or more.	
	VLANs ID: 4K or more and 1K VLANs simultaneously.	
	ACL /QOS entry support : 1K or more.	
	Packet buffer : 8 MB or more	
	The device should be IPv6 ready from day one.	
	Should support the ability to configure backup of the previous configuration automatically.	
3	**Functionality:**	
	The switch should support front plane stacking on uplink port or Backplane stacking or equivalent technology and should have Stacking Performance of minimum 40 Gbps. The switch should support minimum 8 switch in stack."	
	The Switch should support long distance across the Rack and Floor virtual chassis or Switch Stacking.	
	Must support , VXLAN, SPFv2 and v3 Routed Access, Policy-Based Routing (PBR), PIM SM/PIM-SSM/ PIM-DM, and Virtual Router Redundancy Protocol (VRRP) from Day 1.	

	The switch should support IEEE 802.3ad link-aggregation control protocol (LACP) and port trunking.	
	The switch should support IEEE 802.1s Multiple Spanning Tree.	
	The switch should support STP, Trunking, Private VLAN (PVLAN) / VLAN autostate / NAT, Q-in-Q, Shaped Round Robin (SRR)~~STP, Trunking, Private VLAN (PVLAN), VLAN tagging, Q-in- Q,~~ Deficit Weighted Round-Robin(DWRR) or equivalent scheduling, Committed Information Rate (CIR)/Equivalent and eight egress queues per port"	
	Switch shall support rolled back to the previous successful configuration	
	The switch should support SNMPv1, v2, and v3, SSL, SSHv2, Telnet, ping, traceroute	
	The switch should support Zero-Touch Provisioning (ZTP). The switch shall support IP SLA for Voice monitors quality of voice traffic using the UDP Jitter and UDP Jitter for VoIP tests.	
	The switch should be manageable from cloud NMS or On-premises NMS solution offered.	
	The switch should support IEEE 802.1X and MAC filtering	
	The switch should support Port-based authentication,	
	The switch should support MAC-based authentication,	
	The switch should provide IP Layer 3 filtering based on source/destination IP address/subnet and source/destination TCP/UDP port number	
	The switch should support Source-port filtering or IP and Layer-4 port filtering	
	The switch should support RADIUS/TACACS+, Dynamic ARP protection or MAC filterting, Port Security, STP route guard, BPDU guard.	
	OS should have support for Management automation via Netconf/Yang/REST-API, Python or equivalent technology.	
	Should support Netflow/Sflow/Jflow, Port mirroring or equivalent technology.	
4	**Interface Requirement:**	
	16 nos. of 1000 Base-T Ports and 2x 1G/10G SFP+."	
5	**Regulatory Compliance:**	
	Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or equivalent Indian Standard like IS-13252:2010 or better for Safety requirements of Information Technology Equipment.	
	Switch shall conform to EN 55022/55032 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B or equivalent Indian Standard like IS 6873 (Part 7): 2012 or better for EMC (Electro Magnetic Compatibility) requirements.	
6	**OEM qualification criteria, Warranty and Support**	
	The switch shall be offered with minimum 3 Years hardware warranty with NBD Shipment and software updates/upgrades from OEM directly and 3 years of Support	
	Switch or Switch's Operating System on different hardware platform should be tested for EAL 2/NDPP or above under Common Criteria Certification.	

Specifications same as Switch in para 2.4.3. above except number of ports is 16

2.4.5. Firewalls

2.4.5.1. Perimeter (Internet LAN): Secure Firewall HA pair with URL filtering, IPS, DNS security

2.4.5.2. ISFW (Internal Segmentation): Secure Firewall HA pair sized for east-west inter-VRF traffic; IPS enabled on allowed flows; no NAT

Common Features

S/N	Specification	Compliance (Yes/No)
1	The Firewall appliance must be non-ASIC based and should have Multi core architecture to mitigate against the sophisticated threats. If option to disable ASIC is there, then OEM must mention the performance numbers in datasheet (without ASIC)	
2	The Firewall appliance must have a hardened operating system from the OEM and should have 8 Core CPU with 32 GB of RAM to make sure all the security capabilities are provided without degradation form day one.	
3	The Firewall appliance must have minimum 8x10G and 8x1G Ports from day 1 with required SR transceivers as per the ports. ~~Also should have atleast 1 additional network I/O slot to add 8*10G or 2x40G or 4*25G ports in future, depending upon organization's choice. If future choice is not possible then all ports to be provided from day1.~~	
4	The Firewall appliance should not be more than 1U rack- mounted design and must have redundant field replaceable/ hot swappable power supply to remove any single point of failure.	
5	The Firewall appliance must deliver 10 Gbps NGFW throughput with Security features (FW, IPS, and Application Control) enabled and 9 Gbps Threat Prevention throughput. The same must be available in the public datasheet. (must submit evidence) OR The Firewall appliance must deliver 9 Gbps Firewall throughput with Application Identification and logging enabled and 6 Gbps Threat Prevention throughput on layer 7. The same must be available in the public datasheet. (must submit evidence).	
6	The Firewall appliance must deliver 35 Gbps of IPSEC VPN throughput from day 1 on layer 3 OR 4 Gbps on Layer 7. ~~and should support 80K concurrent IPsec VPN SAs without any limitation of VPN Clients~~.	
7	The Firewall appliance must deliver ~~minimum 2.5 Gbps of TLS/SSL inspection throughput and~~ 650K or more concurrent inspected HTTP connections from day1 as default value without adding any additional license.	
8	The Firewall appliance must deliver 500K new connections/sessions per sec and 30 million concurrent connections/sessions from day1 and these should be available per appliance as default no's without additional license. OR	

	100K new connections/second and 1 million concurrent connections on layer 7 and these should be available per appliance as default no's without additional license.	
9	The Firewall appliance must have the security features including IPS, Application Awareness, Anti-Bot, DOS prevention, URL filtering, Anti-Malware, AETs including routing features to be managed from the Central console, no need for any configuration via appliance GUI and Appliance CLI. Solution also support integration with Snort.	
10	The solution must use the server name indication for the https traffic for URL categorization without decrypting the https connection	
11	Solution must support client based agent to check the security posture of endpoints and must be able to employ policies basis the attributes. Policy must be defined on NGFW for discarding the user requests if AV is not updated, OS version is Obsolete, Load on Endpoint is high / OR any users is using the obsolete browsers and should not have any dependencies on the number of client supported & there is should not be any license attached to it.	
12	Solution must have support TLS 1.3 and TLS/SSL server certificate verification before decryption decision is taken and must support full-stream reconstruction with high- speed exploit fingerprinting to examines actual payloads along with connection, usage, command controls	
13	Solution must prevent against the websites via URL filtering that mask their identity using Dynamic DNS services, Elevated exposure by website that camouflage their true nature, domain name that are registered recently, parked domain, Unauthorized Mobile Marketplaces to prevent users visiting the websites that may distribute applications unauthorized by the mobile OS manufacture	
14	Solution must be able to prevent the users to visit the websites that use technologies that alter the operation of a user's hardware, software, or network to decrease owner's control with the intent to gain fraudulent access and with potential malicious intent.	
15	Solution must be able to prevent the users to visit the websites that enable download of software applications or file download servers, download of media content, client software to enable peer-to-peer file sharing and transfer, Sites that store personal files on web servers for backup or exchange.	
16	Solution should support Re-authentication when using browser-based user authentication and support 4096 bit RSA key for Browser Based User Authentication.	
17	Solution should support local user creation options via Central Manager and also support the use of external CA issued certificates in internal management communication and Centralized manager should support to block the access temporarily after multiple failed logon attempts from the same IP.	
18	Solution must have enhanced engine monitoring capability and support for non-TCP traffic, applications that use UDP for data transport.	
19	Solution must have the following categories to take action and to use them in the access rule like abused Drugs, adult content & material, alcohol & tobacco, gambling, hacking, Illegal or Questionable, Intolerance, Marijuana, Militancy & Extremist, Nudity, Sex, Advanced Malware, Bot Networks, Compromised Websites, Custom Encrypted Uploads, Malicious Web Sites,	

	Mobile Malware, Phishing and other Frauds, Potentially Exploited Documents, Proxy Avoidance, P2P, Personal Network Storage, Streaming media, spyware, etc Or Equivalent	
20	Solution must be able to detect protocol abnormality & misuse detection with Exploit and malware detection via high-speed DFA.	
21	The Firewall appliance must support L3 protocol functionality like Static & policy-based routing, static multicast routing, dynamic routing like MP-BGP, ~~RIPng~~, OSPF(v2 & v3), IGMP proxy, BGP, BFD, PIM (SM & SSM), and Application-aware routing.	
22	~~The Firewall solution must support IPv4 and IPv6 from day one. Solution should support NAT66, NAT64 , NAT44, and PAT from day 1 and must support Stateless IPv4/IPv6 translation.~~	
23	The Firewall appliance must support IPv6 capability including Dual stack IPv4/IPv6, ICMPv6, DNSv6, IPv6 static, SLAAC, DHCPv6 relay.	
24	The Firewall appliance must support TLS 1.3 and TLS/SSL server certificate verification before decryption decision is taken.	
25	The Firewall appliance must support security proxies for the following TCP, UDP, HTTP, HTTPS, SSH, FTP, TFTP, SFTP, DNS.	
26	The Firewall appliance must have Firewall for stateful blocking, URL filtering, Anti-Spoofing, IP Reputation, Geo- Protection, Dropping Invalid Connections.	
27	The Solution must allow the administrator to configure CRLs to be be fetched and cached even before those are needed for certificate validation.	
28	The Solution must support SNMPv3 with support for SHA-256 and AES-256 algorithms.	
29	The Firewall solution must support L2 interfaces in the L3 deployment and must allow firewall with Layer 2 Interfaces using VXLAN to provides a solution for extending Layer 2 Interfaces across Layer 3 boundaries.	
30	The Firewall management system's web access interface should have an option to authenticate administrators by using client certificates.	
31	The solution must support client based agent to check the security posture of endpoints and must be able to employ policies basis the attributes. Policy must be defined on NGFW for discarding the user requests if AV is not updated, OS version is Obsolete, Load on Endpoint is high ~~/~~ OR any users is using the obsolete browsers.	
32	Solution must allow mixing of preshared keys as per the RFC 8784 in the IKEv2 to support post-quantum security.	
33	The solution must support high availability and load balancing between multiple ISPs, including VPN connections, Multi-Link VPN link aggregation, QoS-based link selection and admin should be able to manipulate the sensitivity of an application based on jitter, packet loss & latency.	
34	The solution must support configuration rollback feature to detect and recover from software and configuration errors by reverting back to previously active software or configuration.	
35	The Firewall appliance inspection engine must deliver more than 15000 fingerprint/vulnerabilities for detecting exploit attempts against known vulnerabilities in protocol specific tcp/upd port number. Solution must provide Multi-layer inspection to increase network security and performance and it should combine access control to define policies that govern your	

	user's access to network resources, deep inspection to detect advanced threats & file filtering to block malicious file transfers.	
36	The solution must support 4000+ ~~7000+~~ Applications for better control and visibility throughout the environment so that solution should be able to understand applications like 4sync, 4tube, bizible, facebook, youtube etc. Solution should support minimum of 10000 Inspection Signatures and should support QUIC & HTTP/3.	
37	The solution must support Full-Steam Deep Inspection, Anti-Evasion Defense, Dynamic Context Detection, Protocol-Specific Traffic Handling/Inspection, Granular Decryption of SSL/TLS Traffic, Vulnerability Exploit Detection, Custom Fingerprinting, Reconnaissance, Anti- Botnet, Correlation, Traffic Recording, DoS/DDoS Protection, Blocking Methods and Automatic Updates.	
38	The Firewall appliance Inspection Engine/ Anti-Bot must employ the below inspection technologies 1. Multilayer traffic normalization 2. Vulnerability-based fingerprints 3. Evasion and anomaly logging 4. Decryption-based detection 5. Message length sequence analysis	
39	The solution must support FTP and DNS Proxy to restrict the types of traffic and the commands that can be used with DNS and FTP connections. Solution must support DNS sink holing for UDP and TCP service.	
40	The solution must provide steering of applications dynamically & should provide application identification with link monitoring to effectively allocate networking resources, ensuring that the critical applications receive the necessary resources for optimal performance.	
41	The solution must have the technique for monitoring the application health and provide visibility into the organization's network traffic and the administrators should be able detect and resolve bottlenecks before they become a network-wide problem & should provide real- time visibility, historical views, and easy access to connectivity logs directly from the OEM Centralized management dashboard.	
42	The solution should have an option to create alternative policies if the connectivity between the NGFW and central Manager is lost, any policy should be allow to be selected whether it is a normal policy or one of the alternative policies	
43	The solution must prevent against the websites via URL filtering that mask their identity using Dynamic DNS services, Elevated exposure by website that camouflage their true nature, domian name that are registered recently, parked domain, Unauthorized Mobile Marketplaces to prevent users visiting the websites that may distribute applications unauthorized by the mobile OS manufacture	
44	The solution must have DNS sink holing for malicious DNS request from inside hosts to outside bad domains and blocks access to known malicious sites and non-existent IP addresses with ability to proactively measure against command and control (C2) access & second-stage malware downloads for disrupting the communication between infected endpoints and attackers	
45	The solution must provide visibility into application health history along with health status history of network applications.	

46	The solution must support custom script upload via Centralize manager so that same script can be used on multiple NGFW and it should support using FQDN to connect between the Firewall and management server & Log Server.	
47	The solution must support Multi-Layer Traffic Normalization/Full-Stream Deep Inspection, Anti-Evasion Defense, Dynamic Context Detection, Protocol-Specific Traffic Handling/Inspection, Granular Decryption of SSL/TLS Traffic (both TLS 1.2 and 1.3), Vulnerability Exploit Detection, Custom Fingerprinting, Reconnaissance, Anti- Botnet, Correlation, Traffic Recording, DoS/DDoS Protection, Blocking Methods, Automatic Updates	
48	The management platform must be a dedicated OEM appliance/software/vm running on server and should be capable of managing all the firewalls from day 1	
49	Solution must support File Filtering via Policy for multiple ~~minimum 200~~ file types in 15 categories and also support file Reputation checking & blocking for file with Malware reputation	
50	The solution should come with a web-based administration interface in the dedicated centralized manager and must be able to define the custom roles in addition to predefined roles (e.g., Owner, Viewer, Operator, Editor, Super User) to control permissions flexibly and accurately. Soultion must support Documented API enabling easy third-party product and service integration Using REST architecture where data can be XML or JSON coded.	
51	The Firewall appliance must have the ability to support high availability ~~of different model /appliances and versions within the same HA cluster negatively will be preferred.~~	
52	The NGFW should be proposed with all the subscription licenses for NGFW, NGIPS, Anti-Malware, URL Filtering, DNS sinkholing, DNS Proxy features as mentioned above from the date of Go-live.	
53	Solution should provide on Prem APT with Advanced threat protection capabilities for all the major Operating system like Windows, Linux, and Android & solution must deliver low level visibility to file execution activities by looking at custom OS Kernals	
54	Solution must have several static security scans including advanced signature analysis, post which files are detonated by to offer low level visibility to file, network and in memory operations of files as they execute and once the scan is completed, solution must provide a Threat Score and detailed File Threat Analysis, including a Mitre Attack matrix of the suspicious activity.	
55	Sandboxing scan must provide an advanced Threat report, including Mitre Attack insights for threat hunters, analysis of network vulnerabilities and security hardening and must support detection of zip bomb hidden threats and must we go down upto 4 or more~~8~~ layers when it comes to nested zips.	
56	Sandboxing solution must provide ability to detect and report on Ranswomware notes and must detect in memory operations for malicious behavior.	
57	The sandboxing solution must be able to analyze various threats, including malware, exploit kits, ransomware, and zero-day vulnerabilities and solution must be scalable to accommodate increasing threat analysis needs	
58	Solution must support for atleast 500 files per hours and solution must be scalable to process more files by increasing the compute, however no additional should be required.	

Note: Point 52 to 58 are applicable when firewall is connected to the Internet

Final models sized during procurement based on rulebase, throughput, and SSL policy (no SSL decryption assumed inside enclave)

2.5. CDTS Enclave (All CDTS SERVERS with Windows OS)

2.5.1. CDTS scanning servers: 2× 1U/2U x86 servers (12–16 cores, 64–128 GB RAM, 2×10/25 GbE), NVMe ≥ 3.84 TB

2.5.2. Roles: multi-AV, YARA, file hashing, staging to Harbor-Quarantine

2.5.3. CDTS management/ops server: 1× 1U x86 (8–12 cores, 64 GB RAM) for workflow/orchestration, dashboards, and audit log frontend

2.5.4. Sandbox VMs (on CDTS servers): Cuckoo with customer-provided Windows images (licences by customer)

2.5.5. Secure storage: Uses Harbor-Quarantine (on platform cluster) for large artefacts; CDTS local disk for transient staging

2.6. Time Time & DNS

2.6.1. GPS Stratum-1 NTP appliance, dual PSU, 1× GPS outdoor antenna with coax, lightning arrestor, and grounding kit

2.6.2. Mounting kit & cabling to DC rooftop or suitable GPS sky-view position

2.7. Workstations (GPU Workstation Qty- 35(5 for Bangalore) and Standard Workstations-70(15 for Banglalore) for End User Compute)

SNo	Category	Specification Item	OEM-Agnostic Requirement
1	General System	Purpose	High-performance workstation for professional use (CAD/CAM, content creation, data analysis, software dev, light simulation) with standard Monitor and Windows OS, Keyboard and Mouse
		Form Factor	Professional Tower or Small Form Factor (SFF) Workstation
2	Processor (CPU)	Model	Intel Core i9-or similar on benchmark test
		Cores / Threads	**GPU Workstations:-** ≥24 Cores **Standard Workstations**: ≥ 12 Core
		Base Clock (P-cores)	Minimum 2.0 GHz

		Max Turbo Frequency	Up to ~~5.8~~ 5.6 GHz or higher
		Intel Smart Cache	36 MB or higher
		Processor Base Power (TDP)	65W, with dynamic Max Turbo Power support
		Integrated Graphics	**GPU Workstations:-** RTX 4000 Ada (20–24 GB) ~~Or~~ and Intel UHD Graphics 770 (or equivalent integrated graphics) for Non GPU Workstations
3	System Memory (RAM)	Total Installed Capacity	**GPU Workstations:-** ≥64–128 GB RAM **Standard Workstations**: ≥ 32GB
		Configuration	≥2 DDR5 UDIMM Supported
		Speed	Minimum DDR5-5600 MHz
		Type	Non-ECC (Error-Correcting Code)
4	Storage	Primary Drive Type	NVMe (Non-Volatile Memory Express) SSD
		Primary Drive Capacity	**GPU Workstations:-** ≥ 1TB **Standard Workstations**: ≥ 512 GB
		Primary Drive Interface	PCIe Gen4 x4 (or Gen5 x4)
		Primary Drive Performance	Min. 5000 MB/s Sequential Read, Min. 4000 MB/s Sequential Write
		Storage Expansion Slots	Min. 1 additional M.2 NVMe slot (PCIe Gen4 or higher)
		Storage Expansion Bays	~~Min. 2 x 3.5-inch or 2.5-inch SATA drive bays~~ Min. 1 x 3.5-inch or 2.5-inch SATA drive bays
5	Operating System	Version	Microsoft Windows 11 Enterprise (64-bit) Or Microsoft Windows 11Pro (64-bit)
6	Network Connectivity	Wired Ethernet	Integrated 10/100/1000 Mbps Gigabit Ethernet (RJ-45)
		Wireless Connectivity	Wi-Fi 6E (802.11ax) with Bluetooth 5.2 or newer (Recommended)
7	Audio	Integrated Audio	High Definition Audio
8	I/O Ports	Front Ports	Min. 2 x USB 3.2 Gen 1 Type-A, 1 x USB 3.2 Gen 2 Type-C, Audio Combo Jack OR Front Ports: Min. 2 x USB 3.2 Gen 1/2 Type-A, 1 x USB 3.2 Gen 2 Type-C, Audio Combo Jack
		Rear Ports	Min. 4 x USB 3.2 Gen 1 Type-A, 2 x USB 2.0 Type-A, 1 x RJ-45 Ethernet, Audio Line-in/Line-out OR Rear Ports : Min. 4 x USB 3.2 Gen 1 Type-A/TypeC, 2 x USB 2.0 Type-A, 1 x RJ-45 Ethernet
9	Power Supply	Type	Internal, Auto-sensing
		Wattage	Sufficient wattage to power all components at full load, including future expansion.
10	Security Features	Trusted Platform Module	TPM 2.0 (Discrete TPM preferred)

		Secure Boot	UEFI Secure Boot enabled by default
		Chassis Intrusion	Chassis Intrusion Switch
		Physical Security	Kensington Lock Slot
		BIOS/UEFI Security	BIOS/UEFI Password Protection
11	Management Features	Remote Management	Standard desktop manageability features
12	Peripherals	Keyboard	Full-size USB Keyboard
		Mouse	USB Optical Mouse
13	Warranty & Support	Duration	3 Years Warranty and 3 years Support
14	Environmental & Physical	Operating Conditions	Operating Temperature: 10°C to 35°C, Humidity: 20% to 80% non-condensing
		Acoustics	Optimized for quiet operation in an office environment.

2.8. Conference Solutions

2.8.1. Camera Solution

Sno	Category	Specification Item	Required Specification
1	Video Capabilities (Camera)	Resolution	Full HD 1080p (1920 x 1080) at 30 frames per second (fps) or higher. With support for lower resolutions and standard resolutions
		Zoom Capability	Minimum 12x Optical Zoom (or equivalent lossless digital zoom with comparable quality at 12x).
		Pan/Tilt Range	Pan: Minimum ±170 degrees; Tilt: Minimum ±90 degrees.
		Field of View (FOV)	Diagonal Field of View (DFOV): Minimum 82 degrees.
		Autofocus	Fast and accurate autofocus.
		Exposure/White Balance	Automatic exposure and white balance control for various lighting conditions.
		Image Sensor	High-quality image sensor for clear video, even in low light conditions.
2	Audio Capabilities (Speakerphone/Microphone)	Microphone Array	Integrated microphone array with a minimum pickup range of 4.5 meters (15 feet).
		Speaker Output	Integrated speaker with clear audio output for spoken word.
		Full-Duplex Audio	Support for full-duplex audio communication.
		Echo Cancellation	Acoustic Echo Cancellation (AEC) to eliminate echo.
		Noise Reduction	Noise suppression technology to reduce background noise (e.g., keyboard clicks, HVAC sounds).
		Automatic Gain Control (AGC)	Automatic adjustment of microphone levels based on participant distance/volume.

3	Connectivity & Compatibility	Host Connectivity	Single USB 3.0 Type-B connection to host PC/laptop. Backward compatible with USB 2.0 (with potential feature limitations).
		Operating System Support	Compatible with Windows 10/11, macOS (latest versions), and Chrome OS.
		Platform Compatibility	Certified or fully compatible with leading UC platforms (e.g., Microsoft Teams, Zoom, Google Meet, Webex, Skype for Business).
		Physical Interface	RJ45 port for connecting camera to speakerphone (if separate units). Power connection.
4	Features & Control	Camera Presets	Minimum 10 programmable camera presets.
		Auto-Framing/Smart Speaker Tracking (Recommended)	Intelligent framing technology to automatically frame meeting participants or track the active speaker.
		Remote Control	Dedicated IR or RF remote control unit included.
		Management Software	Software utility for advanced configuration, firmware updates, diagnostics, and management from a host PC.
		Security Features	Privacy shutter or equivalent for camera. Firmware updates with security patches.
5	Physical & Environmental	Components	Consists of a PTZ camera unit and a separate speakerphone unit.
		Mounting Options	Camera should support wall mounting, ceiling mounting, and TV/monitor top mounting. Speakerphone to be tabletop.
		Cable Lengths	Sufficient cable length (e.g., 5-10 meters) for connecting camera to speakerphone, and speakerphone to host PC/power. Extendable options available.
		Power Supply	AC Power adapter included. Power over Ethernet (PoE) for camera (if applicable) is a plus.
		Operating Conditions	Operating Temperature: 0°C to 40°C. Operating Humidity: 20% to 80% (non-condensing).
6	Warranty & Support	Warranty	3 years hardware warranty and 3 years support.
		Technical Support	Access to technical support via phone, email, and web portal.

2.8.2. Display Solution for 75-Inch Conference Room Display (Only standard Brands like Sony, Samsung, LG, Panasonic to be provided)

Category	Specification Item	Required Specification	Notes / Considerations
1. Display Panel	Display Size	75 inches (diagonal).	Ideal for medium to large conference rooms to ensure visibility from all seating positions.

	Display Technology	Direct LED Backlit LCD Panel.	Ensures uniform brightness and color across the screen.
	Native Resolution	4K Ultra HD (UHD) - 3840 x 2160 pixels.	Provides exceptional detail and clarity for presentations, video conferencing, and multimedia content.
	Brightness	Minimum 350 cd/m^2 (nits) typical.	Sufficient for well-lit conference rooms without direct glare. Higher brightness is preferable for brighter environments.
	Refresh Rate	60Hz native.	Standard for smooth video playback and content display.
	Viewing Angle	178° (H) / 178° (V).	Ensures consistent image quality and color accuracy from wide viewing angles within the conference room.
	Panel Life	Rated for minimum 50,000 hours of typical operation.	Indicates long-term reliability for commercial use.
2. Connectivity	HDMI Inputs	Minimum 3 x HDMI 2.0 (or newer) ports.	For connecting various sources like laptops, video conferencing codecs, presentation systems. HDMI 2.1 is preferred for future-proofing where supported.
	USB Ports	Minimum 2 x USB Type-A ports (e.g., USB 2.0 or 3.0) for media playback, firmware updates, or peripheral connections.	For direct content display from USB drives or powering external accessories.
	Network Port	1 x RJ-45 Ethernet port for network connectivity (for smart features, digital signage, or remote management).	Essential for remote management, firmware updates, and integration into corporate networks. Wi-Fi (802.11ac/ax) is also highly desirable.
	Audio Outputs	1 x Digital Audio Output (Optical or HDMI ARC/eARC), 1 x 3.5mm Analog Audio Out.	For connecting to external sound systems or conference room audio solutions.
	Control Port	1 x RS-232C port (or equivalent for professional control systems like Crestron/Extron).	For integration with room control systems and automation.
3. Audio	Integrated Speakers	Minimum 2 x 10W (RMS) built-in speakers.	For basic audio playback. Integration with a dedicated conference room audio system is often preferred for optimal sound quality.
4. Smart & Professional Features	Operating System	Integrated Smart TV OS (e.g., proprietary OS from vendor) with app support.	Allows for direct app installation (e.g., video conferencing apps, content sharing apps) without requiring an external PC.
	Wireless Screen Sharing	Built-in wireless screen sharing capabilities (e.g., Miracast, Apple AirPlay 2, or proprietary solutions).	Enables convenient wireless content presentation from laptops, tablets, and smartphones.
	Digital Signage Capable	Support for digital signage functionality (e.g., scheduling content playback, remote content management).	Useful for displaying company announcements, schedules, or welcome messages when not in use for conferencing.
5. Physical & Mounting	Dimensions & Weight	Vendor to provide exact dimensions and weight.	For planning mounting solutions.

	VESA Compatibility	Standard VESA mounting pattern (e.g., 400x400mm or 600x400mm) for wall mounts or floor stands.	Ensures compatibility with a wide range of mounting solutions.
	Bezel Design	Slim bezel design for a sleek appearance and minimized distraction.	Modern aesthetic suitable for professional environments.
6. Power & Reliability	Power Supply	AC 100-240V, 50/60Hz.	Standard power input.
	Power Consumption	Energy Star certified; vendor to specify typical and maximum power consumption.	For energy efficiency and operational cost planning.
7. Warranty & Support	Commercial Warranty	Minimum 3-year commercial warranty.	Also Provide 3 years support
	Technical Support	Access to manufacturer's technical support for troubleshooting and assistance.	

2.9. PDUs

PDUs: 4× (A + B per rack), 32A/Three-phase or per site standard, mixed C13/C19 There are **four racks** for GPU servers with each rack having a fully **redundant power setup**. The "A + B" configuration refers to two separate, independent power feeds running into each rack. This ensures that if one power source or PDU fails (e.g., "A" side), the servers remain powered by the other source ("B" side), providing high availability and preventing downtime. The total quantity of PDUs required is 8 (4 racks x 2 PDUs/rack).

2.10. Media for Cold Export

Encrypted removable HDDs: 12× ≥ 12 TB (one per month) + 2× spare
Docking kit and tamper-evident seals; storage logbook for chain-of-custody

3. Governance [Deleted in Addendum 1]

PART- C: Bill of Quantity cum Price bid

1. Unpriced BID Compliance (Submit with technical Bid)

Tower	**Item**	**Qty**	**Compliance (Yes/No)**	**Proposed Make and Model**	**Reference to the Technical Proposal (Page #)**
GPU Compute	GPU server (2x56 cores @2.1 Ghz, 2048GB RAM, 8× H200 141 GB ; 2×200 GbE) or equivalent PCIe GPUs. **Form Factor:** The solution can be based on either: • **SXM5:** A high-density module with NVLink interconnect for maximum inter-GPU bandwidth. • **PCIe:** A standard PCIe Gen5 card with an NVLink bridge to support multi-GPU communication.	4			
Non GPU Servers	2x32 cores@2.1Ghz, 512 GB RAM, 20–24 TB raw per node (NVMe) or equivalent Configuration	8			
Virtualisation/Platform	VCF/vSAN ESA server (all-NVMe)	512 Cores			
Storage	100 TB at least 200 Gbps throughput with NVMe disks ~~(20% of100TB)~~ Low latency and Scalable	1			
Switching – Core	**DC leaf/L3 switch (upto 400G-capable)**	2			

Tower	Item	Qty	Compliance (Yes/No)	Proposed Make and Model	Reference to the Technical Proposal (Page #)
	High-Performance Leaf Switch (24 x 200G Downlinks; 400GbE Uplinks)				
Switching – Access (Enclave)	Access switch (48×1G; 10G uplinks)	2			
Switching – Access (Internet LAN)	Access switch (48×1G; 10G uplinks)	2			
Switching – Management/OOB	Management/OOB switch (48×1G)(Qty 2) Management/OOB Switch(16X1G)(Qty1)	2+1			
Firewalls – Perimeter	Secure Firewall (FTD) – HA pair	2 (1 HA pair)			
Firewalls – Intranet (ISFW)	Secure Firewall (FTD) – HA pair	2 (1 HA pair)			
CDTS Enclave	CDTS scanning server	2			
CDTS Enclave	CDTS management/ops server	1			
Time & DNS	GPS Stratum-1 NTP appliance (dual PSU)	1			
Time & DNS	GPS outdoor antenna + surge kit + cabling	1 lot			
End-User Compute	Internet GPU workstations (RTX 4000 or 770 class)	35			
End-User Compute	Enclave standard workstations	70			
Conference room Solutions	LED TV, Camera and audio (Speaker Microphone)	2 Set			
PDU for existing RACKs	**PDUs: 4×** (A + B per rack), 32A/Three-	4 racks			

Tower	Item	Qty	Compliance (Yes/No)	Proposed Make and Model	Reference to the Technical Proposal (Page #)
	phase or per site standard, mixed C13/C19				
Media for Cold Export	Encrypted removable HDDs (≥ 4TB)	12/yr + 2 spares			
Optics/Cabling	QSFP56 200G modules/DACs, QSFP-DD 400G leaf optics, SFP+/SFP28 where needed, OM4/OS2 fibre, Cat6A copper	As per detail			
Software/Subscriptions	VMware VCF licences (8 nodes), Cisco FTD licences (Perimeter + ISFW), support	As per detail			
Services	Build & integration WPs, training, hypercare	1 lot			
O&M	Resident Engineers (8×5 and 24×7 options)	As per model			
Spares	Server/optics/NIC/PSU spares kit	2 lot			

Name: Place:

Designation: Date:

2. LIST OF ITEMS PROPOSED TO BE SUPPLIED WITH COSTING(Submit with Financial Bid)

2.1. DETAILS OF BILL OF MATERIAL HARDWARE. SOFTWARE AND OPERATIONS COST

Cat	SNo	Description	Item	Qty	UoM	Unit Price (INR, excl. Tax)	Total Price (INR, excl. Tax)
A	**Hardware**						
	1	GPU Compute	GPU server (2x56 cores @2.1 Ghz, 2048GB RAM, 8× H200 141 GB ; 2×200 GbE)	4	No		
	2	Non GPU Servers	2x32 cores@2.1Ghz, 512 GB RAM, 20-24 TB raw per node (NVMe)	8	No	1.	
	3	High-Performance Storage System (100 TB usable, ≥~~200~~ 160 Gbps throughput)					
B	**Networking**						
	4	Switching – Core	DC leaf/L3 switch (upto 400G-capable)	2	No		
	5	Switching – Access (Enclave)	Access switch (48×1G; 10G uplinks)	2	No		
	5	Switching – Access (Internet LAN)	Access switch (48×1G; 10G uplinks)	2	No		
	6	Switching – Management/OOB	Management/OOB switch (48×1G)	2	No		
	7	Switching – Management/OOB	Management/OOB switch (16×1G)	1	No		
	8	Firewalls – Perimeter Internet LAN	Secure Firewall (FTD) – HA pair	2 (1 HA pair)	Pair		

		Firewalls – Intranet (ISFW)	Secure Firewall (FTD) – HA pair	2 (1 HA pair)	Pair		
C	**Platform & End-User Hardware**						
	9	CDTS Enclave	CDTS scanning server	2	No		
	10	CDTS Enclave	CDTS management/ops server	1	2		
	11	Time & DNS	GPS Stratum-1 NTP appliance (dual PSU)	1	Lot		
	12	Time & DNS	GPS outdoor antenna + surge kit + cabling	1	Lot		
	13	End-User Compute	Internet GPU workstations (RTX 4000 or 770 class)	35	No		
	14	End-User Compute	Enclave standard workstations	70	No		
	15	Conference room	LED TV, Camera and audio (Speaker Microphone)	2 each	Set		
	16	Media for Cold Export	Encrypted removable HDDs (≥ 4 TB)	14	No		
	17	Optics/Cabling	QSFP56 200G modules/DACs, QSFP-DD 400G leaf optics, SFP+/SFP28 where needed, OM4/OS2 fibre, Cat6A copper	As per detail	Lot		
E	**Software and subscriptions**						
	18	Software/Subscriptions	VMware VCF Licences for 8 Nodes (512 Cores) with Support	1	Lot		
	19		Perimeter Firewall Subscriptions (Threat/IPS,	1	Lot		

			URL Filtering, DNS Security) with Support ISFW Firewall Subscriptions (Threat/IPS) with Support				
	20	Services	Build & integration WPs, training, hypercare	1	Lot		
	21	O&M	Resident Engineers (8×5 and 24×7 options)	1	Lot		
	22	Spares	Server/optics/NIC/PSU spares kit	1	Lot		
F	**Data Center Infrastructure**						
	23	PDUs	PDUs for 4 Racks (A+B Feeds, 32A/Three-phase)	8	No		
Other items $$							
	24						
	25						

NOTE: SI needs to cater for NW wiring and connectors for the Nodes as per the building layout which would be a prefab shelter under construction.
$$ Add items if not in the above table

2.2. Operations & Maintenance (O&M) Section

This section should be priced based on the staffing model in Annexure N

SNo	O&M Role	FTE	Monthly Rate (INR, excl. Tax)	Total for 12 Months (INR, excl. Tax)	
1	DC RE (K8s/VCF generalist)	1			
2	Desktop RE	1			
3	SOC/NOC Analyst (business hours)	1			
4	Service Delivery Manager	0.5			
5	On-Call Specialists Support (24x7 Remote Assistance)	1	Lot		
	Sub-Total (B)			<Amount>	

Name: Place:

Designation: Date:

2.3. Summary of Price Bid(Submit with Price Bid)

Description	**Amount (INR, excl. Tax)**

Sub-Total - Hardware, Software & Services Etc	
Sub-Total - Operations & Maintenance	
Grand Total (A+B)	
Applicable GST (%)	
Total Project Cost (Including Tax)	

Name: Place:

Designation: Date: