INDIAN INSTITUTE OF TECHNOLOGY BOMBAY
MATERIALS MANAGEMENT DIVISION

PR NO.1000046017 **RFx No.6100002081**

Technical specifications (1 Unit Master Node, minimum 9 units of compute nodes, minimum 2 units of GPU nodes)

Sr. No.	Item	Description	Technical Compliance (YES / NO)	Additional Information (if any)
Master Node: 1 No				
1	Processor	The server must be a Dual Processor Machine based on Intel AMD Genoa Platform CPUs or substantially equivalent, configured with at least 2 x EPYC 16C with Minimum 3.0Ghz Base Clock, 64M Cache with PciE Gen 5 Architecture & Supporting DDR5 4800 MT/s Memory		
2	System Memory (RAM)	The proposed server must have 24 x DDR5 DIMM Slots appropriately to Provide 256 Memory per node using 32GB DDR 5 4800 MT/s DIMMs		
3	PCIe Slots	The proposed server platform must have a minimum of 3 x PCIe Gen4/5 slots		
4	Network Cards	The system must have Dedicated 1G Port for OOB Management & a minimum of 2 x 1G Ports for additional NW		
5	Internal Storage	The proposed system must be configured with 2 x 960GB SSD for All Nodes in RAID 1 (Hardware RAID) for OS Instance & Should have additional 8 x 3.84 TB SSD for Master Node configuration		
6	GPU Support	The offered Server Platform while configured without any GPUs, should be able to accommodate up to 2 x Single Width GPUs in future if needed.		
7	Firmware	Shall provide cryptographic signed firmware updates by Server OEM.		
8	Embedded Security Features	Shall provide FIPS 140-2, Common Criteria Certified EAL-2+, TPM 2.0 v3, NIST SP 800-193 ("Platform Firmware Resiliency") NIST SP 800-147B (“BIOS Protection Guidelines for Servers”) and NIST SP 800-155 (“BIOS Integrity Measurement Proposed Guidelines”)		
		Should be able to verify BIOS integrity and authenticity from malicious firmware and support automatic BIOS recovery if BIOS is corrupted		
		Should be able to create firmware and configuration baselines for compliance monitoring and enable automated updates on schedule (download of update packages and firmware should be free from any warranty/service contract obligations)		

		Shall provide dual Immutable Silicon Root of Trust to verify the integrity of BIOS and the BMC Firmware Image while booting to trusted OOB Management Platform and Secure OS respectively		
		Shall provide dynamic system lock down server to		
		prevent malicious attacks against embedded firmware and configuration drift in your data centre without need to reboot the server		
		Shall provide dynamic USB enable / disable ability without need to reboot the server.		
		Shall provide Chassis Intrusion detection even when no power is available		
9	Management Capabilities	Shall support Telemetry Streaming 150+ metrics for various use cases which includes but not limited to AHS Logs		
		Shall support Simple Certificate Enrollment Protocol (SCEP) to automate certificate enrollment & renewal.		
		BMC should support automatic backup system configuration settings (BIOS, iDRAC, NIC), Service Tag and other licensed data to the flash memory to restore from a prompt in case the motherboard needs to be replaced.		
		Should allow create custom reports for various metrics at a time for specific component monitoring and troubleshooting such as processor, memory, I/O, power, thermals, drives, GPU(s), SFP etc. and enable custom actions based on alerts.It should be of the same brand as of the server supplier		
		Should be able to manage at least 5000 devices offering a single point / console for the overall health and management. It should be enabled with Elastic search feature capable of accessing all information within the console		
		The Dashboard minimum should display a health summary of the following: • Server Profiles • Server Hardware • Appliance alerts		
		Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD.		
		The Server Management Software should be of the same brand as of the server supplier.		
		Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.		
		Solution should support deploy configuration templates to quickly make changes to groups of servers		
10	Power and Cooling requirements (Power Supply & Fans)	The system must be Configured with a minimum of 2 x 800/1100/1400 W Titanium Grade Hot Swap Power Supply Units in Redundant Mode with C13-14 connectors for PDU & Must be supplied with High performance Hot Swap fans installed on the rear of the system		
11	Rack space	Maximum 1U with Sliding Ready Rail		

12	OS	Open-Source Linux / Ubuntu Linux		
13	Industry Standard Compliance	UEFI Specification, v2.7 or above, SMBIOS Specification, v3.3.0 or above, ACPI Specification, v6.4 or above, PMBus Specification, v1.2 or above, NVMe Express Base Specification, v2.0c or above, USB SuperSpeed v3.0,		
		Redfish API, Advanced Encryption Standard (AES), SNMP v3, TLS 1.3 or above, DMTF Systems Management Architecture for Server Hardware Command Line Protocol (SMASH CLP), Active Directory v1.0 and ASHRAE A3/A4		
		Manufactured with quality standards ISO 9001:2015, Compliance to Safety of IT Equipment : IEC 62368, Standards for EMC (Electro Magnetic Compatibility) : EN 55035 Class A and RoHS: EN IEC 63000 and ENERGY: Commission Regulation (EU) No. 2019/424 or substantially equivalent standards		
14	Provisioning and Automation Support	Should support automation using Ansible Modules, RESTful API Redfish, Standards APIs (Python, PowerShell), RACADM Command Line Interface (CLI) and GitHub Scripting Libraries, Provision one to many servers using own scripts to discover and deploy with Linux or Windows Scripting Tools.		
15	Cloud Enabled Monitoring and Analytics	1. Secure connection from customer sites to cloud service 2. Unified Identity & Access Management 3. Manages and controls servers regardless of physical location 4. Subscription-based entitlement 5. Efficient Device Onboarding 6. Firmware Update Awareness with Intelligent delta-only based updates 7. Set Group firmware Baseline and Compliance monitoring and notification 8. Group based firmware management that can be scheduled or on-demand 9. Remote Site management with low bandwidth/high latency network connectivity 10. Role-based access and views for managed customer environments 11. GUI and Rest APIs for core features		
Compute Node: Minimum 9 units				
Sr. No.	**Item**	**Description**	**Technical Compli-ance (YES / NO)**	**Addition-al Infor-mation (if any)**
1	Processor	The server must be a Dual Processor Machine based on Intel AMD Genoa Platform CPUs or substantially equivalent, configured with at least 2 x EPYC 48C with Minimum 2.75Ghz Base Clock, 256M Cache with PciE Gen 5 Architecture & Supporting DDR5 4800 MT/s Memory		
2	System Memory (RAM)	The proposed server must have 24 x DDR5 DIMM Slots appropriately to Provide 384 Memory per node using 32GB DDR 5 4800 MT/s DIMMs		

3	PCIe Slots	The proposed server platform must have a minimum of 3 x PCIe Gen4/5 slots		
4	Network Cards	The system must have Dedicated 1G Port for OOB Management & a minimum of 2 x 1G Ports for additional NW		
5	Internal Storage	The proposed system must be configured with 960GB SSD for All Nodes in RAID 1 (Hardware RAID) for OS		
		Instance		
6	GPU Support	The offered server platform while configured without any GPUs, should be able to accommodate upto 2 x Single Width GPUs in future if needed		
7	Firmware	Shall provide cryptographic signed firmware updates by Server OEM.		
8	Embedded Security Features	Shall provide FIPS 140-2, Common Criteria Certified EAL-2+, TPM 2.0 v3, NIST SP 800-193 ("Platform Firmware Resiliency") NIST SP 800-147B (“BIOS Protection Guidelines for Servers”) and NIST SP 800-155 (“BIOS Integrity Measurement Proposed Guidelines”)		
		Should be able to verify BIOS integrity and authenticity from malicious firmware and support automatic BIOS recovery if BIOS is corrupted		
		Should be able to create firmware and configuration baselines for compliance monitoring and enable automated updates on schedule (download of update packages and firmware should be free from any warranty/service contract obligations)		
		Shall provide dual Immutable Silicon Root of Trust to verify the integrity of BIOS and the BMC Firmware Image while booting to trusted OOB Management Platform and Secure OS respectively		
		Shall provide dynamic system lock down server to prevent malicious attacks against embedded firmware and configuration drift in your data centre without need to reboot the server		
		Shall provide dynamic USB enable / disable ability without need to reboot the server.		
		Shall provide Chassis Intrusion detection even when no power is available		
9	Management Capabilities	Shall support Telemetry Streaming 150+ metrics for various use cases which includes but not limited to AHS Logs		
		Shall support Simple Certificate Enrollment Protocol (SCEP) to automate certificate enrollment & renewal.		
		BMC should support automatic backup system configuration settings (BIOS, iDRAC, NIC), Service Tag and other licensed data to the flash memory to restore from a prompt in case the motherboard needs to be replaced.		
		Should allow create custom reports for various metrics at a time for specific component monitoring and troubleshooting such as processor, memory, I/O, power, thermals, drives, GPU(s), SFP etc. and enable custom actions based on alerts. It should be of the same brand as of the server supplier		

		The Dashboard minimum should display a health summary of the following: • Server Profiles • Server Hardware • Appliance alerts		
		Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD.		
		The Server Management Software should be of the same brand as of the server supplier.		
		Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.		
		Solution should support deploy configuration templates to quickly make changes to groups of servers		
10	Power and Cooling requirements (Power Supply & Fans)	The System must be Configured with a minimum of 2 x 800/1100/1400 W Titanium Grade Hot Swap Power Supply Units in Redundant Mode with C13-14 connectors for PDU & Must be supplied with High performance Hot Swap fans installed on the rear of the system		
11	Rack space	Maximum 1U with Sliding Ready Rail		
12	OS	Open-Source Linux / Ubuntu Linux		
13	Industry Standard Compliance	UEFI Specification, v2.7 or above, SMBIOS Specification, v3.3.0 or above, ACPI Specification, v6.4 or above, PMBus Specification, v1.2 or above, NVMe Express Base Specification, v2.0c or above, USB SuperSpeed v3.0, Redfish API, Advanced Encryption Standard (AES), SNMP v3, TLS 1.3 or above, DMTF Systems Management Architecture for Server Hardware Command Line Protocol (SMASH CLP), Active Directory v1.0 and ASHRAE A3/A4		
		Manufactured with quality standards ISO 9001:2015, Compliance to Safety of IT Equipment: IEC 62368, Standards for EMC (Electro Magnetic Compatibility) : EN 55035 Class A and RoHS: EN IEC 63000 and ENERGY: Commission Regulation (EU) No. 2019/424 or substantially equivalent standards		
14	Provisioning and Automation Support	Should support automation using Ansible Modules, RESTful API Redfish, Standards APIs (Python, PowerShell), RACADM Command Line Interface (CLI) and GitHub Scripting Libraries, Provision one to many servers using own scripts to discover and deploy with Linux or Windows Scripting Tools.		

15	Cloud Enabled Monitoring and Analytics	1. Secure connection from customer sites to cloud service 2. Unified Identity & Access Management 3. Manages and controls servers regardless of physical location 4. Subscription-based entitlement 5. Efficient Device Onboarding 6. Firmware Update Awareness with Intelligent delta-only based updates 7. Set Group firmware Baseline and Compliance monitoring and notification 8. Group based firmware management that can be scheduled or on-demand 9. Remote Site management with low bandwidth/high latency network connectivity 10. Role-based access and views for managed customer environments 11. GUI and Rest APIs for core features		
GPU Node: Minimum 2 units				
Sr. No.	**Item**	**Description**	**Technical Compli-ance (YES / NO)**	**Addition-al Infor-mation (if any)**
1	Processor	The server must be a Dual Processor Machine based on Intel AMD Genoa Platform CPUs or substantially equivalent, configured with at least 2 x EPYC 48C with Minimum 2.75Ghz Base Clock, 256M Cache with PciE Gen 5 Architecture & Supporting DDR5 4800 MT/s Memory		
2	System Memory (RAM)	The proposed server must have 24 x DDR5 DIMM Slots appropriately to Provide 256 Memory per node using 32GB DDR 5 4800 MT/s DIMMs		
3	PCIe Slots	The proposed server platform must have a minimum of 3 x PCIe Gen4/5 slots		
4	Network Cards	The system must have dedicated 1G Port for OOB Management & a minimum of 2 x 1G Ports for additional NW		
5	Internal Storage	The proposed system must be configured with 2 x 960GB SSD for All Nodes in RAID 1 (Hardware RAID) for OS Instance		
6	GPU Support	The offered server platform while configured 2 (or more) x NVIDIA L40S, PCIe, 350W, 48GB Passive, Double Wide, Full Height GPU		
7	DPU Support & Certification	The proposed server platform must be compliant & certified for NVIDIA Bluefield DPUs for future scalability as and when needed		
		Shall provide cryptographic signed firmware updates by Server OEM.		
8	Embedded Security Features	Shall provide FIPS 140-2, Common Criteria Certified EAL-2+, TPM 2.0 v3, NIST SP 800-193 ("Platform Firmware Resiliency") NIST SP 800-147B (“BIOS Protection Guidelines for Servers”) and NIST SP 800-155 (“BIOS Integrity Measurement Proposed Guidelines”)		

		Should be able to verify BIOS integrity and authenticity from malicious firmware and support automatic BIOS recovery if BIOS is corrupted		
		Should be able to create firmware and configuration baselines for compliance monitoring and enable automated updates on schedule (download of update packages and firmware should be free from any warranty/service contract obligations)		
		Shall provide dual Immutable Silicon Root of Trust to verify the integrity of BIOS and the BMC Firmware Image while booting to trusted OOB Management Platform and Secure OS respectively		
		Shall provide dynamic system lock down server to prevent malicious attacks against embedded firmware and configuration drift in your datacentre without need to reboot the server		
		Shall provide dynamic USB enable / disable ability without need to reboot the server.		
		Shall provide Chassis Intrusion detection even when no power is available		
9	Management	Shall support Telemetry Streaming 150+ metrics for		
	Capabilities	various use cases which includes but not limited to AHS Logs		
		Shall support Simple Certificate Enrollment Protocol (SCEP) to automate certificate enrollment & renewal.		
		BMC should support automatic backup system configuration settings (BIOS, iDRAC, NIC), Service Tag and other licensed data to the flash memory to restore from a prompt in case the motherboard needs to be replaced.		
		Should allow create custom reports for various metrics at a time for specific component monitoring and troubleshooting such as processor, memory, I/O, power, thermals, drives, GPU(s), SFP etc. and enable custom actions based on alerts.It should be of the same brand as of the server supplier		
		Should be able to manage at least 5000 devices offering a single point / console for the overall health and management. It should be enabled with Elastic search feature capable of accessing all information within the console		
		The Dashboard minimum should display a health summary of the following: • Server Profiles • Server Hardware • Appliance alerts		
		Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD.		
		The Server Management Software should be of the same brand as of the server supplier.		
		Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.		

		Solution should support deploy configuration templates to quickly make changes to groups of servers		
10	Power and Cooling requirements (Power Supply & Fans)	The system must be Configured with a minimum of 2 x 800/1100/1400 W Titanium Grade Hot Swap Power Supply Units in Redundant Mode with C13-14 connectors for PDU & Must be supplied with High performance Hot Swap fans installed on the rear of the system		
11	Rack space	Maximum 1U with Sliding Ready Rail		
12	OS	Open-Source Linux / Ubuntu Linux		
13	Industry Standard Compliance	UEFI Specification, v2.7 or above, SMBIOS Specification, v3.3.0 or above, ACPI Specification, v6.4 or above, PMBus Specification, v1.2 or above, NVMe Express Base Specification, v2.0c or above, USB SuperSpeed v3.0, Redfish API, Advanced Encryption Standard (AES), SNMP v3, TLS 1.3 or above, DMTF Systems Management Architecture for Server Hardware Command Line Protocol (SMASH CLP), Active Directory v1.0 and ASHRAE A3/A4		
		Manufactured with quality standards ISO 9001:2015, Compliance to Safety of IT Equipment: IEC 62368, Standards for EMC (Electro Magnetic Compatibility) : EN 55035 Class A and RoHS: EN IEC 63000 and ENERGY: Commission Regulation (EU) No. 2019/424 or substantially equivalent standards		
14	Provisioning and Automation Support	Should support automation using Ansible Modules, RESTful API Redfish, Standards APIs (Python, PowerShell), RACADM Command Line Interface (CLI) and GitHub Scripting Libraries, Provision one to many servers using own scripts to discover and deploy with Linux or Windows Scripting Tools.		
15	Cloud Enabled Monitoring and Analytics	1. Secure connection from customer sites to cloud service 2. Unified Identity & Access Management 3. Manages and controls servers regardless of physical location 4. Subscription-based entitlement 5. Efficient Device Onboarding 6. Firmware Update Awareness with Intelligent delta-only based updates 7. Set Group firmware Baseline and Compliance monitoring and notification 8. Group based firmware management that can be scheduled or on-demand 9. Remote Site management with low bandwidth/high latency network connectivity 10. Role-based access and views for managed customer environments 11. GUI and Rest APIs for core features		

Interconnect Ethernet Switch	24 Port 1G Ethernet Switch with Required Number of Ethernet Cables to connect All Master Node and Compute Node.
42 Rack	42 Server Rack with Standard Accessories and Two PDU's
UPS	20KVA UPS with 30 Minutes backup

Eligibility Criteria				
Sr No	**Particulars**	**Suggested supporting document**	**Technical Compli-ance (YES / NO)**	**Addi-tional Infor-mation (if any)**
1	Participating OEM must be the Manufacturer of and be capable of providing End to End Hardware Stack proposed as a part of the RFP Including Servers, Storage & Networking and would be a Single point of contact for Directly owning the Warranty of the Proposed Infrastructure and any Technical Support Incidents for the Product Lifecycle: The Warranty provided for the Entire Hardware component will be directly owned by the OEM, visible on their website tagged to the serial number of the provided Hardware : Any Software Package, 3rd Party Components Provided as a part of the Stack must be through the OEM's Engagement Channel fully	The OEM should submit a self- declaration with all the details mentioned on the company letterhead		
	supported with a Collaborative Support in conjunction with the OEM's existing relationship with Software Vendor. The Responsibility of Support for the Complete Stack will lie with a Single OEM.			
2	The OEM/Bidder should have local support engineers in the same Region for faster response. These engineers should be technically qualified and capable to handle the installation of various HPC Cluster & Software	Submit the escalation matrix with engineer details		
3	MAF from the Interconnect OEM as well as the server OEM with Tender number	Valid documents need to be submitted.		
4	The Bidders should have done the installations of minimum 3 similar in other Academic Institutes / R&D or other Government Organizations.	Purchase order copy with Installation report need to submit		
5	Compute node OEM must have minimum 2 entries in latest list (January 2025) of India Top Supercomputer (https://topsc.cdacb.in/) print of the list showing the system supplied by the OEM marked should be submitted with the technical bid.	List on https://topsc.cdacb.in/		
6	The OEMs of quoted products should have their own corporate office or spare parts warehouse and service centre or RMA depot in MMR with fully qualified engineers	Any government authorized document in support or the OEM website URLs where this information is published or a self-declaration with all the details mentioned on the company letterhead		

7	The OEM should be well equipped and located to honor 4 hours of response time in case of failures.	The OEM should submit a self- declaration with all the details mentioned on the company letterhead		
8	The OEM should be well established at least for last 10+ years in enterprise servers, Storage & Networking	Any government authorized document which will prove the establishment of OEM/Brand and or copy of PO needs to be attached.		
9	The OEM should have a direct presence in India at least for the last 10 years	Any government authorized document which will prove the establishment of OEM/Brand and or copy of PO needs to be attached.		
10	The OEM should have their own 24x7 technical support center in India (presence in MMR preferred) and the technical support resources should be on direct payrolls with the OEM.	Any government authorized document in support of this or the OEM website URLs where this information is		
		published or a self-declaration with all the details mentioned on the company's letterhead.		
11	The OEM should not be from a country that shares a land border with India.	Self-declaration should be given on company's letterhead		
12	The OEM should not be blacklisted by any of the following entities: Any department of IIT Bombay, any other IITs, any state or central government body or organization, any autonomous body governed by state or central government, in Government E-Marketing portal (GeM) in the past 5 years w.r.t the tender date. Self-declaration should be given on companies Letterhead.	Self-declaration should be given on companies letterhead		