Foundation for Innovation and Technology Transfer (FITT)
Indian Institute of Technology Delhi, Hauz Khas, New Delhi-110016

Ref.: FT/NCIIPC/EOI/2025-2026
Date: 22nd July 2025

EOI AMENDMENTS: FINALIZED POST PRE-BID QUERY MEETING HELD ON 18 Jul 2025 from 1400-1730 Hrs

1. Please refer to EOI tender Reference IITD/FT/EOI/2025-26 and Tender ID 2025_IIT_868121_1 dated 09 Jul 2025.
2. The Pre bid queries were received from vendors by 18 July 2025 and a draft response of the proposed changes based on the suggestions and inputs received from the vendors was circulated via email on 17th July 2025 to ensure transparency and to facilitate focused discussion during the session.
3. During the meeting, the Committee and other attending members deliberated upon the queries raised by the participating vendors. Clarifications were provided in detail with respect to the scope of work, technical specifications, eligibility criteria, and documentation requirements as outlined in the original EOI. The final compilation of queries, amendments, and corresponding clarifications as discussed and agreed during the meeting has been enclosed as Annexure "A" for reference.
4. In addition to the above, several vendors requested an extension of the EOI submission deadline, citing limited time post-clarification for preparation of their respective responses. In view of the above the EOI submission deadline has been extended up to **28th July 2025, 11:00 hrs (by e-mail).**
5. Also, the following is reiterated for clarity: -
    a. Should a minor deviation in specifications render an Original Equipment Manufacturer (OEM) ineligible to propose a product for supply via the System Integrator (SI), the SI is requested to provide a detailed reason/justification along with their proposed alternative. This proposal will be subject to evaluation during the Expression of Interest (EOI) process.
    b. All supplied licenses must be explicitly bound to the end-user.
    c. Should equipment supplied post-RFP fail to meet the benchmark stipulated requirements/specifications, the bidder shall be obligated to provide a solution or hardware that fully conforms to the final RFP document's specifications/benchmark.
    d. Also, the SI should clearly give the following details: -
        i. The specifications for the PDUs required for supply and installation in the existing data centre racks to meet the power demands of the GPU servers along with estimated cost.
        ii. Confirmation that all equipment supplied as part of this project is fully enabled for seamless connectivity to the existing data centre network.
6. All clauses not explicitly addressed in this document remain unchanged.
7. Vendors would be asked to present there solutions in the week 29th Jul 2025 to 01st Aug 2025.
8. The amended clauses are attached as Annexure 'A' (27 Pages)

Col Naveen Gopal
Project Head

Additional Queries

Pg. No.	**Reference For EOI**	**Amended Clauses (For)**	**Final Amended Clauses**
101	Annexure V	Please affix the signature of the authorized signatory of the statutory auditor/**CA** of the Bidder with name, designation, seal, and date here. The Annexure V can be on a suitable letter head stamps of CA and Company Authorised signatory	Please affix the signature of the authorized signatory of the statutory auditor/**CA** of the Bidder with name, designation, seal, and date here. The Annexure V can be on a suitable letter head stamps of CA and Company Authorised signatory
86	Annexure V	60 X 48 U Racks (40 racks are available)The details are 42U/800 mm Width X 1200 mm Depth, PLN and AP8853	61 X 48 U Racks (40 racks are available)The details are 42U/800 mm Width X 1200 mm Depth, PLN and AP8853
7	Chapter 1 Clause no 14	14.Software: All software required to be supplied should be preferably Open source (With Enterprise support Management EOM) and in case of any proprietary software being recommended the SI should justify the same. Also in case of Proprietary software the number of licenses has to be clearly mentioned along with the justification	14.Software: All software required to be supplied should be preferably Open source (With Enterprise support Management EOM) and in case of any proprietary software being recommended the SI should justify the same. Also in case of Proprietary software the number of licenses has to be clearly mentioned along with the justification
10	Chapter 2 Misc Nodes Clause D	d) Database Servers The Database Server should serve as the central repository and management system for all data that drives AI research, development, and deployment. While GPU servers perform the computations and application servers provide interfaces, the database server ensures that the "fuel" for AI—data—is organized, accessible, reliable, and secure. Types of databases envisaged to be used are:- i) Relational Databases (e.g., PostgreSQL, MySQL, SQL Server ii) NoSQL Databases (e.g., MongoDB, Cassandra, Redis, Elastic Search). iii) Vector Databases (e.g., Pinecone, Milvus, Qdrant, or databases with vector capabilities like PostgreSQL with pgvector, Elastic Search) iv) Server should support below controllers, must support Mixed Mode which combines RAID and HBA mode operation simultaneously	d) Database Servers : The Database Server should serve as the central repository and management system for all data that drives AI research, development, and deployment. While GPU servers perform the computations and application servers provide interfaces, the database server ensures that the "fuel" for AI—data—is organized, accessible, reliable, and secure. Types of databases envisaged to be used are:- i) Relational Databases (e.g., PostgreSQL, MySQL, SQL Server ii) NoSQL Databases (e.g., MongoDB, Cassandra, Redis, Elastic Search). iii) Vector Databases (e.g., Pinecone, Milvus, Qdrant, or databases with vector capabilities like PostgreSQL with pgvector, Elastic Search) iv) Server should support below controllers, must support Mixed Mode which combines RAID and HBA mode operation simultaneously
69	Chapter 3 Display Solution for 75-Inch Conference Room Display Clause 4	Built-in wireless screen sharing capabilities .	Built-in wireless screen sharing capabilities .
84	Chapter 4 16 Eligibility Criteria; Clause No-vi	Prospective bidders must possess demonstrated expertise in the delivery and seamless integration of the required equipment, extending beyond mere supply.as part of the datacenter creation/operations: 1. Creation of datacentre 2. storage, compute 3. NW security	Prospective bidders must possess demonstrated expertise in the delivery and seamless integration of the required equipment, extending beyond mere supply.as part of the datacenter creation/operations: 1. Creation of datacentre 2. storage, compute 3. NW security

6	Chapter 1 About the project	Since this procurement is covered under 3(b) of Ministry of Commerce and Industry (DPIIT) Order No. P-45021/2/2017-PP(BE-II) dated 04-06-2020 on Public Procurement (Preference to Make in India), only Class-I & Class-II Local Suppliers, as defined in the order are eligible to participate in this tender. (Calculated on the total cost of the Tender)	Since this procurement is covered under 3(b) of Ministry of Commerce and Industry (DPIIT) Order No. P-45021/2/2017-PP(BE-II) dated 04-06-2020 on Public Procurement (Preference to Make in India), only Class-I & Class-II Local Suppliers, as defined in the order are eligible to participate in this tender. (Calculated on the total cost of the Tender)
6	Chapter 1 Scope of project	Establishment of a secure 1 Gbps leased line between Mayur Vihar and Ayanagar locations for communication between the LAN established at Mayur Vihar and server room infrastructure at Ayanagar, in case the Office Infrastructure is established at Mayur Vihar. The IP Encryption Units for securing the link will be provisioned and deployed by NCIIPC. The SI would be given the dark fibre and SI would need to Install and commission and deploy the terminal equipment and activate the dark Fiber provided by FITT IIT Delhi(BILLING TO HAPPEN DIRECTLY BY ISP TO END USER)	Establishment of a secure 1 Gbps leased line between Mayur Vihar and Ayanagar locations for communication between the LAN established at Mayur Vihar and server room infrastructure at Ayanagar, in case the Office Infrastructure is established at Mayur Vihar. The IP Encryption Units for securing the link will be provisioned and deployed by NCIIPC. The SI would be given the dark fibre and SI would need to Install and commission and deploy the terminal equipment and activate the dark Fiber provided by FITT IIT Delhi(BILLING TO HAPPEN DIRECTLY BY ISP TO END USER)
6	Chapter 1 12. Scope of Work Clause d Point -i	i) Ten workstations for connection with internal/Internal network (Internal is airgapped NW and External is with Internet)	i) Ten workstations for connection with internal/Internal network (Internal is airgapped NW and External is with Internet)
12	Chapter 2 Point 10 c	NW Switch (Qty 2) The data centre requires 1G/10G or 40/100G bandwidth to connect a diverse set of nodes like GPU servers, inference servers, storage control nodes, and management nodes.	NW Switch (Qty 2) The data centre requires 1G/10G or 40/100G bandwidth to connect a diverse set of nodes like GPU servers, inference servers, storage control nodes, and management nodes.
	12. (c)	Establishment of a secure 1 Gbps leased line between Mayur Vihar and Ayanagar locations for communication between the LAN established at Mayur Vihar and server room infrastructure at Ayanagar. Dark fiber not in scope of bidder	Establishment of a secure 1 Gbps leased line between Mayur Vihar and Ayanagar locations for communication between the LAN established at Mayur Vihar and server room infrastructure at Ayanagar. Dark fiber not in scope of bidder
	13. Warranty & Support	All hardware components proposed and supplied in response to this Expression of Interest (EoI) must be covered by a three (3) year manufacturer's warranty. This warranty shall commence from the date of final acceptance of the hardware. Additionally, three (3) years of End-of-Service (EOS) support must be provided post the end of warranty period. OEM needs to provide declaration for End of Service support for 3 years after warranty period.	All hardware components proposed and supplied in response to this Expression of Interest (EoI) must be covered by a three (3) year manufacturer's warranty. This warranty shall commence from the date of final acceptance of the hardware. Additionally, three (3) years of End-of-Service (EOS) support must be provided post the end of warranty period. OEM needs to provide declaration for End of Service support for 3 years after warranty period.

Chaper 1 (GPU Server)			
Sl NO	**Components**	**Specifications Published EOI 09.07.2025**	**Additional Points**
		8 x Dual Port InfiniBand NDR200 Adapter	**8 x Single Port InfiniBand NDR Adapter**
		2 x Dual Port InfiniBand NDR200 Adapter for storage interconnect	**2 x Single Port InfiniBand NDR Adapter**
10	Multi Instance GPU	Single GPU can be partitioned into as many as 7 GPU instances. Required software license for GPU partitioning to be provided from day1.	Single GPU can be partitioned into as many as 7 GPU instances. Required software license for GPU partitioning to be provided from day1. Virtualization required for control/ management nodes
11	Power Supply	6x 2800-Watt capacity per server system providing N+2 redundant hot-swap Power Supplies	N+N redundant hot-swap Power Supplies to meet the peak load power requirements
		Quoted OS should be under enterprise support from the OEM.	Quoted OS should be under enterprise support from the OEM / supported by bidder
18	Form Factor	6U rack mountable or lower	Deleted
19	Warranty		Warranty GPU hardware support for 3 Years & for Software 3 years warranty +3 years support.

Chapter -2 Inference Node Server		
Item	**Specifications Published EOI 09.07.2025**	**Final Amended Clauses**
Chassis	2U Rack Mountable	
CPU	Min Two or more x86 Architecture based server Processors*, Each CPU with at least 36/48 Cores,2.1GHz Base or higher with 105MB Cache or more.	Min Two or more x86 Architecture based server Processors*, Each CPU with at least 32 cores,2.1GHz Base or higher with 60 MB Cache or more.
Memory	32DIMM slots Server should be configured with 512GB RAM - scalable upto 8.0 TB using DDR5 Registered DIMM (RDIMM) operating at 4800 MT/s	24 DIMM slots or more Server should be configured with 256GB RAM or more- scalable upto 6.0 TB using DDR5 Registered DIMM (RDIMM) operating at 4800 or more.
Bus Slots	Server should support upto four PCI-Express Slots 4.0 slots or higher or mix of Additional two x8 or higher OCP 3.0 slots	Server should support upto four PCI-Express Slots 4.0/5.0 X16 slots (Can be a mix of 4.0 or 5.0 OR only 5.0) Additional one x8 or higher OCP 3.0 slots
Controller	Server should support below controllers, must support Mixed Mode which combines RAID and HBA mode operation simultaneously :Embedded / PCIe based x16 RAID controller with 8GB 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. 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	Server should support below controllers, must support Mixed Mode which combines RAID and HBA mode operation simultaneously :Embedded / PCIe based x16 RAID controller with 8GB Flash backed write cache, supporting RAID 0, 1, 5, 6, 10, 50, 60.Must support mix-and-match SAS, SATA , SSD and NVMe drives to the same controller. Controller must support 6G SATA, 12G SAS, 16G NVMe, SSD Above mentioned controller must support following or equivalent certifications: 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	Server should be populated with below networking cards: Broadcom BCM57412 Ethernet 10Gb 2-port SFP+ Adapter Broadcom BCM5719 Ethernet 1Gb 4-port BASE-T OCP3 Adapter 2 nos. of dual port InfiniBand NDR200 in redundancy	Server should be populated with below networking cards:"Serial - 1 (Optional) 1GbE Dedicated management port" Ethernet 10Gb 2-port SFP+ Adapter Ethernet 1Gb 4-port BASE-T OCP3 Adapter 2 nos. of single port InfiniBand NDR200/Ethernet 200Gig in redundancy Should support hot plug redundant power supplies with minimum platinum grade
Interfaces	Serial - 1 (Optional) USB support with Up to 5 total: 1 front, 2 rear, 2 internal. 1GbE Dedicated management port	Serial - 1 (Optional) USB support with Up to 3 total or more ports 1GbE Dedicated management port
Power Supply	Should support hot plug redundant low halogen power supplies with minimum 94% efficiency	Should support hot plug N+N redundant power supplies
Industry Standard Compliance	ACPI 6.3 Compliant PCIe 5.0 Compliant WOL Support Microsoft® Logo certifications PXE Support Energy Star SMBIOS 3.2 UEFI 2.7 Redfish API IPMI 2.0 Secure Digital 4.0 Advanced Encryption Standard (AES) SNMP v3 TLS 1.2 DMTF Systems Management Architecture for Server Hardware Command Line Protocol (SMASH CLP) Active Directory v1.0	ACPI 6.3 Compliant PCIe 5.0 Compliant WOL Support Microsoft® Logo certifications PXE Support Energy Star SMBIOS 3.2 UEFI 2.7 Redfish API IPMI 2.0 Secure Digital 4.0 Advanced Encryption Standard (AES) SNMP v3 TLS 1.2 Line Protocol (SMASH CLP) Active Directory v1.0 ASHRAE A3/A4 OR **Equivalent or better certifications**
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) 1.2 option 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	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) 1.2 option TPM (Trusted Platform Module) 2.0 option Advanced Encryption Standard (AES) on browser 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 OR Equivalent or better certifications
Operating Systems and Virtualization Software Support	Windows Server. Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) VMware ESXi. Canonical Ubuntu Oracle Linux and Oracle VM Citrix	Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) VMware ESXi. Canonical Ubuntu Or any other Open source software with support to meet the requirements

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 1Gbps remote management port 3. Server 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 7. Local or Directory-based user accounts with Role based access control 8. Remote console sharing upto 6 users simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Microsoft Terminal Services Integration, 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. 9. Should support managing multiple servers as one via Group Power Control Group Power Capping Group Firmware Update Group Configuration Group Virtual Media and Encrypted Virtual Media Group License Activation 10. Should support RESTful API integration 11. System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support 12. Server should have security dashboard : displaying the status of important security features, the Overall Security Status for the system, and the current	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 1Gbps remote management port 3. Server 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 7. Local or Directory-based user accounts with Role based access control 8. Remote console sharing upto 6 users simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Microsoft Terminal Services Integration, 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. 9. Should support managing multiple servers as one via Group Power Control Group Power Capping Group Firmware Update Group Configuration Group Virtual Media and Encrypted Virtual Media Group License Activation 10. Should support RESTful API integration 11. System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support 12. Server should have security dashboard : displaying the status of important security features, the Overall Security Status for the system, and the current configuration for the Security State and Server Configuration Lock features. 13. One-button Secure Erase designed to decommission/repurpose servers 15. Workload Performance Advisor - Provides server tuning recommendations to improve server performance
	Zero Touch Provisioning (ZTP) using SSDP with remote access	Zero Touch Provisioning (ZTP) using SSDP with remote access Or equivalent

Chapter -3 Misc Nodes (Management, Control Plane and other nodes)		
Item	**Specifications Published EOI 09.07.2025**	**Final Amended Clauses**
CPU	Min Two or more x86 Architecture based server Processors*, Each CPU with at least 36/48 Cores,2.1GHz Base or higher with 105MB Cache or more	Min Two or more x86 Architecture based server Processors*, Each CPU with at least 32 cores or higher ,2.1GHz Base or higher with 60 MB Cache or more.
Memory	- 64DIMM slots. -1TB DIMMS scalable up to 8.0 TB using DDR5 Registered DIMM (RDIMM) operating at 4800 MT/s	25 DIMM slots or more Server should be configured with 256GB RAM or more- scalable upto 6.0 TB using DDR5 Registered DIMM (RDIMM) operating at 4800 or more.
Bus Slot	Server should support upto 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	Server should support upto four PCI-Express Slots 4.0/5.0 X16 slots (Can be a mix of 4.0 or 5.0 OR only 5.0) Additional ONE x8 or higher OCP 3.0 slots
HDD Bays	Up to 24 SFF SAS/SATA/SSD/NVMe populated with 2X 480GB SSD drives	Up to 24 SFF / 12 LFF SAS/SATA/SSD/NVMe populated with 2X 480GB SSD drives
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	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,SSD, 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 or equivalent certifications: 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	Server should be populated with below networking cards: 1. 1Gb 4-port network adaptors 2. 10GBaseT 2-port Ethernet adap 3. Infini Band :2 X 200Gb Single or Dual port Adapter * For Point 3: Applicable for 6 Severs planned as control and Management nodes.	Server should be populated with below networking cards: **1.** 1Gb 4-port network adaptors **2.** 10GBaseT 2-port Ethernet adapt **3.** Single Port InfiniBand NDR Gbps Adapter Note: **For Point 3**: Applicable for 6 Severs planned as control and Management nodes.
Interfaces	Serial - 1 (Optional) USB support with Up to 5 total: 1 front, 2 rear, 2 internal. 1GbE Dedicated management port	Serial - 1 (Optional) USB support with Up to 3 total or more ports 1GbE Dedicated management port
Power Supply	Should support hot plug redundant low halogen power supplies with minimum 94% efficiency	Should support hot plug redundant N+N power supplies

Industry Standard Compliance	ACPI 6.3 Compliant PCIe 5.0 Compliant WOL Support Microsoft® Logo certifications PXE Support Energy Star SMBIOS 3.2 UEFI 2.7 Redfish API IPMI 2.0 Secure Digital 4.0 Advanced Encryption Standard (AES) SNMP v3 TLS 1.2 DMTF Systems Management Architecture for Server Hardware Command Line Protocol (SMASH CLP) Active Directory v1.0 ASHRAE A3/A4	ACPI 6.3 Compliant PCIe 5.0 Compliant WOL Support Microsoft® Logo certifications PXE Support Energy Star SMBIOS 3.2 UEFI 2.7 Redfish API IPMI 2.0 Secure Digital 4.0 Advanced Encryption Standard (AES) SNMP v3 TLS 1.2 Line Protocol (SMASH CLP) Active Directory v1.0 ASHRAE A3/A4 Or Equivalent Certifications
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) 1.2 option 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	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) 1.2 option TPM (Trusted Platform Module) 2.0 option Advanced Encryption Standard (AES) on browser 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	Windows Server. Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) VMware ESXi. Canonical Ubuntu Oracle Linux and Oracle VM Citrix	Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) VMware ESXi. Canonical Ubuntu Or any other Open source software to meet the requirements
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 1Gbps remote management port 3. Server 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 7. Local or Directory-based user accounts with Role based access control 8. Remote console sharing upto 6 users simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Microsoft Terminal Services Integration, 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. 9. Should support managing multiple servers as one via Group Power Control Group Power Capping Group Firmware Update Group Configuration Group Virtual Media and Encrypted Virtual Media Group License Activation 10. Should support RESTful API integration 11. System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support 12. Server should have security dashboard : displaying the status of important security features, the Overall Security Status for the system, and the current configuration for the Security State and Server Configuration Lock features. 13. One-button Secure Erase designed to decommission/repurpose servers 14. NVMe wear level display 15. Workload Performance Advisor - Provides server tuning recommendations to improve server performance	**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 1Gbps remote management port** **3. Server 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** **7. Local or Directory-based user accounts with Role based access control** **8. Remote console sharing upto 6 users simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Microsoft Terminal Services Integration, 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.** **9. Should support managing multiple servers as one via** **Group Power Control** **Group Power Capping** **Group Firmware Update** **Group Configuration** **Group Virtual Media and Encrypted Virtual Media** **Group License Activation** **10. Should support RESTful API integration** **11. System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support** **12. Server should have security dashboard : displaying the status of important security features, the Overall Security Status for the system, and the current configuration for the Security State and Server Configuration Lock features.** **13. One-button Secure Erase designed to decommission/repurpose servers** **14. Workload Performance Advisor - Provides server tuning recommendations to improve server performance**
	Zero Touch Provisioning (ZTP) using SSDP with remote access	Zero Touch Provisioning (ZTP) using SSDP with remote access Or equivalent

Chapter-4

(a) 100TB NVMe Usable capacity PFS based AI Storage with 35GB/s read and write throughput performance

Sl No	Component	Specifications Published EOI 09.07.2025	Final Amended Clauses
1	Capacity & Performance	Hardware RAID based PFS Storage system with a minimum usable capacity of 100TB ALL Flash NVMe controller appliance with 35 GB/s write performance. The read performance should be equivalent or higher than the write performance Storage should give consistent 35 GB/s (or better) throughput for read and 35 GB/s throughput for write for files up to size 2 TB on 100TB NVMe	Hardware / Decluttered/ GRID RAID 6 (8+2) based PFS Storage system with a minimum usable capacity of 100TB ALL Flash NVMe controller appliance with 35 GB/s write performance. The read performance should be equivalent or higher than the write performance Storage should give consistent 35 GB/s (or better) throughput for read and 35 GB/s throughput for write for files up to size upto 2 TB on 100TB NVMe
2	Scalability	Storage Controller System hybrid configuration should scale up to four*5U 84 NL SAS Drive enclosures or all flash configurations should scale out up to 4* all flash arrays	Storage Controller System hybrid configuration should scale up seamlessly.
3	High Availability & Redundancy	Storage solution must have a minimum of two active controllers, hot swappable redundant power supplies and fans with no single point of failureFast rebuilds: Storage must offer fast rebuild capability for replacing failed drives. Bidders must demonstrate rebuilding in less than 16 hours.	Storage solution must have a minimum of two active controllers with N+N hot swappable redundant power supplies and fans with no single point of failure/ Software-defined storage architectures achieve high availability (HA) through multi-node clustering Fast rebuilds: Storage must offer fast rebuild capability for replacing failed drives. Bidders must demonstrate rebuilding.

4	File System	Only OEM commercially supported solution is accepted. Entire solution should be from single OEM.	File system must be an OEM-supported(Lustre/GPFS), enterprise-grade parallel file system with full support.
		f) Data striping across multiple I/O nodes and RAID LUNS	Data striping across multiple I/O nodes and RAID LUNS or equivalent
5	Online Spare	2% of disk drives of PFS should be configured as hot online spare drives	2% of disk drives/ Capacity of PFS should be configured as hot online spare drives / CAPACITY
7	Connectivity	-Storage interface should be minimum 8 nos. of 200 Gbps IB with sufficient ports to meet performance requirement.-Necessary cable and connectors as per solution requirement should be provided.20:20	Storage interface should be minimum 4 nos. or more of 200 Gbps IB/ Ethernet with sufficient ports to meet performance requirement.-Necessary cable and connectors as per solution requirement should be provided
8	Benchmarking	-Bidder should submit the IOR/FIO benchmark for 35 GB/s write performance and 35 GB/s read performance with 1 MB block size & metadata benchmarks MDTEST for 100,000 files create/sec.-Benchmark report should be submitted along with the bid.	Bidder should submit the IOR/FIO benchmark for 35 GB/s write performance and 35 GB/s read performance with 1 MB / 4MB / 16MB block size or as suggested by OEM & metadata benchmarks MDTEST for 100,000 files create/sec. -Benchmark report should be submitted along with the bid. The report would be recreated at the time of handover for reference check.
9	Management	Storage solution to be provided with OEM certified Enterprise level GUI based platform for configuration, management and Monitoring for storage and file system.	Storage solution to be provided with OEM certified Enterprise level GUI / CLI based platform for configuration, management and Monitoring for storage and file system.

Chapter -4 (b) **100TB NVMe Usable capacity high-performance, scale-out network-attached storage (NAS)with 35GB/s read and write throughput performance**			
Sno	Component	**Specifications Published EOI 09.07.2025**	**Final Amended Clauses**
1	Capacity & Performance	POSIX Compliant Parallel/ scaleout Filesystem based Storage with NSPOF. The solution must deliver 30GB/s of reads (100%) throughputs The solution must deliver 15GB/s of write (100%) throughputs Capacity : 200TiB usable capacity based on maximum 7.68TB NVMe drives DRAM cache : 2.5TB usable DRAM based cach Data protection : Dual parity data protection (8D+2P) of RAID / De-clustered Raid / Erasure Coding or their equivalent.	POSIX Compliant Parallel/ scale out Filesystem based Storage with NSPOF. The solution must deliver 30GB/s of reads (100%) throughputs The solution must deliver 15GB/s of write (100%) throughputs Capacity : 100TiB usable capacity based on maximum 7.68TB NVMe drives DRAM cache : 1TB OR MORE usable DRAM based cache Data protection : Dual parity data protection (8D+2P) of RAID / De-clustered Raid / Erasure Coding or their equivalent.
2	Features	- The offered storage system should be provided with single unified addressable global namespace / single filesystem capability on complete storage solution with at least 200TiB usable capacity available to each client system	The offered storage system should be provided with single unified addressable global namespace / single filesystem capability on complete storage solution with at least 100TiB usable capacity available to each client system
		Disk amounting to minimum additional 10% of usable space should be provided as hot spare and snapshot space	Disk amounting to minimum additional 10% of usable space should be provided as spare and snapshot space
		The solution shall provide the means to globally automate data services at a file-granular level across all storage types and locations without disruption to users/ applications. These include data protection services, such as global snapshots, clones, DR replication, etc. as well as data mobility actions, such as tiering, migration, etc.	The solution shall provide the means to globally automate data services at a file-granular level across all storage types and locations without disruption to users/ applications. These include data protection services, such as global snapshots/ clones, DR replication, etc. as well as data mobility actions, such as tiering, migration, etc.
		Solution shall allow administrators to build policies with simple IF / THEN statements via the user interface/API/ CLI.	Solution shall allow administrators to build policies with simple statements)(like IF/Then etc) via the user interface/API/ CLI.
		Solution shall allow administrators to define policies that control data protection at cluster, directory of file level. These policies shall be set via GUI/ API/ CLI.	Solution shall allow administrators to define policies that control data protection at cluster or directory or file level. These policies shall be set via GUI/ API/ CLI.

		The solution shall provide the means to globally automate data services at a file-granular level across all storage types and locations without disruption to users/ applications. These include data protection services, such as global snapshots, clones, DR replication, etc. as well as data mobility actions, such as tiering, migration, etc.	The solution shall provide the means to globally automate data services at a file-granular level across all storage types and locations without disruption to users/ applications. These include data protection services, such as global snapshots/clones replication, etc. as well as data mobility actions, such as tiering, migration, etc.
		The solution shall allow for expansion of a filesystem without downtime, Storage should be able to scale up/scale out to 100 times the usable capacity within same namespace.	The solution shall allow for expansion of a filesystem with min downtime and without loss of data. Storage should be able to scale up/scale out to seamless with minimum 20 times the usable capacity and number of offered nodes within same namespace.
		The solution shall support snapshots and clones of an entire filesystem without performance degradation.	The solution shall support snapshots and clones of an entire filesystem with or without performance degradation.

Chapter -5 SAN Storage		
S. No	**Specifications Published EOI 09.07.2025**	**Final Amended Clauses**
1	The offered storage should be a SAN storage with specialised *Operating system for Storage.Modified operating system as Storage OS shall not be considered. The storage should have Symmetric/ dual Active-Active Controller architecture where a LUN should be accessible by all the controllers simultaneously. File System should be compatible with block, object file storage*	The offered storage should be a SAN storage with specialised Operating system for Storage.Modified operating system as Storage OS shall not be considered. The storage should have Symmetric/ dual Active-Active Controller architecture where a LUN should be accessible by all the controllers simultaneously. File System should be compatible with block, object and file storage
2	SAN Storage for thin client solution should be supplied with minimum 100TB usable capacity using SSD's on RAID 6. The proposed system should be upgradable to 500TB of capacity. The supported disks should be dual ported with minimum 12Gbps or higher full-duplex data transfer capability.	SAN Storage for thin client solution should be supplied with minimum 100TB usable capacity using SSD's /NVME on RAID 6. The proposed system should be upgradable to min of 500TB of capacity. The supported disks should be dual ported with minimum 12Gbps or higher full-duplex data transfer capability.
5	SAN Storage should have minimum 4 x FC ports (16 Gbps) and 4 x 10Gbps for host connectivity on the same set of proposed controllers. Storage should have minimum 4 x 12Gbps SAS Links for Disk connectivity on the same set of proposed controllers	SAN Storage should have minimum 4 x FC ports (16 Gbps) and 4 x 10Gbps for host connectivity on the same set of proposed controllers. Storage should have minimum 4 x 12Gbps or higher SAS/ NVME Links for Disk connectivity on the same set of proposed controllers

9	SAN storage system should have support for multi-path configuration for redundant path to connected hosts. Any Licenses (unlimited/frame based) required for this should be provided with Storage from day one. The storage should have protection of cache data during a power down by de-staging the data in cache to non-volatile Disk.	SAN storage system should have support for multi-path configuration for redundant path to connected hosts. Any Licenses (unlimited/frame based) required for this should be provided with Storage The storage should have protection of cache data during a power down by de-staging the data in cache to non-volatile Disk.
10	The SAN storage should support data tiering between different storage tiers namely SSD/ SAS/ NL-SAS within the same storage array. Optional tiering license for Unlimited Capacity should be included in the proposal.	The SAN storage should support data tiering between different storage tiers namely SSD/ SAS/ NL-SAS/NVME within the same storage array. Optional tiering license for Unlimited Capacity should be included in the proposal.
11	Storage should be supplied with Storage management, virtual/thin provisioning, remote replication copy (sync and ASYSNC both). Remote replication license to be supplied for Unlimited capacity.	Storage should be supplied with Storage management, virtual/thin provisioning, remote replication copy (sync and Async both). Remote replication license to be supplied for Unlimited capacity.

Chapter -7 Management Switch(Qty 1)		
Sr.No	**Specifications Published EOI 09.07.2025**	**Final Amended Clauses**
1	**General Features:** **Access Switch 48 Ports and 4 x 1G/10G SFP+ 4X100G uplink ports**	Access Switch 48 nos. of 1000 Base-T Ports and 4 x 1G/10G SFP+."
	Switch should have integrated trusted platform module (TPM) or equivalent for platform integrity to ensure the boot process is from trusted sourceOR The Switch should support image pre-check. The firmware installation is performed only if the result of the pre-check successful.	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.
	Operating temperature of 0°C to 45°C.	Operating temperature minimum of 0°C to 40°C or better
	The switch will have at up to 880 Gbps switching capacity.	The switch will have at up to 880 Gbps switching capacity or more
	Forwarding rates: The switch should have 650Mpps forwarding rates.	Forwarding rates: The switch should have 650Mpps forwarding rates or more.
	IPv4 Routing entry support : 60K or more.	IPv4 Routing entry support : 24K or more.
	IPv6 Routing entry support : 60K or more.	"IPv6 Routing entry support : 12K or more.."
	The switch will have at up to 128 Gbps switching capacity.	The switch will have at up to 128 Gbps switching capacity or more
	Forwarding rates: The switch should have 95Mpps forwarding rates.	Forwarding rates: The switch should have 95Mpps forwarding rates or more

	VLANs ID: 4K or more and 2K VLANs simultaneously.	VLANs ID: 4K or more and 1K or more VLANs simultaneously.
	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 support minimum 10 switch in stack	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 to allow integrated backplane. The switch should support minimum 8 switch in stack
	Must support EVPN, BGP, BGP4, 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.	Must support , VRF, VXLAN, OSPFv2 and v3 Routed Access, Policy-Based Routing (PBR)/ PIM SM/ PIM-DM/ PIM-SSM /Virtual Router Redundancy Protocol (VRRP) from Day 1.
	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 support Zero-Touch Provisioning (ZTP). The switch shall support IP SLA or equivalent
	The switch should be manageable from cloud NMS or On-premises NMS solution offered.	The switch should be manageable from cloud NMS or from On-premises NMS solution offered
	The switch should support IEEE 802.1X or MAC filtering	The switch should support IEEE 802.1X and MAC filtering
	The switch should support Port-based authentication, if solution is based on 802.1x	The switch should support Port-based authentication
	The switch should support MAC-based authentication, if solution is based on 802.1x	The switch should support MAC-based authentication
	Switch or Switch's Operating System on different hardware platform should be tested for EAL 2/NDPP or above under Common Criteria Certification.	Deleted

Chapter-8 Network Switch 48 Ports (Qty 2)		
Sr.No	**Specifications Published EOI 09.07.2025**	**Final Amended Clauses**
	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.	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
	Operating temperature of 0°C to 45°C	Operating temperature minimum of 0°C to 40°C or better
	The switch will have at up to 880 Gbps switching capacity.	The switch will have at up to 880 Gbps switching capacity or more
	Forwarding rates: The switch should have 650Mpps forwarding rates.	Forwarding rates: The switch should have 650Mpps forwarding rates or more.
	IPv4 Routing entry support : 60K or more.	IPv4 Routing entry support : 24K or more.
	IPv6 Routing entry support : 60K or more.	IPv6 Routing entry support : 12K or more
	VLANs ID: 4K or more and 4K VLANs simultaneously.	VLANs ID: 4K or more and 1K VLANs simultaneously.
	The swith 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 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 to allow integrated backplane. The switch should support minimum 8 switch in stack
	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	Must support , VRF, VXLAN, OSPFv2 and v3 Routed Access, Policy-Based Routing (PBR)/ PIM SM/ PIM-DM/ PIM-SSM /Virtual Router Redundancy Protocol (VRRP) from Day 1.
	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	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

	DCB Exchange Protocol (Pre-standard LLDP DCBX IEEE 1.01 version)	DCB Exchange Protocol (DCBX IEEE 1.01 version)
	Switch should have SCSI, Lossless iSCSI, RDMA over Converged Ethernet version 2 (RoCE v1 and v2) and Non-Volatile Memory Express (NVMe over Fabrics)	Switch should have SCSI, Lossless iSCSI, RDMA over Converged Ethernet version 2 (RoCE v1 and v2) and Non-Volatile Memory Express
	Switch or Switch's Operating System on different hardware platform should be tested for EAL 2/NDPP or above under Common Criteria Certification.	**Switch or Switch's Operating System on different hardware platform should be tested for EAL 2/NDPP or above under Common Criteria Certification or equivalent certifications**
	The OEM shall be in Leaders Quadrant of Gartner report for Wired & Wireless LAN Infrastructure for minimum 5 Consecutive Years.	**Deleted**

Chapte-9 Network Switch(Other side user Connectivity Qty2 48 Port)		
Sr. No	**Specifications Published EOI 09.07.2025**	**Final Amended Clauses**
1	**General Features**	
	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 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
	Operating temperature of 0°C to 45°C	Operating temperature of 0°C to 40°C or better
	Must support EVPN, BGP, BGP4, 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	Must support , VRF, VXLAN, OSPFv2 and v3 Routed Access, Policy-Based Routing (PBR)/ PIM SM/ PIM-DM/ PIM-SSM /Virtual Router Redundancy Protocol (VRRP) from Day 1.
	New Clause	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
	New Clause	**Switch or Switch's Operating System on different hardware platform should be tested for EAL 2/NDPP or above under Common Criteria Certification or equivalent certifications**

Chapter 10 Cyber Security Suite NGFW(Next-Generation Firewall)		
Sr.No	**Specifications Published EOI 09.07.2025**	**Final Amended Clauses**
	Make & Model (Specify the model no.)	
1	**Appliances Requirements**	
3	Appliances should be rack mountable and with at least 64 GB RAM or higher from day 1 . Supply of Rack mounting kit along with all accessories is under bidders scope.	Appliances should be rack mountable and with at least 32 GB RAM or higher from day 1 . Supply of Rack mounting kit along with all accessories is under bidders scope.
7	Appliance should **have 36 Gbps of NGFW throughput** and scalable to 70 Gbps in near future (including Firewall, application control/app-ID and IPS.	Appliance should have minimum of 25 Gbps of NGFW throughput and scalable minimum of 50 Gbps in near future (including Firewall, application control/app-ID and IPS.
10	Appliances should have a least 12 Gbps real world/ enterprise mix/Production Mix Threat Prevention throughput from day one and scalable to 24 Gbps in near future (including FW, IPS, Application Control, Anti-Virus, Anti-BOT & URL filtering) at various TCP packets/size from day 1. Should submit public document.	Appliances should have a least 10 Gbps or more real world/ enterprise mix/Production Mix Threat Prevention throughput from day one and scalable to 24 Gbps or more in near future (including FW, IPS, Application Control, Anti-Virus/Antimalware, Anti-BOT & URL filtering) at various TCP packets/size from day one.
16	Appliance should support minimum 180k connections per second and scalable to 360K connections per second in future.	Appliance should support minimum 180k connections or more per second and scalable to 360K or more connections per second in future .
17	Appliance should support at least >10 million concurrent sessions/connection from day one and scalable to 32 million in future.	Appliance should support at least >50 million concurrent sessions/connection from day one and scalable to 180 million in future.

21	Solution should provide IPv4 and IPv6 dual stack support from day one. OEM should be IPv6 logo approved. Supporting documents to be submitted.	Solution should provide IPv4 and IPv6 dual stack support from day one. OEM should be IPv6 / USGv6 or equivalent logo approved. Supporting documents to be submitted.
	and behavior-based detection.	
46	IPS should be able to detect and prevent the following threats: • Protocol misuse • Malware communication • Tunnelling attempts • Denial of service • Oher generic types without predefined signatures	IPS should be able to detect and prevent the following threats: • Protocol misuse with Evasion and anomaly logging • Malware communications and Message length sequence analysis • Tunnelling attempts • Denial of service • Multilayer traffic normalization with Vulnerability-based fingerprints •Oher generic types without predefined signatures
63	Solution should protect from DNS Cache Poisoning and prevents users from a accessing blocked domain addresses.	Solution should protect from DNS Cache (it should also prefebally protect against DDNS/ DGA/DOT/ DNS tunneling, DNS injection, DNS spoofing)Poisoning and prevents users from a accessing blocked domain addresses.
65	The Solution should include next generation threat prevention features including Antibot and Antivirus functionality multi-thread detection engine which includes the reputation of Ips, URLs and DNS addresses and detect patterns of bot communications and scanning of malicious files.	The Solution should include next generation threat prevention features including Antibot and Antivirus/Antimalware functionality multi-thread detection engine which includes the reputation of Ips, URLs and DNS addresses and detect patterns of bot communications and scanning of malicious files.
72	The firewall should belong to product family which minimally attains EAL4+ certified. Bidder to submit supporting documents.	The firewall should belong to product family which minimally attains EAL4+ certified or common criteria certified. Bidder to submit supporting documents.

76	Dedicated Firewall Management, log server and reporting server must be hardware appliance at On-prem only. must be managed from the same management appliance. Must be rack mountable.	Dedicated Firewall Management, log server and reporting server must be hardware appliance or OEM provide Software at On-prem only. If Software is provided then Bidder to factor the hardware to run the solution. We have to keep the same as column C
77	Appliance must have minimum 4x 10G SFP+ port, minimum 4TB storage 100 GB per day of Logs, 8000 (Sustained log per sec), minimum 32GB of memory and minimum10 device license management from day one.	**Appliance must have minimum 4x 1G Copper port or 2X * 10G SFP+ port or more , minimum 4TB storage 100 GB per day of Logs, 2000 (Analytic Sustained rate) or better, and minimum10 device license management from day one**
87	The firewall should belong to product family which minimally attains EAL4+/NDPP certified. Bidder to submit supporting documents.	**Deleted**
88	Complete Solution must be from same OEM. Whitelabling of product is not allowed.	**Deleted**

HIPS (Host Intrusion Prevention System) Workstations		
Sr.No	**Specifications Published EOI 09.07.2025**	**Final Amended Clauses**
10	The proposed solution must be able to automatically deploy protection to virtual infrastructures based on VMware ESXi, Microsoft Hyper-V, Citrix XenServer, KVM, Nutanix Acropolis virtualization platform.	The proposed solution must be able to automatically deploy protection to virtual infrastructures based on VMware ESXi, Microsoft Hyper-V, **as well as OS** Citrix XenServer, KVM, Nutanix Acropolis virtualization platform.
28	Suggested solution must be able to scan powered off Linux virtual machines with the following file systems: EXT2, EXT3, EXT4, XFS, BTRFS.	Suggested solution must be able to scan powered off Linux virtual machines with the following file systems: EXT3, EXT4, XFS, BTRFS.
36	Suggested solution must support scanning secure connections that are established using the SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, or TLS 1.3 protocols.	Suggested solution must support scanning secure connections that are established using the SSL 3.0, TLS 1.2, or TLS 1.3 protocols.

SIEM (Security Information and Event Management)		
Sr.No	**Specifications Published EOI 09.07.2025**	**Final Amended Clauses**
133	Technical support must include custom parsers (at least 10 types) for data sources not supported by solution ‘out-of-the-box’.	Delete
134	Technical support must be via a dedicated manager provided by the Vendor.	Technical support must be via a provided by the SI as part of operations support

Chapter-11 Workstations(Qty 85+20*)				
SNo	Category	Specification Item	**Specifications Published EOI 09.07.2025**	**Final Amended Clauses**
	Storage			
		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 or 1x 9.5mm slim optical disk drive bay
	Graphics Card	GPU Model	NVIDIA Quadro T1000	NVIDIA Quadro A1000 or GPU's similar or better benchmarking

Chapter-12 Conference Solutions				
Sno	Category	Specification Item	**Specifications Published EOI 09.07.2025**	**Final Amended Clauses**
		Zoom Capability	Minimum 12x Optical Zoom (or equivalent lossless digital zoom with comparable quality at 12x).	Minimum 6x Optical Zoom (or equivalent lossless digital zoom with comparable quality at 6x).
		Pan/Tilt Range	Pan: Minimum ±170 degrees; Tilt: Minimum ±90 degrees.	Pan: Minimum ±170 degrees or more; Tilt: Minimum ±45 Degree or more.
4	Features & Control	Camera Presets	Minimum 10 programmable camera presets.	Minimum 2 or more programmable camera presets.