Open Tender Notice No. /खुला प्रस्ताव निविदा सूचना नंबर: IITD/FT/EOI/2025-26

NOTICE INVITING EXPRESSION OF INTEREST (EOI)

The Foundation for Innovation and Technology Transfer (FITT), New Delhi invites Expression of Interest (EOI) from eligible firms for the following work.

Name of the work: Creation of IT Infrastructure for Startup India Grand Challenge with the theme of "Responsible AI for National Security".

Interested firms may visit our website (https://fitt-iitd.in/) and apply through CPP portal.

The last date for the submission of proposal (one envelop system) is 23rd July 2025 (15 Days from Publication **D Day**) till 1700 Hrs.

Key Dates (Subject to Change to next working day if day is a non-Working day)

1.	Publication	D Day
2.	Site Visit Data Center	D+5 (Tentative time 1400Hrs)
3.	Pre-Bid Query	D+7 (Time 1700 Hrs)
4.	Pre-Bid Meeting (Hybrid Mode)	D+9/10 (Time 1400 Hrs)
5.	Submission date	D+15 (Time 1700 Hrs)
6.	Evaluation Dates	D+16 to 21 (Time 1700 Hrs)

Proposals can be sent on email to nciipc@fitt-iitd.in. For any queries via WhatsApp (9810601703, 9718934343)

Also, send hard copy of your proposal at the following address.

To,

Chief Operating Officer
Foundation for Innovation and Technology Transfer (FITT)
Research and Innovation Park (Room 3A1A)
Indian Institute of Technology Delhi
Hauz Khas
New Delhi -110016

Note: Extension in the last date of submission of EOI shall be allowed only in exceptional case.

Table of Contents

Chapter- 1

Introduction

About FITT

1. The Foundation for Innovation and Technology Transfer (FITT) is a prominent industry-academia interface organization (Not for Profit) established by the Indian Institute of Technology Delhi (IIT Delhi). FITT at IIT Delhi has been the vanguard of knowledge transfer activities from academia since its inception in 1992. This techno-commercial organization from academia is counted amongst the successful such organizations. FITT provides superior program management services and is steadily increasing its operational landscape. The varied roles of FITT can be seen in enabling innovations and technopreneurship, business partnerships, technology development, consultancy, collaborative R&D, technology commercialization, development programs, corporate memberships etc. These roles are necessitated by the key agenda of the Foundation to showcase the Institute's "intellectual ware" to industry, and thereby unlock it's knowledgebase and inculcate industrial relevance in teaching and research at IIT Delhi.
2. FITT's core mission is to foster, promote, and sustain the commercialization of science and technology developed at IIT Delhi for mutual benefits with industry. It is designed to be an effective interface with the Industry to foster, promote and sustain commercialization of Science and Technology for the Academia, Startup ecosystem and Industry mutual benefits."
3. With this mission mode, FITT has enabled knowledge transfer and created partnerships and linkages with business and community.

4. Key functions and activities of FITT include:
   a) Research & Development Partnerships: Facilitating collaborations between IIT Delhi's researchers and industry partners for technology development, addressing specific technological challenges, and developing proprietary knowledge.
   b) Intellectual Property (IP) Management: Managing the intellectual property (IPR) of IIT Delhi, including filing patents and facilitating the commercialization of IP assets and know-how through technology transfer and licensing agreements.
   c) Innovation & Entrepreneurship: Nurturing an entrepreneurial ecosystem by managing incubation programs (like Technology Business Incubation Units - TBIUs, Biotechnology Business Incubation Facilities - BBIFs, and Atal Incubation Centres) to support startups and innovators. They provide mentorship, infrastructure, and access to funding.
   d) Technology Transfer & Commercialization: Bridging the gap between academic research and market needs by transferring proven R&D outputs to industry, leading to new products, processes, and services.

e) Consultancy and Training: Offering innovative problem-solving consultancy services to industry clients and conducting specialist development programs and training courses in emerging technologies.
f) Research Park: Developing and managing a research and innovation park that serves as a hub for interaction between IIT Delhi, industry, entrepreneurs, and government agencies to create advanced technological solutions.
g) Government and Corporate Programs: Participating in various government initiatives (e.g., SPARSH, MSME, NIDHI) and collaborating with Startup ecosystem, corporate entities to support innovation and technology development.

5. FITT plays a crucial role in translating academic research into real-world applications, supporting the startup ecosystem, and enhancing industry relevance in teaching and research at IIT Delhi. It has been recognized as a Scientific and Industrial Research Organization (SIRO) by DSIR, making it eligible for certain exemptions on imports for R&D programs.

About the Project

6. NCIIPC a Government of India undertaking has partnered with FITT, IIT Delhi for conduct of NCIIPC Startup India Grand Challenge with the theme of "Responsible AI for National Security". The challenge focuses on identifying and fostering the development of cutting-edge AI solutions for Twelve critical problem statements defined by the technical and operational teams at NCIIPC and SME from the academia. (Refer to website https://ai-grand-challenge.in/ for the details.)
7. The IT hardware being procured for the datacentre will be used to provide Compute resources to the Startups which would be incubated in the Incubation facility being created as a part of this challenge in which shortlisted startups i.e. upto a maximum of 3 Startups per problem statement (Maximum of 36 Startups) would work on the Problem statements to create AI models. The Startups will be provided with compute facility and resources to access Customised data sets being generated as a part of the challenge.

8. ***FITT invites EoI from System Integrators (SI) for creation of facilities and support for Operations as per the details given below for a datacentre and Incubation Centre being created as part of the challenge.***

9. **Make in India (Purchase preference)-** The brief of Public Procurement order 2017 (Preference to Make in India) issued by Ministry of Commerce & Industry dated 15.6.2017 and subsequent revision issued by Ministry of Commerce and Industry vide order dated 28.5.2018, 29.05.2019, 04.06.2020, 16.09.2020 and Notification of Ministry of Textiles dated 01.02.2019 to be followed as under:-
10. 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.

11. **Purchased preference** - The 'Class-I local supplier' will get purchase preference over 'Class-II Local Supplier' as per the existing procedures
12. **Scope of Work D**eployment of the incubation facility will be done at the locations, as under: -

    a) **DataCenter Ayanagar, New Delhi**. Utilise the existing Tier 3 data center to deploy Hardware consisting of Domain Management server, Database server, Application server, Secure email server, Collab suite server, GPU facility and central Storage connected over a Network fabric with Switches connecting servers and GPUs in the existing Tier-III Data Centre located in the premises. (BOQ is attached as Annexure 1)

    b) **Establishment of IT Office Infrastructure** The project also envisages a creation of an Incubation Centre at Mayur Vihar/ Ayanagar, New Delhi. to include Seating Capacity 85 (Cubicles, Furniture, AC, 2 x Mini Conference Halls), Workstations (85 for LAN/ standalone),conference rooom and with Electrical Supply through requisite deployment of Genset and UPS for office infra and workstations. It will also require some basic utility provisions washrooms, drinking water, basic pantry area for these 80-85 people. ***The SI is required to provide only the IT hardware and the networking components as per the details in the document.***

    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, 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.***

    d) **IT infra Supply** Supply IT hardware to an existing Premises (Bengaluru) The facility will be equipped as under: -

    i) Ten workstations for connection with internal/Internal network
    ii) Ten Standlone work stations and Five external HDD
    iii) One LED screen for meetings over internal network with Delhi teams
    iv) Two internal network VOIP terminals

    e) **Operational Support** Provide operational support up to 12 months from date of installation and acceptance.
13. **Warranty and 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. This EOS support must encompass, but not be limited to, access to technical assistance, firmware/software updates (as applicable to hardware functionality), and hardware replacement services, as defined by the manufacturer's standard EOS terms, ensuring operational continuity and problem resolution for the entire duration of six years i.e. 3 Years warranty and 3 years EoS Support..

14. **Software:** All software required to be supplied should be preferably Open source 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

Chapter- 2

Tentative Network Diagram

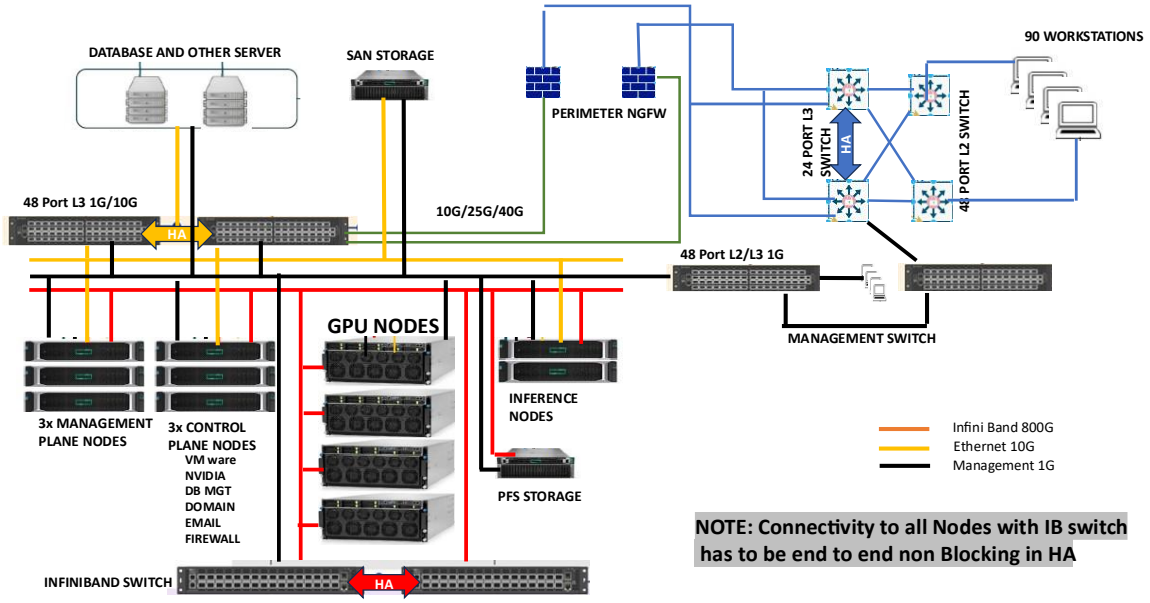

Figure 1:

Hardware requirements:

(Detailed technical Specifications are given in Chapter 3)

1. ***The tentative quantity of material required is given below. The SI is free to recommend addition/reduction in the BOQ with justification. Also, FITT is empowered to add/reduce required Hardware depending on the change in scope of work when the RFP is finalised. The Change in any scenario is not visualized to exceed 20% of the BOQ listed in this document.***

2. ***SI has to ensure connectivity with ancillaries for the solution to be made functional with onsite spares***

3. The SI can examine the given requirements and suggest/advice on the changes to make the EoI Specifications more open and robust within the existing scope, by focussing on architectural principles, best practices, and strategic choices that enhance flexibility, resilience, and long-term viability without fundamentally changing the core functionality.

4. GPU Servers (Qty 4): Purpose of having GPU servers is fundamentally to provide the massive, parallel computational power required to develop, train, and deploy modern Artificial Intelligence models, especially leveraging deep learning. GPU servers is crucial to ensure optimal performance, scalability, and cost-effectiveness. Hardware specifications of

this dedicated hosting server should be easily upgradable and scalable with easy access to the SAN Storage

a) The GPU would be provided to the Startups in the incubation center for training there AI models based on Data being provided by NCIIPC
b) Minimum Requirement
    i) Total 4 nodes are required and each Node must be configured with 8 x H200 141GB GPUs (SXM5) connected via Nvlink and NV Switch with minimum 900GB/s bidirectional communication bandwidth
    ii) 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.
    iii) The total aggregate memory per node from the GPUs should be at least 1128 GB.

5. Inference Node Servers(Qty 2) These severs are visualised to host and execute trained AI models to generate predictions or insights in real-time or near real-time. They are the operational endpoints for the AI models. The Severs should be optimised for

a) **Low Latency:** Many inference tasks (e.g., fraud detection, facial recognition) require immediate responses. Inference servers are configured to minimize the time it takes to process a single request.
b) **High Throughput:** They must be able to handle a large volume of concurrent inference requests efficiently, serving many users or applications simultaneously.
c) **Cost-Efficiency:** Inference often doesn't require the same sheer compute power per GPU as training. Organizations can deploy GPUs specifically designed for inference

6. Misc Nodes(Qty 24)***:-***

a) *Management node: They are planned to be the management* centres of an HPC cluster. They will be used for orchestrating the entire environment. Their primary roles include:
    i) *Job scheduling and resource allocation*
    ii) *Monitoring and logging*
b) *Control Node:-* These nodes serve as the central brain of the cluster, responsible for its overall operation and coordination. Their primary functions include:
    i) *Resource Management*
    ii) *User Access*
    iii) *System Configuration and Deployment*

c) *Application Servers* should serve as the crucial interface and operational backbone for interacting with, utilizing, and deploying those trained AI models. It shall be able to bridge the gap between raw AI capabilities and practical, usable applications and workflow. The hardware

specifications of these server should be easily upgradable and scalable with easy access to the SAN Storage.

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).
   iii) Vector Databases (e.g., Pinecone, Milvus, Qdrant, or databases with vector capabilities like PostgreSQL with pgvector)
   iv) Server should support below controllers, must support Mixed Mode which combines RAID and HBA mode operation simultaneously

e) *Management Server* Management Server (or a cluster of management servers) should act as the central control plane and operational hub for the entire IT infrastructure. Its primary purpose is to ensure the efficient, secure, stable, and automated functioning of all other critical components. Server should support controllers, must support Mixed Mode which combines RAID and HBA mode operation simultaneously.

f) *Domain Management Server* Domain Management Server should serve the critical purpose of providing a centralized, secure, and streamlined system for managing identities, access, and resources across the IT infrastructure

g) *Collaboration Suite Server* should serve as a vital role in fostering communication, streamlining teamwork, and enhancing productivity among researchers, data scientists, engineers, and project managers

NOTE: The server /nodes must include 480GB x 2 internal storage capacity for local operations. In addition, the System Integrator (SI) is required to propose a shared storage solution with a minimum capacity to support all servers/VMs, accessible over a 10G network interface. The shared storage should ensure high availability, redundancy, and optimal performance for the server/VM operations

7. *SAN Storage with OS for Shared Storage Access Suite Server(100TB)* A high-performance, block-level storage solution designed to provide shared access to multiple servers. Capable of operating independently of individual server storage systems and is connected via high-speed protocols like Fibre Channel or iSCSI, ensuring low-latency and high-bandwidth data transfer. When configured with an appropriate operating system, it should enable seamless mounting of shared storage space on

multiple servers, supporting high-availability, redundancy, and scalability for enterprise workloads. It should work seamlessly in environments requiring shared access, such as database clusters, virtualization, and HPC workloads, while ensuring data consistency and efficient resource utilization

8. 100TB NVMe Usable capacity PFS based AI Storage or high-performance, scale-out network-attached storage (NAS)

a) The storage solution for the HPC environment must provide high-performance, scalable, and reliable data handling capabilities to support computational tasks. It should enable rapid data access, seamless integration with the HPC cluster, and efficient management of large datasets.
Options for Bidders:

- Bidders are required to propose a storage solution meeting the specified performance and capacity requirements. They may supply either of the following::
  - **Parallel File System (PFS) Solution:** Suitable for narrowly focused HPC scenarios, emphasizing high performance for specific workloads but lacking the flexibility and manageability required for diverse, multi-workload enterprise environments.
  - **NAS-based Solution:** Designed for AI and enterprise-scale workloads, offering predictable multi-protocol performance, live frictionless scaling, and operational simplicity. It ensures robust support for rapid AI development and production environments.

The proposed solution should align with the operational and scalability needs of the HPC and AI workloads.

9. Cyber Security Suite to include**:- (Preferably Open Source applications)**

a) *NGFW* **:** NGFWs integrating advanced security features like
i) Intrusion prevention (IPS),
ii) Deep packet inspection
iii) Application control
iv) Threat intelligence.

It should provide a comprehensive network protection by understanding the context of network traffic, identifying and blocking sophisticated threats at the application layer, and enforcing granular security policies**.**

b) *EDR* EDR solutions continuously monitor endpoint devices (like laptops, desktops, servers) for suspicious activities, collect telemetry data, and analyze it for potential threats. Provide advanced detection capabilities to

identify sophisticated attacks that bypass traditional antivirus, enable rapid investigation of security incidents.

c) *HIPS* Host Intrusion Prevention System) HIPS application runs on individual host computers to protect them from unauthorized access and malicious activity. It monitors system calls, file integrity, registry changes, and network connections on the host, actively preventing or blocking suspicious behaviours that indicate an attempted intrusion or malware execution.

d) *STORAGE SECURITY* The data residing in the storage systems (like SAN, NAS, cloud storage, or individual drives) should be prevented from unauthorized access, modification, or destruction. It should provide features like encryption of data at rest, access controls, data loss prevention (DLP) mechanisms, secure deletion, and continuous monitoring to ensure data confidentiality, integrity, and availability.

e) *SIEM* (Security Information and Event Management) SIEM solutions aggregate and analyze security events and log data from various sources across an organization's IT infrastructure, including servers, network devices, applications, and security tools.It should provide centralized visibility into security incidents, use correlation rules and threat intelligence to identify potential threats and anomalies, and support compliance reporting and forensic investigations by providing a historical record of security-related activity**.**

10. NW Equipment for Data Centre and Incubation Centre

a) *IB switch (Qty 2)* For high-speed network to handle extreme performance in demanding computing environments. The switch should provide ultra-low latency and incredibly high bandwidth for interconnection of High-Performance Computing (HPC) nodes i.e GPU Servers

b) *Management Switch (Qty 1)* To manage the Servers in the data *centre*

c) *NW Switch (Qty 2)* The data centre requires 1G/10G/20G bandwidth to connect a diverse set of nodes like GPU servers, inference servers, storage control nodes, and management nodes.

d) *NW Switch (Qty 2)* The distribution switch would be used to connect datacentre to the Incubation centre through WAN on fibre.

Suitable connectors & cables for the NW also are to be catered for

11. Workstation for Incubation Centre (Qty 90)

GPU accelerated workstations along with high-performance CPUs and large RAM, fast storage are required for computationally intensive demands of AI model development, particularly for deep learning. The workstations would be used for Model Training, Hyperparameter Tuning, Data Preprocessing: Inference and Validation.

These workstations would provide a dedicated, high-performance local environment for experimentation, rapid prototyping, and fine-tuning models before deployment to larger, more expensive server clusters or cloud resources.

12. LED TV and Camera for conference room(Qty 2 each) An integrated LED TV and Conference Camera Solution, combines a high-definition LED television, serving as the primary display for content sharing and remote participants, with an advanced conference camera system. The camera system ensures crystal-clear video capture, offering features like wide-angle views, optical zoom, and intelligent framing to perfectly capture every participant. Coupled with superior audio capabilities from the integrated speakerphone, this setup guarantees that every word is heard and every visual detail is seen, fostering richer interactions.

13. Smart Rack for Data Center Infrastructure Smart Racks are required for Data Center Infrastructures. The racks should be designed to provide precision cooling, an Uninterrupted Power supply Systems (UPS), Remote monitoring solution with Biometric Access control for security and Gas Based Fire Suppression System for critical IT component to be housed inside Racks

NOTE* **The requirement of smart racks is to be ascertained after visit to the data centre. However the SI must include the same in his EoI submission. The requirement can be amended /Deleted after the EOI.**

Also please provide inputs on the data centre additions required for successful installation and commissioning of the HPC hardware

Chapter- 3

Technical Specification and compliances

1. GPU Server

Sl NO	Components	Specifications	Compliance Yes/No
1	Quantity of Nodes	4	
2	CPU	Min Two or more x86 Architecture based server Processors*, Each CPU with at least 56 Cores,2.1GHz Base or higher with 105MB Cache or more.	
3	RAM	2048 GB using Dual Rank x4 DDR5-5600 Registered Standard Memory or better Registered ECC RAM installed from day one. Total 32DIMM Slots or higher.	
4	Storage for OS	Each Node must have the provision to be configured with minimum 2 (or More)x 480 GB NVME Drives for OS	
5	Local Storage		Justification for the requirement should be given as we have catered for a PFS storage
6	Networking	Each node must be configured with minimum	
		8 x Dual Port InfiniBand NDR200 Adapter	
		2 x Dual Port InfiniBand NDR200 Adapter for storage interconnect	
		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	
7	GPU	Each Node must be configured with 8 x H200 141GB GPUs (SXM5) connected via Nvlink and NV Switch with minimum 900GB/s 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.	
8	AI Enterprise Software and required SDKs with Support	Licensed AI Enterprise software & subscription for each GPU to be included from day one.	
		NVIDIA Base Command with NVIDIA AI Enterprise Subscription is required.	
		The quoted system should be certified on the NVIDIA AI Enterprise Software Stack.	
		NVIDIA NVAIE License for 5 years support (Per GPU license)	
9	GPU Memory	The total aggregate memory per node from the GPUs should be at least 1128 GB.	
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.	
11	Power Supply	6x 2800-Watt capacity per server system providing N+2 redundant hot-swap Power Supplies	
12	Industry Standard Compliance	1. ACPI 6.3 Compliant	
		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	
		9.Redfish API	
		10.IPMI 2.0	
		11.Advanced Encryption Standard (AES)	
		12.SNMP v3	
13	Embedded Remote Management	Integrated management controller should support:	
		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	
14	System management	Secure Boot that enables the system firmware, option card firmware, operating	

	and system security	systems, and software collaborate to enhance platform security	
15	Operating System	Must support latest versions of	
		a) Red Hat Enterprise Linux (RHEL)	
		b) Ubuntu	
		Quoted OS should be under enterprise support from the OEM.	
16	Operating Environment	Air cooled with support up to 30 degrees C inlet	
17	Installation	Installation, Testing, Training, and Implementation costs for all above mentioned solution must be included from day one.	
18	Form Factor	6U rack mountable or lower	
19	Warranty	3 years + 3 years support	

2. Inference Node Server(Qty 2)

Item	Description of Requirement	Compliance Yes/No
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.	
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	32DIMM slots Server should be configured with 512GB RAM - scalable upto 8.0 TB using DDR5 Registered DIMM (RDIMM) operating at 4800 MT/s	
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	
GPU Support	4 double-wide accelerators (Present) or 8 single-wide accelerators(future) Server should be populated with 4 X L40S Nvidia Cards	
HDD Bays	Upto 8 SFF SSD/NVMe 4 X480 GB NVMe MU SSD drives	
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	
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	
Interfaces	Serial - 1 (Optional) USB support with Up to 5 total: 1 front, 2 rear, 2 internal. 1GbE Dedicated management port	
Power Supply	Should support hot plug redundant low halogen power supplies with minimum 94% efficiency	
Fans	Redundant hot-plug system fans	
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	
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	
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	
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	
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	
Server Management	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	

	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 accesible from anywhere. The portal should provide one stop, online access to the product, support information and provide information to track warranties, support contrats and status. The Portal should also provide a personalised 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	

3. Misc Nodes (Management, Control Plane and other nodes)

Item	**Description of Requirement**	**Compliance Yes/No**
Qty of Nodes 26		
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	
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	- 64DIMM slots. -1TB DIMMS scalable up to 8.0 TB using DDR5 Registered DIMM (RDIMM) operating at 4800 MT/s	
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	
HDD Bays	Up to 24 SFF 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	
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.
Interfaces	Serial - 1 (Optional) USB support with Up to 5 total: 1 front, 2 rear, 2 internal. 1GbE Dedicated management port	
Power Supply	Should support hot plug redundant low halogen power supplies with minimum 94% efficiency	
Fans	Redundant hot-plug system fans	
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	
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	
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, 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. 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 and Encrypted Virtual Media Group License Activation 11. NVMe wear level display 12. Workload Performance Advisor - Provides server tuning recommendations to improve server performance	
Server Management	Software should support dashboard view to quickly scan the managed resources to assess the overall health of the data centre. 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	
	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 personalised 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	

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

PFS based AI Storage			
Sl No	**Component**	**Specification**	**Compliance Yes/No**
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	
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	
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 failure	
		Fast rebuilds: Storage must offer fast rebuild capability for replacing failed drives. Bidders must demonstrate rebuilding in less than 16 hours.	
4	File System	Only OEM commercially supported solution is accepted. Entire solution should be from single OEM.	
		PFS should support a) User & Group Quota b) POSIX compliant c) Should support GPUDirect d) Fine grained locking so that multiple clients can read/write from the same file simultaneously e) Ability to read and write in parallel to same file or different files. f) Data striping across multiple I/O nodes and RAID LUNS	
		No Windows based storage server solution will be accepted.	
5	Online Spare	2% of disk drives of PFS should be configured as hot online spare drives	
6	Metadata	Metadata should be NVMe drives to accommodate 2 Billion files with performance of 100,000 files create/sec. (or better)	
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.	
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.	
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.	
10	Installation	Storage installation must be carried out by bidder or OEM engineers.	
11	Warranty	3 Years +3 years support	

4(b) OR 100TB NVMe Usable capacity high-performance, scale-out network-attached storage (NAS)with 35GB/s read and write throughput performance

Sno	Component	Specifcation	**Compliance Yes/No**
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 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	
		- Usable capacity will need to shall be demonstrated using Linux “df -h” command on the mounted filesystem.	
		`- The solution should provide a single namespace that can scale to 100x the asked capacity	
		The Solution should have Truly distributed fully clustered architecture and which should have scalability of minimum 50 PB as delivering Single Global Name Space with Parallel/scale out file system functions	

		Disk amounting to minimum additional 10% of usable space should be provided as hot spare and snapshot space	
		PFS / scale out filesystem storage should support fast rebuild performance for replacement of failed drives	
		All disks should be hot replaceable	
		The entire DRAM cache should be protected against power failure by battery backed cache/ destage to drive. Solution should be able to handle unexpected power loss without any data loss, data corruption or lengthy file system checks when power is restored.	
		SED based data at rest, motion should be encrypted using the approved cryptographic algorithm like AES. Critical data fields like passwords, pins, etc. should be encrypted before transmission	
		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 a full-featured GUI in addition to a command line interface. All tuning parameters must be accessible through the GUI	
		The management dashboard should have health and performance reporting, visualization, and overall system management functions are accessible using the command line interface (CLI) or the intuitive graphical user interface (GUI) management console	
		Must allow for expansion of a filesystem without downtime	
		Must support user authentication via LDAP and Active Directory	
		Solution shall allow administrators to build policies with simple IF / THEN statements 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.	
		The PFS/ scale out filesystem system and all offered subsystem should be configured with no Single Point of Failure (SPOF),	

		The PFS./scale out filesystem should have redundancy for all systems, component, sub component The Redundancy should be incorporated in PFS/ scale out filesystem solution design such that failure of one redundant system/component/ subcomponent (for eg node, file server, Metadata server, network switch, network card etc wherever offered) should not lead to loss of data or degradation in maximum throughput capability of storage by more than 20%	
		PFS/ scale out filesystem system should provide non-disruptive maintenance.	
		Solution should have Redundant paths and capacity components ensure that maintenance doesn't impact critical services and performance	
3	Connectivity and Data Security	Necessary network infrastructure to be provided for PFS/ scale out filesystem for Ethernet/infiniband based access to clients	
		Storage Solution should be sized with sufficient Ethernet/infiniband interfaces of minimum 200Gbps to meet the required performance and High Availability	
		Network and storage Should support RoCE (RDMA Over Converged Ethernet)/ RD	
		`- POSIX Compliant Parallel File System/ scale out filesystem	
		`- CIFS and SMB natively	
		`- NFSv3, NFSv4	
		`- S3	
		`- GPU Direct storage (GDS)	
		The solution shall support user authentication via LDAP and Active Directory	
		Must have role-based access control (RBAC) to restrict access to authorized end users	
		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 support snapshots and clones of an entire filesystem without performance degradation.	
4	Misc aspects		
		Snapshots and clones occur instantaneously and are differential after the first instance without any performance degradation.	
		Ability to recover the entire filesystem or individual file from snapshots, without administrator intervention	

		Running on compute nodes with 1 MB transfer size and file size double than total storage cache and I/O node memory. The total transfer size should be greater than the RAM available on the AI compute nodes	
		Benchmark must deliver the write throughput for storage min. 15 GB/s.	
		Benchmark must deliver the read throughput for storage min. 30 GB/s	
		OEM Must have deployed atleast one high performance storage in past with minimum 500TB capacity and 30 GBps as sustained performance.	
5	Warranty	3 Years comprehensive warranty with Enterprise level Highest/Premium Support. Quoted all products should not be End of support till 6 years from the date of issue of the bid.	

5 SAN Storage :-

S. No	Minimum Requirements	Compliance (Yes/No)
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	
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.	
3	Storage should be scalable on the same set of controllers.	
4	SAN Storage System should have multiple Global Hot Spares. One Hot spare disk should be provided for every 15 Disk Drives	
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	
6	SAN storage system should have minimum 128 GB cache on the same set of proposed controllers. The complete cache should be accessible by all the controllers in the storage system. Cache memory should be delivered on DRAM, any other device or HDD should not be considered as cache.	
7	The storage should be with No Single Point of Failure (SPOF). All the components should be redundant and hot swappable including power supply, fans, batteries etc. The	

	proposed storage must support non-disruptive replacement of hardware component	
8	The storage must provide non-disruptive firmware/micro code upgrade, device reallocation and configuration changes.	
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.	
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.	
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.	
12	Storage management software should be browser based/ web enabled accessible over IP. Storage management s/w should have roles based access for user accounts to the storage system. Storage management software should be able to perform and monitor local and remote replication operations. Storage management software should be able to configure and manage tiering.	

6 IB NDR Switch (Qty2)

Sl No	Component	Specification	Compliance Yes/No
1	Standard Specifications	64-port Non-blocking Managed NDR 400Gb/s InfiniBand Smart Switch with cables with inbuilt RPS	
		The 1U rack mount switches feature 64, 400Gb/s non-blocking ports with aggregate data throughput up to 51.2 Tb/s 32 octal small form-factor pluggable (OSFP) connectors	
		NDR (400Gbps) per port bidirectional	
		Supports passive copper or active copper or Fiber cable with optical module	
		Compliant with IBTA 1.5	
2	Power Supply	Dual redundant (1+1) hot-swappable power supplies	
3	Cooling	Power to connector airflow Hot-swappable fan units	
4	Cables	Passive copper or active copper or Fiber cable with optical module as per the required length.	
5	Warranty	3 Years +3 years support	

7. Management Switch(Qty 1)

Access Switch 48 Ports and 4 x 1G/10G SFP+ 4X100G uplink ports

Sr.No	Minimum Technical Specification	Compliance (Yes/No)
1	**General Features:**	
	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 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 8 GB DRAM and 16 GB Flash.	
	The switch will have at up to 128 Gbps switching capacity.	
	Forwarding rates: The switch should have 95Mpps forwarding rates.	
	IPv4 Routing entry support : 2K or more.	
	IPv6 Routing entry support : 1K or more.	
	IGMP Groups and MLD Group : 1K or more.	
	MAC addresses support: 32K or more.	
	VLANs ID: 4K or more and 2K 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 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 long distance across the Rack and Floor virtual chassis or Switch Stacking.	
	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.	
	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, Deficit Weighted Round-Robin(DWRR) or equivalent 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 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 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:**	

	48 nos. of 1G/10G SFP+ 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.	

8 Network Switch 48 Ports (Qty 2)

48 Ports 1G/10G SFP+ and 4 x 40G/100G QSFP28 Uplink ports

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 switching capacity.	
	Forwarding rates: The switch should have 650Mpps forwarding rates.	
	IPv4 Routing entry support : 60K or more.	
	IPv6 Routing entry support : 60K or more.	

	IPv4 and IPv6 Multicast Routes : 4K or more.	
	MAC addresses support: 32K 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 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 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) and Non-Volatile Memory Express (NVMe over Fabrics)	
	The switch should be manageable from cloud and On-premises solution.	
	The switch should support IEEE 802.1X or MAC filterting	
	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.	
	The OEM shall be in Leaders Quadrant of Gartner report for Wired & Wireless LAN Infrastructure for minimum 5 Consecutive Years.	

9 Network Switch(Other side user Connectivity Qty2 48 Port)

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 portsfrom 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.	
	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 16GB DRAM and 32GB Flash.	
	The switch will have at up to 1.7 Tbps switching capacity.	
	Forwarding rates: The switch should have 1000 Mpps forwarding rates.	
	IPv4 Routing entry support : 24K or more.	
	IPv6 Routing entry support : 12K or more.	
	IPv4 and IPv6 Multicast Routes : 4K or more.	
	MAC addresses support: 32K or more.	
	VLANs ID: 4K or more and 1K VLANs simultaneously.	
	ACL /QOS entry support : 4K or more.	
	Packet buffer : 32 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 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 orStacking Performance of minimum 160 Gbps.	
	The Switch should support long distance across the Rack and Floor Switch Virtual chassis or Stacking.	
	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	
	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, Deficit Weighted Round-Robin(DWRR) or equivalent 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 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 or MAC filterting	
	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 filtering , 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) 48 nos. 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.	

10 Cyber Security Suite

NGFW(Next-Generation Firewall)

Sr.No	Minimum Technical Specification	Compliance (Yes/No)
	Make & Model (Specify the model no.)	
1	**Appliances Requirements**	
2	The offered solution should run on a hardened OS and delivered on purposeful built hardware appliance manufactured by offered firewall OEM only.	
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.	
4	The proposed firewall solution must run on purpose-built chassis hardware or proposed firewall solution must be hyper scalable in nature.	
5	The solution must be scalable in nature to support future throughputs requirements without changing the hardware.	
6	The firewall appliance shall support support virtual systems/VDOM /virtual contexts. All virtual domains must work as dedicated firewall with all features.	
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.	
8	Appliance should have 50 Gbps of IPS throughput and scalable to 100 Gbps in near future.	
9	Appliance should have VPN throughput of 20 Gbps from day one and scalable to 40 Gbps in near future.	
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.	
11	The proposed firewall must be built on an open architecture utilizing multi-core CPUs to ensure protection and scalability against evolving security threats.	
12	Appliance should have minimum 64 GB or higher RAM from dayone.	
13	Appliance should have at least 400 GB of SSD storage onboard from dayone	
14	Appliance shall have minimum following ports from day one and expansion slot/fixed ports to support additional ports requirement. - 2 x 40G/100GBASE-F QSFP28 and 8x 10G SFP+ Ports from day one. - Separate & Dedicated 1 x 1G port for out of band management. - Separate & dedicated port for HA connectivity. - Short Range Transceiver must be included from dayone. Additionality support interface required in future. 18x 10/25GbE port or 6x 100GBASE-F QSFP28 ports.	
15	Appliance should have redundant power supply and Fans.	

16	Appliance should support minimum 180k connections per second and scalable to 360K 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.	
18	Appliance should be supplied, installed and configured in high availability for redundancy a) Solution should provide high availability (Active-Active & Active-passive) at gateway level. Appliance failover shall be completed stateful in nature without any manual intervention and should be completely transparent to end-user without any session drops. b) All the features running should provide stateful failover. c) Authentication for adding new HA member should be required. d) Solution should not require any downtime/reboot for failover & backup purpose.	
19	It should be possible to manage appliance including its hardware and networking features over secure channels (https and ssh).	
20	Appliances should be supplied with the support for static and dynamic routing protocols	
21	Solution should provide IPv4 and IPv6 dual stack support from day one. OEM should be IPv6 logo approved. Supporting documents to be submitted.	
22	Solution should support system authentication with Local DB/RADIUS/Microsoft AD. It should have ability to dynamically fall back to the local user database in case of external AAA server outage.	
23	Appliance shall support Link aggregation functionality to group multiple ports as single channel.	
24	The proposed solution should be a purpose built Security Firewall Device and should not have wireless access component within its hardware and software	
25	**Network Protocols/Standards Support Requirements.**	
26	The firewall should have granular application identification technology based upon deep packed inspection.	
27	The Firewall should provide stateful engine support for all common protocols of the TCP/IP Stack.	
28	All internet based application shall be supported for filtering like Telnet, FTP, SMTP, Http, DNS, ICMP, DHCP, RPC, SNMP, Lotus Notes, Ms-Exchange etc.	
29	IPSec. Encryption shall be supported with AES-128 & AES-256 standards.	
30	The Firewall should provide NAT functionality including dynamic and static NAT transitions. Network Address Translation(NAT): a) Network address translation(NAT) shall be supported so that the private IP address of hosts and the structure of an internal network can concealed by the firewall b) Network Address Translation (NAT) shall be configured as 1:1, 1: many, many: 1, many: many flexible NAT (overlapping IPs) c) Reverse NAT Shall be supported. d) Port address translation/ Masquerading shall be supported.	

31	a) The firewall should support internet Protocol Security (IPSec.). b) key exchange with latest internet key Exchange (IKE),public key infrastructure PKI (X.509) shall be catered to. c) Support latest Encryption algorithms including AES 128/192/256 (advanced Encryption standards) 3DES(Data Encryption standard) etc. d) Support Latest Authentication algorithms including SHA-1 (Secure Hash Algorithim-1) SHA-2 (Secure Hash Algorithim-2) etc. e) IPSec NAT traversal shall be supported.	
32	**Firewall Filtering Requirements.**	
33	Solution should be able to configure access policy base on the following parameter: a) Source/Destination IP/Port b) Time and date access c) User/group role (After integration with AD) d) Combination of one or multiple of above mentioned parameter.	
34	Solution should have rich Geo location feature and it should facilitate following Geo Location access policy scenario at least. a) Blocking/allow for all objects based on source/destination Geo location (Source/destination can be defined as specific country, specific continent or entire globe) b) Blocking/allow for specific object (Viz. web server, destination IP etc.) based on source/destination Geo location (source/destination can be defined as specific country, specific continent or entire globe.	
35	Solution should have provision of taking custom feed of IP address and URLs from any publicity/internally hosted web page. It should give flexibility to administrator to utilize this custom feed and block any inbound or outbound traffic to/form custom feed.	
36	It should have following features : a) The firewall should mask the internal network from the external world. b) Multi-layer, stateful, application-inspection-based filtering should be supported. c) it should provide network segmentation reduces with capabilities that facilitate deploying security for various internal, external and DMZ (Demilitarized zone) sub-groups on the network to prevent unauthorized access. d) ingress/egress filtering capabilities shall be provided e) There should be support for detection of reconnaissance attempt such as IP address sweep, port scanning etc. f) Should include basic attack protection features listed below but not limited to: • Maximum no of protection against attacks that exploit weakness in the TCP/IP protocol suite. • it shall enable rapid detection of network attacks • TCP reassembly for fragmented packet protection. • SYN Flood, half open Connections and NULL Packets •Protection against IP spooling • Malformed packet protection. • Java blocking and ActiveX blocking	
37	**QoS(Quality of Service)**	

38	Solution should support the ability to create Qos Policy: • by destination address • by user/user group as defined by AD • by application (such as Skype, Bit torrent, YouTube)	
39	The proposed firewall shall define Qos traffic classes and shall support real-time prioritization of traffic identity Awareness Features	
40	Solution should support identity based control for Granular user, group and machine based visibility and policy enforcement.	
41	Solution should support the identify based logging applicating detection and usage controls.	
42	Solution should provide seamless Ad integration with multiple deployment options like Clientless, Captive Portal or identity Agent.	
43	Should support redundancy High Availability, Load Sharing and clustering.	
44	**Threat Preventions features.**	
45	IPS should be based on the following detection mechanisms exploit signature protocols anomalies, application controls and behavior-based detection.	
46	IPS should be able to detect and prevent the following threats: • Protocol misuse • Malware communications • Tunnelling attempts • Denial of service • Oher generic types without predefined signatures.	
47	IPS should have options to create profiles for either client or server based protections or a combination of both.	
48	IPS should provide at least two pre-defined profiles/Polices that can be used immediately.	
49	IPS updates should have both options of automatic downloads and scheduled update so that it can be scheduled for specific days and time. Updates may be either directly taken using gateway routes or using proxy credentials. It should not require reboot of appliance.	
50	IPS should support network exceptions based on source, destination, service or a combination of either.	
51	IPS should include a troubleshooting mode which sets the in use profile to detect only, without modifying individual protections.	
52	The administrator should be able to automatically activate new protections based on configurable parameters to improve security and performance of network	
53	IPS should be able to collect packed capture for specific protections.	
54	IPS should have Microsoft, Adobe IIS/Apache web Server specific protections	
55	Solution should support more than 15000 (excluding custom signature) IPS signatures or more.	
56	IPS profiles should have an option to create customer's own signature with an open signature than can be activated/de-activities as per customer environment.	
57	IPS should provide details information on each protection, including : Vulnerability and threat descriptions, Threat severity, Release	

	date CVE Reference, Performance Impact Confidence index, Threat severity etc.	
58	IPS should also have an option to create customer's own signatures with an open signature language.	
59	Signatures should have severity level defined to it so that the administrator can understand and decide which signature to enable for what traffic (e.g. for severity level: high medium low.)	
60	Solution should support Granular Application Detection and Usage Control and shall be able to identify, allow block or limit application regardless of port, protocol etc.	
61	Should have more than 8000+ pre-defined distinct application signature (excluding custom application signatures) as application detection mechanism to optimize security effectiveness and should be able to create new application categories for operational efficiency.	
62	Solution should have creation with easy to understand name e.g. Business Applications, instant Messaging File Storage and Sharing Mobile Software, Remote Administration SMS Tools, Search Engine, virtual World, Webmail etc.	
63	Solution should protect from DNS Cache Poisoning and prevents users from a accessing blocked domain addresses.	
64	Solution should support web content filtering up to layer 7 traffic like HTTP, HTTPS, DNS, etc, with Application identification like IM, torrent etc. Allow/Deny traffic based on source/Destination IP/ Networks, Web URLs, Regular expressions, Web plug-ins such as ActiveX, Java Applet & Cookies Regular file extensions, Spy wares and Ad wares.	
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.	
66	The antivirus signature database of proposed solution should comprise of up to date list of signature of virus malwares, spyware etc.	
67	Solution's Antivirus engine should support inspection of at least 50 file type	
68	Solution should be able to detect & prevent & prevent Unique communication patterns used by BOTs i.e. Information about Botnet family	
69	Solution should be able to detect & Prevent attack type such as spam sending click fraud or self-distribution, that are associated with Bots.	
70	The Malware prevention engine of the proposed solution should be able to detect& prevent the Spyware, Ransomware & Adware for pattern based blocking at the gateways.	
71	Solution should be able to discover the Bot infected machine.	
72	The firewall should belong to product family which minimally attains EAL4+ certified. Bidder to submit supporting documents.	
73	Complete license must be quoted with 3 years including Firewall, IPS, Web/Uri Filtering, AntiBot, Application control, Antivirus, Anti-spam, DNS Security, VPN from day one.	
74	Complete Solution must be from same OEM.	

	Administration, Management and logging.	
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.	
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.	
78	Solution must have tracking mechanism for the changes done on policy management dashboard and maintain audit trails.	
79	The Solution shall receive logs for the overall proposed solution in a single system, and shall not be separate for each module of proposed firewalls.	
80	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.	
81	The proposed solution must support the ability to lock configuration while modifying it, avoiding administrator collision when there are multiple people configuring the appliance.	
82	Solution must have the granularity of administrators that works on parallel on same policy without interfering each other.	
83	Solution must be able to install threat related protections and access related rules separately or in a single policy.	
84	Log viewer must have a free text search capability.	
85	Appliance must support minimum 10 appliance from day one.	
	OEM Eligibility Criteria	
87	The firewall should belong to product family which minimally attains EAL4+/NDPP certified. Bidder to submit supporting documents.	
88	Complete Solution must be from same OEM. Whitelabling of product is not allowed.	

EDR (Endpoint Detection and Response)

Sr.No	Minimum Technical Specification	Compliance (Yes/No)
1	The solutions should have all its components deployed on premise and in Air-gapped environment.	
2	The Solutions should provide a web-based console for all functionalities and should allow administrators to access the management interface from any authorised machine, without installing additional software.	
3	The solution should support a multi-tenancy architecture, enabling site-wise distributed management consoles while ensuring all operations roll back to the primary management console.	
4	The solution architecture should be scalable and support a Master-Slave framework, where the multiple slave servers handle the endpoint load while ensuring centralized management and full visibility through the master management console.	

5	The solution should offer the native data lake for stroing and processing the telemetry. It should also offer native threat hunting capabilities on the native data lake	
6	The solution should not offer and rely on any 3rd party solutions for the data lake for the telemetry processing and storing the same.	
7	The solution should provide number of customizable dashboards to provide insights into systems activity and analytical results, including: system health and activity, queue lengths, events registered, their status and the technologies used to provide verdicts, lists of the IPs, domains, and emails most frequently related to incidents	
8	The Endpoint Detection and Response (EDR) capabilities must be available for Windows, Linux, and macOS.	
	The solution should support EDR for workstation and server OS'es architecture	
Functional Requirements		
9	The solution must offer Endpoint Protection (EPP) and Endpoint Detection & Response (EDR) capabilities within a single agent provided by the same OEM. Additionally, the following security features must also be available.	
9.1	Anti Malware(Signature based and Signature less)	
9.2	Device Control	
9.3	Application Control	
9.4	Web Protection	
9.5	Drive Encryption	
9.6	File/Folder Encryption	
9.7	Removable drive encryption	
9.8	Web Access control(Category based URL blocking and Wildcard)	
9.9	Vulnerability Assessment	
9.1	Patch Management	
9.11	Hardware and Software Inventory Management	
9.12	Root Cause Analysis	
9.13	Threat Hunting	
9.14	Endpoint Firewall	
10	The proposed Solutions should provide context-aware endpoint investigation and response (EDR), recording and detailed reporting of system-level activities to allow threat analysts to rapidly assess the nature and extent of an attack. The Solutions must have feature for Custom detection, intelligence, and controls.	
11	The product should have capability to stream all endpoint activity data including but not limited to telemetry data like process created, command lines, modules loaded, registry, Behavioral Indicators, Login activity, DNS, URL, Command Scripts, Driver Load, DLL Module Load, Named Pipes & file changes etc.	
12	The solution should provide an option to obtain a list of files stored in a specified folder on an endpoint, list of processes running on a	

	given endpoint, process memory dump, full memory dump, disk image, registry keys, NTFS metafiles and autorun points list.	
13	The solution must be flexible to add custom indicators of compromise (IOC) and indicators of attack (IOA) rules for classifying and analysing events.	
14	EDR Solution should provide the ability to execute YARA scans on endpoints for identification of malicious files	
15	Antivirus detections should also enrich endpoint telemetry for improved visibility and must be easily searchable by analysts on the same management console	
16	The solution must provide a comprehensive threat hunting UI to build multi-level hunting queries with AND & OR operands	
17	Solutions should have ability to disable agent via the management console for temporary troubleshooting or testing.	
18	The Solutions should have capability to uninstall the agent remotely from the management console.	
19	Solutions should be able to publish customized alert messages on managed endpoints.	
20	The proposed solution must be able to detect existing vulnerabilities in operating systems and in other installed applications, and then analyst to respond by automatically downloading/pushing the necessary patches to endpoints.	
21	The proposed solution must be able to block the use of USB storage devices and allow access only to permitted devices, and allow read/write access only by authorized users, to reduce data theft and enforce lock policies.	
22	The proposed solution must be able to log the file operations (Write and Delete) on USB storage devices.	
23	The proposed solution should include features to manage computers remotely, including: · Remote installation of third-party software · Manage the hardware and software inventory of the assets · Monitoring for the installation of unauthorized software	
24	The proposed solution should include an integrated feature for remote desktop access, enabling secure connection to client machines for performing incident response tasks and administrative activities. Additionally, it should have the capability to log all activities conducted during such sessions for accountability and auditing purposes.	
25	The proposed solution must have the ability to allow and block applications based on their digital signature certificates, MD5, SHA256, File Path, and pre-defined application security categories.	
26	The proposed solution must support the blocking of prohibited (Deny-List) applications from being launched on the endpoint, and the blocking of all applications other than those included in Allow-Lists.	
27	The solution should support rogue device identification on the network by scanning it and deploying the security agent wherever feasible.	
28	The proposed solution must have ability to block/allow user access to web resources based on websites, content type, user and time of day.	

29	The proposed solution must prevent the connection of reprogrammed USB devices such as emulating keyboards, and enable control of the use of onscreen keyboards for authorization.	
30	The proposed solution must provide Anti-Bridging functionality for Windows workstations to prevent unauthorized bridges to the internal network that bypass perimeter protection tools. Administrators should be able to ban the establishment of simultaneous wired, Wi-Fi, and modem connections.	
31	The proposed solution must enforce user-based policies for Device, Web and Application Control.	
32	The proposed solution should specifically allow the blocking of the following devices:	
	· Bluetooth	
	· Mobile devices	
	· External modems	
	· CD/DVDs	
	· Cameras and Scanners	
	· MTPs	
	· And the transfer of data to mobile devices	
33	The proposed solution must include a built-in tool to perform remote diagnostics and collect troubleshooting logs without requiring physical access to the computer.	
34	The solution should provide on-premises, native sandboxing capabilities which should be integrated with the endpoint for suspicious files submission to identify the zero day attacks.	
35	The integrated sandbox must have ability to provide the following information to analyst	
35.1	· Comprehensive Host Modification Report available after execution in VM	
35.2	· Copy of malware binary(s)	
35.3	· network metadata identifying the locations to which the malware attempts to communicate	
35.4	· Importance information	
35.5	· screenshots of the desktop activity	
36	The sandbox must be able to simulate end user actions in order to force the execution of malware that rely on triggers from the end user, like a mouse click for a better analysis of the malware objects.	
37	The proposed solution should be able to provide the below contextual information to analysts after execution of suspicious samples in sandbox VM 1) Suspicious activity list in execution order once sample executed in the VM and it should be mapped to MITRE ATT&CK matrix 2) Suspicious activity list also show the criticality of the executed events 3) Graphical visulization of the activity tree which should be interactive and intiutive to assist analyst in investigation	
38	The suggested solution must support to roll back the changes done by the identified malware binaries respone	

39	The suggested solution must support at least the following response actions that an administrator can perform when threats are detected:	
39.1	Prevent object execution	
39.2	Host isolation.	
39.3	Get File	
39.4	Delete object from host or group of hosts.	
39.5	Terminate a process on the device.	
39.6	Quarantine an object	
39.7	Run system scan	
39.8	Remote program / process / command execution	
39.9	Start IoC scan for a group of hosts.	
40	Alerts and events from endpoint sensors should enrich with the MITRE ATT&CK Matrix	
41	Solution must provide an option to store endpoint telemetry data for a necessary period of time . Local storage must be extendable if required to accommodate data.	

HIPS (Host Intrusion Prevention System) Workstations

Sr.No	Minimum Technical Specification	Compliance (Yes/No)
1	The solution should support the installation of the management server on both Windows and Linux server OS.	
2	The solution should have all its components deployed on premise and in Air-gapped environment.	
3	The Solution should provide a web-based console for all functionalities and should allow administrators to access the management interface from any authorised machine, without installing additional software.	
4	The solution should support a multi-tenancy architecture, enabling site-wise distributed management consoles while ensuring all operations roll back to the primary management console.	
8	The proposed solution must provide for the centralized installation, update and removal of anti-malware software, together with centralized configuration, administration, and the viewing of reports and statistical information about its operation.	
9	The proposed solution must feature the centralized removal (manual and automatic) of incompatible applications from the administration center.	
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.	
11	The proposed solution must be able to generate graphical reports for anti-malware software events, and data about the hardware and software inventory, licensing and must be able to export of reports to PDF and XML files while allowing the admin to create custom reports.	

12	The proposed solution's management server must maintain a revision history of the policies, tasks, packages, management groups created, so that modifications to a particular policy/task can be reviewed.	
13	The proposed solution must have the ability to perform inventory scan to generate application inventories on installed applications, scripts and .dll files.	
14	The proposed solution must have the ability to tag/mark computers based on and later that tags can be used to enforce policies.	
	Network Attributes(Name, Domain and/or Domain Suffix, IP address)	
	Location in Active Directory(Organizational Unit,Group)	
	Operating System(Type and Version, Architecture, Service Pack number)	
	Application registry(Application name, Version, Manufactorer)	
15	The proposed solution must allow the administrator to define restricted settings in policy/profile settings, so that a virus scan task can be triggered automatically when a certain number of viruses are detected over defined amount of time. The values for the number of viruses and timescale must be configurable.	
16	The proposed solution must have a built-in feature/module to remotely collect the data needed for troubleshooting from the endpoints, without requiring physical access.	
17	The proposed solution should support the installation of endpoint protection on servers without the need to restart.	
18	The proposed solution must include Role Based Access Control (RBAC) with customizable predefined roles.	
19	The proposed solution must support Single Sign On (SSO) using NTLM and Kerberos.	
20	The proposed solution must support sending notifications by email and SMS	
Functional Requirements		
21	The solution must offer Server protection, HIPS, Device Control, Web Control, File integrity Monitoring & Control , Log Inspection, Firewall capabilities within a single agent provided by the same OEM.	
22	The proposed solution must be able to detect following types of threat: Viruses (including polymorphic), Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, Phishing sites and links, Zero-Day Vulnerabilities and other malicious and unwanted software.	
23	Suggested solution must have heuristic analyser to detect and block previously unknown malware.	
24	Suggested solution must support ability to determine anomalous behavior by an application by analyzing its execution sequence. Ability to roll back malware operations during treatment.	
25	Suggested solution must support ability to restrict the privileges of executable programs such as writing to the registry or accessing files and folders.	
26	Suggested solution must allow administrators an ability to scan powered-off virtual machines (without bringing them online).	

27	The solution must allow administrators to specify different actions for threats found in powered on and powered-off virtual machines	
28	Suggested solution must be able to scan powered off Linux virtual machines with the following file systems: EXT2, EXT3, EXT4, XFS, BTRFS.	
29	Suggested solution must perform anti-malware scanning and other resource-intensive tasks on a dedicated secure virtual machine rather than on guest virtual machines.	
30	The solution should offer application control rules to block the installation and/or running of a program. The component should be able to control the application via program path, hash(SHA256), certificate and predefined categories of applications provided by the vendor.	
31	Application control for Windows Servers must have both whitelist and blacklist logic.	
32	Suggested solution must support application privilege control that logs activity of applications in the operating system of the protected virtual machine and regulates application activity depending on the group to which the application was assigned.	
33	Suggested solution must support automatic exploit prevention that can blocks the exploitation of application vulnerabilities commonly used by cyber-criminals, dramatically increasing the overall level of protection.	
34	Suggested solution must support built-in web protection, which detects and blocks malicious URLs.	
35	Suggested solution must support protection of shared folders from remote encryption.	
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.	
37	Suggested solution should be able to scan boot sectors, system memory, Kernel Memory Scanning, and startup objects in Linux Operating system.	
38	The solution must include File Integrity Monitoring (FIM) to ensure the integrity of system files, logs, and critical applications. It should continuously monitor files and directories for unauthorized changes to their contents or attributes, detect and respond to such changes, and block any unauthorized modifications.	
39	Suggested solution must protect files in local directories with network access by SMB/NFS protocols from remote malicious encryption.	
40	The proposed solution must provide Memory Scanning for Windows workstations.	
41	The proposed solution must support the following security features:	
	· Manual Scanning	
	· On-Access Scanning	
	· On-Demand Scanning	
	· Compressed File Scanning	
	· Scan Individual File, Folder and Drive	
	· Script Blocking and Scanning	
	· Registry Guard	

	· Buffer Overflow Protection	
	· Background/Idle Scanning	
	· Removable Drive Scanning on connection with system	
42	The proposed solution should be password-protected to prevent the AV process being halted/killed and for self-protection, regardless of the user authorization level on the system.	
43	The proposed solution must include a personal firewall capable, as an absolute minimum, of:	
	· Blocking network activities of applications based on their categorization.	
	· Blocking/allowing specific packets, protocols, IP addresses, ports and traffic direction.	
	The automatic and manual addition of network subnets, and modification of network activity permissions.	
44	The proposed solution must prevent the connection of reprogrammed USB devices emulating keyboards, and enable control of the use of onscreen keyboards for authorization.	
45	The proposed solution must have local storage on endpoints to keep copies of files that have been deleted or modified during disinfection. These files must be stored in a specific format that ensures they cannot pose any threat.	
46	The proposed solution must include protection against attacks that exploit vulnerabilities in the ARP protocol in order to spoof the device MAC address.	
47	The solution should implement Forced Data Execution Prevention (DEP) to block arbitrary code execution in non-executable memory regions. This prevents attackers from injecting and executing shellcode in a protected allocation space.	
48	The solution should include Structured Exception Handler Overwrite Protection (SEHOP) to prevent attackers from overwriting Structured Exception Handlers (SEH), mitigating the risk of exception hijacking.	
49	The solution should block LoadLibrary Network Call execution (Anti ROP) to prevent dynamic libraries from being loaded from untrusted network locations, reducing the risk of remote DLL injection.	
50	The solution should implement Simple Export Address Table Access Monitoring to protect against unauthorized read access to system-critical export address tables in kernel32.dll, kernelbase.dll, and ntdll.dll. This protection mitigates API hooking and function redirection attempts by attackers.	
51	The solution should prevent Heap Spray Allocation to block attackers from injecting shellcode at predictable memory locations, a common technique used to exploit browser vulnerabilities and other applications.	
52	The solution should support Execution Flow Simulation (Anti ROP) to detect and neutralize RET chain instructions in critical Windows API components such as CreateProcess and CreateThread, preventing attackers from chaining gadgets to execute malicious payloads.	
53	The solution should enforce Attack Surface Reduction (ASR) mechanisms to limit the exposure of vulnerable modules, APIs, and processes. This reduces the overall attack surface by blocking	

	the execution of scripts, macros, and untrusted processes that could be exploited.	
54	Suggested solution for must support log inspection that monitors the integrity of the protected environment based on the results of an inspection of Windows event logs.	
55	The proposed solution should have the ability to prioritize custom and on-demand scanning tasks for Linux workstations.	
56	The proposed solution should include the functionality to isolate infected computers.	
57	The proposed solution must be able to log file operations (Write and Delete) on USB storage devices.	
58	The proposed solution must have ability to block/allow user access to web resources based on websites, content type, user and time of day.	
59	The proposed solution should specifically allow the blocking of the following devices:	
	· Bluetooth	
	· Mobile devices	
	· External modems	
	· CD/DVDs	
	· Cameras and Scanners	
	· MTPs	
	the transfer of data to mobile devices. And ability to create a list of trusted devices by their ID and the ability to grant privileges to use external devices to specific AD users.	
60	The proposed solution must have ability to manage user access rights for Read and Write operations on CDs/DVDs, removable storage devices and MTP devices.	
61	The proposed solution must have the ability to restrict application activities within the system according to the trust level assigned to the application, and to limit the rights of applications to access certain resources, including system and user files.	
62	The proposed solution must provide protection against hacker attacks by using a firewall with an intrusion detection and prevention system (IDS/IPS) and network activity rules for more popular applications when working in computer networks of any type.	
63	The proposed solution must include the antivirus checking and disinfection of files that have been packed using programs like PKLITE, LZEXE, DIET, EXEPACK, etc.	
64	The proposed solution must include the anti-malware checking and disinfection of files in archives using the RAR, ARJ, ZIP, CAB, LHA, JAR, ICE formats, including password-protected files.	

Storage Security

Sr.No	Minimum Technical Specification	Compliance (Yes/No)

1	The Storage security solution should include robust anti-malware protection to defend against viruses, ransomware, and other malicious threats targeting storage systems.	
2	The Storage security solution should support centralized management, monitoring, and updates to allow administrators to oversee security policies, monitor threats, and deploy updates from a unified console.	
3	The Storage security solution should provide protection for NAS and file servers to ensure the security of network-attached storage (NAS) devices and file servers against malware infections.	
4	The Storage security solution should allow regular updates for anti-malware databases and network attack patterns to keep security definitions up to date and effectively detect and respond to emerging threats.	
5	The Storage security solution should ensure protection of shared folders from crypto-malware to prevent ransomware attacks and unauthorized encryption of critical shared files and directories.	
Requirements for file server security solution		
6	The security solution for file servers should implement the following functionality:	
6.1	Protection against malware in real time and during scheduled scanning	
6.2	Cloud-based protection against new threats, allowing the application to contact the security vendor’s specialized resources for a file verdict during real-time or scheduled scanning	
6.3	On-demand (manual) scanning of selected file servers	
6.4	Scanning selected files, folders or the whole system	
6.5	Prevent re-scanning of files	
6.6	Blocking, neutralization and removal of malware, notification of administrators	
6.7	Single management console for all protection components	
6.8	Ability to exclude files with a specific name, files located at a specific address and files with a specific mask from protection	
6.9	Ability to export/import a list of exceptions	
6.1O	List of frequent exceptions compiled in accordance with Microsoft recommendations	
6.11	Storage of backup copies of deleted files	
6.12	Support for activation using an activation code provided via subscription	
6.13	Provide information on number of objects scanned	
6.14	Provide information on antivirus database details	
6.15	Import or export the list of scan and protection exclusions in scan tasks and protection profiles	
6.16	Special protection against file-encrypting malware for shared network resources, providing reliable defenses against ransomware.	
Requirements for NAS security solution		
7	The security solution should support integration with the following network attached storages:	
7.1	NetApp® running under one of the following systems: Data ONTAP® 7.x and Data ONTAP 8.x 7-mode,Data ONTAP® 8.x and 9.x Cluster-mode	

7.2	EMC™ Celerra™ / VNX™ with the following software: Operating system EMC DART 6.0.36 or later,	
7.3	Celerra Anti Virus Agent (CAVA) 4.5.2.3 or later,EMC Isilon™ running under OneFS™ 7.0 operating system or later	
7.4	Hitachi NAS installed on one of the following platforms: HNAS 3080 / 3090 / 4040 / 4060 / 4080 / 4100, VSP G200 / G400 / G600 / G800 / G1000 / G1500.	
7.5	IBM® NAS of IBM System Storage® N series	
7.6	Oracle® NAS Systems of the Oracle ZFS Storage Appliance family	
7.7	Dell Compellent™ FS8600 on FluidFS 6.x	
7.8	Dell Compellent™ FS8600 on FluidFS 5.x	
7.9	HPE 3PAR StoreServ File Controller on File Persona 3.3.1	
7.1O	HPE 3PAR StoreServ 7000c, 8000, 9000, 20000 Storage on File Persona 3.3.1	
8	The security solution for NAS should implement the following functionality:	
8.1	Protection against malware in real time and during scheduled scanning	
8.2	Cloud-based protection against new threats, allowing the application to contact the security vendor’s specialized resources for a file verdict during real-time or scheduled scanning	
8.3	Scanning selected files, folders or the whole system	
8.4	On-schedule scanning of all NAS	
8.5	On-demand (manual) scanning of selected NAS	
8.6	Scanning selected files, folders or the whole system	
8.7	Prevent re-scanning of files	
8.8	Blocking, neutralization and removal of malware, notification of administrators	
8.9	A single management console for all protection components	
8.1O	Detailed information about events on NAS and the implementation of tasks	
8.11	Ability to apply different security settings for different NAS	
8.12	Ability to exclude files with a specific name, files located at a specific address and files with a specific mask from protection	
8.13	Ability to export/import a list of exceptions	
8.14	List of frequent exceptions compiled in accordance with Microsoft recommendations	
8.15	Storage of backup copies of deleted files	
8.16	Support for a licensing scheme according to the number of protected users and according to the number of security servers	
8.17	Support for activation using an activation code provided via subscription	
8.18	Provide information on number of objects scanned	
8.19	Provide information on anti-virus database details	
8.2O	Import or export the list of scan and protection exclusions in scan tasks and protection profiles.	
Requirements for anti-malware database update mechanisms		
9	Updatable anti-malware databases should implement the following functionality:	

9.1	Multiple methods of updating, including global communication channels, shared resources on local network and removable media.	
9.2	Verification of the integrity and authenticity of updates by means of electronic digital signature.	

SIEM (Security Information and Event Management)

Sr.No	Minimum Technical Specification	Compliance (Yes/No)
1	SIEM Must be three tier Architecture with physical segregation of duties consisting of Collection layer, Log Management layer and Correlation layer as physical appliance form factor or HW	
2	SIEM must be Hardware or Sotware applicance consisting of end to end every component from bidder and must be sized for 5000 Sustained EPS/ 10000 Peak EPS or equivalent GB per day (1 EPS = 500 Bytes) and must not drop or que any logs up to peak limit	
3	The solution must support horizontal scaling of its key components: collector, correlator and event storage, without the need to purchase additional software licenses.	
4	The solution components must support installation in distributed and isolated networks without the need for Internet access.	
5	The solution must provide centralized management via a web console without the need to install additional software on the administrator's workstation.	
6	The solution must support multi-tenancy.	
7	The solution must support granular access control to events at the space level, allowing administrators to restrict user access to specific events within a tenant.	
8	The solution must support centralized configuration updates or component reboots, including forced reboots.	
9	The solution must support flexible configuration of event routing between components.	
10	The solution must provide a fault-tolerant cluster mode of operation for all components with hot-switching (high availability).	
11	The solution must support operation with multiple independent event storage clusters to enable flexible schemes of geographically distributed systems.	
12	The solution must support deployments in a geographically distributed infrastructure, with the ability to send events from remote offices to central correlators.	
13	The solution must support searching for events in remote offices from the central hub of the system.	
14	The solution must provide a RESTful API for asset management, active lists, work with registered base and correlation events: search, get context information on base and correlation events, manage processing status.	
15	The solution must support automatic updates of normalization and correlation rules issued by the vendor. The possibility of revision of changes by the operator after receiving notification of new available resources must be implemented. The system must support updates	

	without direct access to the Internet using the "update mirror" mechanism.	
16	The solution must support the ability to write the log of the installation process to a file.	
Requirements for event collection, analysis and storage		
17	The solution must provide both active and passive collection of events from data sources.	
18	The solution must provide a unified data model.	
19	The solution must support the following log formats (i.e. normalizers, parsers) 'out-of-the-box':	
	• JSON	
	• CEF (Common Event Format)	
	• Regexp (Regular Expression)	
	• Syslog (as per RFC3164 and RFC5424)	
	• CSV (with custom delimiter)	
	• Key-value	
	• XML	
	• NetFlow v5	
	• NetFlow v9	
	• Sflow5	
	• Ipfix(v10)	
20	The solution must support the following log transport mechanisms (i.e. connectors) 'out-of-the-box':	
	• Internal	
	• TCP	
	• UDP	
	• Netflow	
	• Sflow	
	• NATS-jetstream	
	• Kafka	
	• HTTP	
	• SQL (MSSQL, MySQL, PostgreSQL, Cockroach_DB, SQLite3, Oracle, Firebird)	
	• File	
	• 1C-log	
	• 1C-xml	
	• Diode	
	• FTP	
	• NFS	
	• WMI (remote Windows Event Log collection)	
	• WEC (local Windows Event Log collection)	
	• SNMP	
	• SNMP-trap	
	• Vmware	
	• Elastic	
	• ETW	

21	The solution must support bulk deletion of multiple assets and resources.	
22	The solution must support tracking and warning of concurrent resource edits by multiple users.	
23	The solution must provide a central interface for managing the list of event collectors.	
24	The solution must support optional raw event storage. The settings must allow both unconditional saving of the event and saving only in case of event parsing errors.	
25	The solution must support the ability to add custom event source types and configure parsing and normalization rules accordingly.	
26	The solution must support the creation of custom parsers based on supported data collection formats and protocols.	
27	The solution must provide the ability to write normalization rules from the system web interface to parse events, including using regular expressions, and the ability to check the syntax of their writing using the example of the source event.	
28	The solution must support receiving events in Syslog, CEF formats without additional parsing (normalization) settings.	
29	The solution must support the ability to create custom fields to implement arbitrary custom taxonomies. It must be possible to create fields of the following types:	
	• String	
	• Numeric	
	• Floating point	
	• String Array	
	• Array of numbers	
	• Floating point array	
30	The solution must provide ipHexToDotted and ipDecimalToDotted mutations.	
31	The solution must support the ability to perform sequential hierarchical parsing (normalization) of events.	
32	The solution must have an event collection component (collector) that provides buffering of events on the local disk in the event of temporary unavailability of event receivers, as well as automatic forwarding of buffered events when the connection is restored. The buffer size for storing events must be configurable.	
33	The solution must support the ability to monitor the receipt of events from sources with tracking of the number of events in a specified time period and automatic email notification in the event of deviation from specified monitoring parameters for each of the sources in particular.	
34	The solution must support the separation of event storage levels ("hot" and "cold" levels). Events must be equally available in all storage levels. The parameters of the storage periods must be defined by the user in the graphical interface of the system.	
35	The solution must support event storage periods by days, gigabytes, or percentage of disk space.	
36	The solution must support the ability to offload events to a long-term storage archive.	
37	The solution must support the logical division of the total storage volume into groups with different event retention periods and the ability to distribute events to these groups according to user filters.	

38	The solution must support the ability to search the event database based on an arbitrary search of the event database using the query builder.	
39	The solution must support the ability to search the event database based on a SQL-like query language with the ability to perform grouping and calculation operations.	
40	The solution must support the ability to save the search history.	
41	The solution must support query organization through folders, allowing for quick navigation and editing of queries	
42	The solution must support the ability to export selected events in TSV format.	
43	The solution must support the ability to output field statistics on the event database.	
44	The solution must support import/export of content and resources: correlation rules, parsers, connectors, etc.	
45	The solution must support building a resource dependency graph, allowing analysts to customize the display of resource types and export the graph in SVG format	
46	The solution must support adding arbitrary tags to resources and searching by tags to quickly find related filters, dictionaries, and rules.	
47	The solution must support full-text search of resources, services and content allowing analysts to search by name and/or attribute.	
48	The solution must support the ability to collect events of different formats by a single collector	
49	The solution must have agent capable of reading multiple text log files and assign each a specific name.	
50	The solution must have agent capable of reading text file logs.	
51	The solution must support advanced DNS log collection.	
52	The solution must support an administrator-configurable method for determining event sources.	
53	The solution must support the ability to handle multi-line auditd events.	
Event enrichment requirements		
54	The solution must support event enrichment both at the collectors (at the event collection and processing stage) and at the correlator (to enrich correlated events).	
55	The solution must support the ability to perform event-specific enrichment on an analyst's query to an online reputation service. The query must be performed on domains, web addresses, IP addresses and file hashes, and enriched with information about dangerous and malicious as well as legitimate objects.	
56	The solution must support the ability to enrich events containing IP addresses with geographic data based on downloaded geodata lists.	
57	The solution must provide native threat intelligence feeds. These feeds should be backed by dedicated expert research teams to ensure the delivery of up-to-date intelligence, enriching security events with relevant threat context.	
58	The solution must include native intelligence feeds including Malicious URL, Malicious IP and Malicious URL, supported by expert research capabilities. This expertise should be evidenced by	

	the publication of at least 200+ comprehensive threat research reports, with a focus on sophisticated APT campaigns.	
59	The solution must support the use of geodata obtained from MaxMind and IP2Location services.	
60	The solution must support the creation of custom event enrichment dictionaries and the ability to populate them via web interface and/or API.	
61	The solution must support the ability to enrich events with information about the time offset of the event source relative to Coordinated Universal Time (UTC).	
62	The solution must support the following event enrichment mechanisms and sources:	
	• Threat intelligence data feeds.	
	• Threat intelligence lookup services.	
	• Information about assets and infrastructure.	
	• Information about software vulnerabilities and software installed on endpoints.	
	• Information about users (accounts) from Microsoft® Active Directory.	
	• Information about FQDN or IP from DNS system.	
	• Information from user-created dictionaries.	
	• Information from user-created templates.	
	• Information from user-created variables.	
	• IP address geodata information	
63	The solution should also use a purpose-built Threat Intelligence Platform designed to aggregate, deduplicate, normalize, and store multiple incoming threat intelligence feeds and detection events for efficient analysis and response.	
64	The solution should provide a single, unified console for managing both SIEM and Threat Intelligence Platform functionalities, ensuring streamlined visibility and operational efficiency.	
65	The solution should support real-time correlation of threat intelligence data with events from the SIEM to identify malicious activity and support timely detection and response to cyber threats.	
66	The solution should support ingestion of threat data feeds in widely used formats including JSON, STIX, MISP, XML, CSV, E-Mail, and PDF, using standard protocols like HTTP(S), FTP(S), and TAXII.	
67	The solution should support integration of both proprietary and open-source threat intelligence feeds.	
68	The solution should support advanced filtering of both threat intelligence feeds and incoming log events using criteria such as threat type, geolocation, popularity, timestamps, and other contextual attributes.	
69	The solution should support a centralized database of indicators enriched with full-text search and advanced query capabilities, enabling complex searches across all metadata fields, including those tied to intelligence context.	
70	The solution should support detailed, deduplicated indicator views with information aggregated from multiple threat intelligence sources, along with analyst collaboration features like comments and internal annotations.	

71	The solution should support exporting sets of indicators (e.g., blocklists) in standardized formats like CSV for integration with other security controls.	
72	The solution should support historical correlation (retrospective analysis) to identify previously undetected threats using updated threat intelligence against past events.	
73	The solution should support measurement of threat feed effectiveness through detailed usage statistics, including overlap matrices and performance metrics per feed provider.	
Event correlation requirements		
74	The system must provide streaming correlation of events in near real-time.	
75	The correlation component must support the use of Active List / Reference Set in correlation rules.	
76	Active lists must support the following operations:	
	• Creation and deletion of lists by the user via the UI;	
	• Existence checking, adding, modifying and deleting rows as a result of correlation rules;	
	• Import and export lists in spreadsheet format;	
	• Support for customizable time to live (TTL) for records in active lists;	
	• Support for changing the set of columns without recreating the active list.	
77	The solution must come with a set of predefined correlation rules created based on research of current threats and attack methods developed on the basis of the MITRE ATTACK matrix;	
78	The solution must support the ability to create custom correlation rules. It must be possible to write filter conditions and correlation rules in the form of code, as well as in a graphical editor.	
79	The solution must support the ability to test correlation rules on historical data without installing additional modules.	
80	The solution must show not used correlation rules (not linked to the existing correlator)	
81	The solution must support configuring exclusions for correlation rules in the alert management interface, allowing operators to add field values to exclusions for false positives	
82	The solution must support multi-level application of correlation rules, when the results of triggering of one correlation rule are sources for the following correlation rules.	
	Correlation rules in the system must support:	
	• Correlation by quantitative characteristic;	
	• Correlation by event sequence;	
	• Event fragment selection operations (substring, regexp, etc.);	
	• Automatic notification when a correlation rule is triggered;	
	• Correlation by global and local variables.	
83	The solution must support a converter that can translate Sigma rules into filter selectors, event search SQL queries, or correlation rules.	
84	The solution must automatically prioritize the information security threats identified, both in terms of the level of criticality of the correlation rule and in terms of the criticality and number of information assets affected.	

85	The solution must provide the ability to write correlation rules considering the asset group.	
86	The solution must support automatic aggregation of correlated events according to flexibly customizable user filters.	
87	Global correlation variables must operate within the correlator on which they are declared and, when used in correlation rules, must be able to take different values within each correlation rule (selector) triggering condition.	
88	Local correlation variables must operate only within the correlation rule and the correlation rule (selector) triggering condition in which they are declared.	
	Correlation variables must support the following functions:	
	• Retrieve information from the active worksheet about a value in a specified column;	
	• Retrieve information about the value in a specified dictionary column;	
	• Return the number of characters in a string;	
	• Convert the characters in the string to lower case;	
	• Convert the characters in a string to upper case;	
	• Add characters to the end of a line;	
	• Add characters to the beginning of a string;	
	• Return a substring from a string using the coordinates of the start and end of the substring;	
	• Delete specified characters/substrings from the beginning and/or end of a string;	
	• Replacing all occurrences of string A with string B in the string	
	• Replacing all occurrences of string A with string B in the string;	
	• Replacing the sequence of characters in the string that matches the regular expression with the sequence of characters and capture groups of the regular expression;	
	• Obtaining a result from the original string that satisfies the regular expression condition;	
	• Obtaining a timestamp in epoch format;	
	• Obtaining atomic representations of time (as year, month, day, hour, minute, second, day of week) from fields and variables with time in epoch format;	
	• Convert time from RFC3339 format to epoch format and vice versa;	
	• Rounding time in epoch format (to seconds/minutes/hours/day);	
	• Obtaining the time interval between two-time stamps in epoch format (in seconds/minutes/hours/days);	
	• Basic mathematical operations:	
	o Addition;	
	o Subtraction;	
	o Multiplication;	
	o Division;	
	o Division by modulo;	
	o Rounding a number (up/down);	
	o Getting	
89	The solution must support writing the conditions of correlation rules in the form of code.	

90	The solution must support a mechanism to visualize the coverage of the MITRE ATT&CK matrix with correlation rules in the SIEM system.	
91	The solution must support the ability to convert the original field using the information entropy calculation function.	
Asset Information Management Requirements		
92	The solution must collect and automatically update the following information asset inventory information and store it in a built-in database:	
	• IP	
	• MAC	
	• FQDN	
	• List of installed software	
	• Current software vulnerability information	
	• Hardware information	
	• CII category	
	• Date of last security update	
	• Status of security software installed on the asset	
93	The solution must provide the ability to add custom fields to the asset card;	
94	The solution must support the following mechanisms for populating and updating the embedded information asset base:	
	• Automatic collection and updating of information through integration with the management server of endpoint protection tools;	
	• Automatic collection and updating of information through integration with the industrial/technical network protection tool;	
	• Manually adding asset and vulnerability information reports from the vulnerability scanner. o Manually adding or editing asset and vulnerability information reports;	
	• Manually add or edit asset information via the system GUI;	
	• Import assets via the REST API.	
95	The solution must support the creation of user groups (categories) of assets;	
96	The solution must provide the ability to automatically categorize assets based on one or a combination of attributes: OS, IP address, FQDN, CVE ID, AI risk score and OS version.	
97	The solution must support logical operators AND, OR, NOT, as well as their grouping when setting conditions for automatic asset categorization	
98	The solution must provide the ability to test the specified conditions against the existing database of information assets when setting conditions for automatic asset categorization	
99	The solution must support the ability to search for assets stored in the built-in database.	
100	The solution must support the asset audit function and track the following events:	
	• An asset is added to the system;	
	• Change in asset parameters (name, IP address, MAC address, FQDN, OS);	
	• Removal of an asset from the system;	
	• Adding vulnerability information to the asset;	

	• Delete/modify the asset's vulnerability information;	
	• Change (add/remove) the asset's category.	
Requirements for Incident Handling Functions		
101	The solution must provide for the generation of a detection event map.	
102	The incident card must support the following capabilities:	
	• Change the incident priority;	
	• Assigning the incident to a selected analyst;	
	• Navigate to related base events from the incident map;	
	• Automatic logging of status changes and card actions taken;	
	• Display information assets, users associated with the incident and available contextual information about them;	
	• Highlight information about assets and users associated with the discovery event with their value;	
	• Manually link additional events to analyze the cause of the incident.	
103	The solution must support the ability to combine multiple correlation events into a single incident, both manually and automatically: based on the time range of correlation event generation, based on user account.	
104	The solution must support the ability to manually associate additional information with an incident - by user, asset, correlation event with the ability to categorize the incident.	
Visualization and reporting requirements		
105	The solution must provide visualization (dashboards) and reporting tools for the following objects	
	• Events;	
	• Alerts	
	• Incidents	
	• Assets;	
	• Event Sources;	
	• Active lists.	
106	The solution must come with a pre-installed set of graphical dashboards and reports.	
107	The solution must support the ability to create custom templates and rules for event and incident notifications.	
108	The solution must allow the following incident data to be displayed in graphical form (dashboards):	
	• Incidents created;	
	• Closed incidents for the period;	
	• Incidents not closed by criticality;	
	• Distribution of incidents;	
	• Incidents by level of criticality;	
	• Assets and asset groups affected;	
	• Sources of events with the highest number of incidents;	
	• Correlation rules with the highest number of incidents;	
	• Distribution of incidents by tenant (with comparison to previous period);	
	• Distribution of incidents by time of discovery (first seen);	

	• Distribution of the number of assets affected by incidents by tenant.	
109	The solution must provide dashboard display of the following event data:	
	• Common internal IP addresses in Netflow;	
	• Common external IP addresses in Netflow;	
	• Statistics on traffic volumes in relation to ports;	
	• Statistics on sources with the largest number of events.	
110	The solution must support the creation of custom dashboards and report templates.	
111	The solution must support the creation of dashboards based on user queries to the event repository.	
112	The solution must support the creation and customization of dashboards entirely in a graphical interface.	
113	The solution must provide the ability to generate reports from available templates:	
	• by source;	
	• by incident.	
114	The solution must provide incident reports with the following information:	
	• the number of active incidents;	
	• number of unallocated incidents;	
	• distributed incidents by time;	
	• recent incidents by time;	
	• number of incidents distributed by criticality level;	
	• number of incidents by performer;	
	• number of incidents categorized by status;	
	• affected assets and asset groups;	
	• sources of events with the highest number of incidents;	
	• correlation rules with the highest number of incidents;	
	• affected accounts;	
	• based on a random search of the event database using the constructor.	
115	The solution must provide source-based reporting with the following information:	
	• Common internal IP addresses in Netflow;	
	• Common external IP addresses in Netflow;	
	• Statistics on traffic volumes in relation to ports;	
	• Statistics on sources with the largest number of events.	
116	The solution must provide the ability to email reports, store the report on the network storage, and publish the report through the system management console.	
117	The solution must support emailing of reports according to a customizable schedule.	
118	The solution must provide the ability to export reports in HTML, CSV, Split CSV, XLSX formats.	
119	The solution must support different colors to indicate component status.	
120	The solution must support the ability to group arbitrary event fields.	
Performance monitoring requirements		

121	The solution must collect and store performance metrics for all components of the system.	
122	Performance metrics must be displayed in the graphical user interface of the system.	
123	The solution must collect, store and display at least the following performance metrics:	
	• Memory usage;	
	• The number of events processed per second (incoming to and outgoing from the component), broken down by source;	
	• Latency at each stage of event processing;	
	• Parameters of working with active lists (number of requests, latency).	
	• Parameters of working with active lists (number of requests, delays);	
	• Parameters of work with external systems (number of requests, delays).	
124	The solution must support the transfer of performance metrics to external monitoring systems.	
125	The solution must support the ability to send email notifications when certain thresholds are exceeded.	
Security requirements		
126	The solution must differentiate access rights based on a role model;	
127	The solution must log access events and significant configuration changes;	
128	The solution must support authentication and authorization using the following mechanisms	
	· Local database of user credentials (by login password);	
	· AD, ADFS, FreeIPA.	
129	The solution must have built-in mechanisms to counter password mining attempts.	
130	The solution must support RESTful API for integration with 3rd party solutions. RESTful API must be documented	
Technical support requirements		
131	The Solution must include Vendor technical support and a dedicated manager provided by the Vendor.	
	Technical support must include:	
	· Remote connectivity between the customer and the vendor's; support specialists for problem-solving;	
	· Recommendations on solution optimization;	
	· Product updates;	
	· Personal technical account manager.	
132	Regular reporting on incidents handled by the vendor against the SLA	
133	Technical support must include custom parsers (at least 10 types) for data sources not supported by solution 'out-of-the-box'.	
134	Technical support must be via a dedicated manager provided by the Vendor.	

11. Workstations(Qty 85+20*)

* Twenty for Bangalore center

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
		Form Factor	Professional Tower or Small Form Factor (SFF) Workstation
2	Processor (CPU)	Model	Intel Core i9-or similar on benchmark test
		Cores / Threads	24 Cores (8 P-cores, 16 E-cores) / 32 Threads
		Base Clock (P-cores)	Minimum 2.0 GHz
		Max Turbo Frequency	Up to 5.8 GHz or higher
		Intel Smart Cache	36 MB or higher
		Processor Base Power (TDP)	65W, with dynamic Max Turbo Power support
		Integrated Graphics	Intel UHD Graphics 770 (or equivalent integrated graphics)
3	System Memory (RAM)	Total Installed Capacity	32GB on delivery on single DIMM Slot
		Configuration	2 x 32 GB 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	1000 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
5	Graphics Card	GPU Model	NVIDIA Quadro T1000
		Dedicated Memory	8GB GDDR6
		Display Outputs	1 x VGA port + Multiple Digital Outputs
		Digital Output Resolution	Support up to 5120x2880 @ 60Hz per digital output.

6	Operating System	Version	Microsoft Windows 11 Pro (64-bit) or a Linux OS
7	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)
8	Audio	Integrated Audio	High Definition Audio
9	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
		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
10	Power Supply	Type	Internal, Auto-sensing
		Wattage	Sufficient wattage to power all components at full load, including future expansion.
11	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
12	Management Features	Remote Management	Standard desktop manageability features
13	Peripherals	Keyboard	Full-size USB Keyboard
		Mouse	USB Optical Mouse
14	Warranty & Support	Duration	3 Years Warranty and 3 years Support
15	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.

12. Conference Solutions

Camera Solution

Sno	Category	Specification Item	Required Specification	Compliance Yes/No
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/SmartSpeaker 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.	

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/m² (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,	For direct content display from USB drives or powering external accessories.

		or peripheral connections.	
	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	Ensures compatibility with a wide range of mounting solutions.

		wall mounts or floor stands.	
	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.	

13. Smart Rack Systems*

Sr.No	Minimum Technical Specification	Compliance (Yes/No)
1	**Scope of Work**	
1.1	This specification covers intelligent integrated/inbuilt infrastructure, standalone system design, engineering, manufacture, assembly, testing at manufacturer's works, supply, delivery at site, unloading, handling, proper storage at site, erection, testing and commissioning at site of complete infrastructure for the proposed Data Centre to be installed at FITT IIT DELHI , as detailed in the specification, complete with all accessories required for efficient and trouble-free operations	
1.2	Modular and scalable design for power and cooling: The critical components like Cooling used to design the system should be redundant and in the Events of failure the components can be maintained easily. All the components of the infrastructure should be such that it can be easily dismantled and relocated to a different location.	
2	**Requirements**	
2.1	Intelligent Integrated Smart Rack DC Infrastructure with inbuilt hot and cold aisle containment of 05 racks should cater IT load up to 100kW.	
2.2	Intelligent Integrated Smart Rack DC Infrastructure essentially should include internal redundant or backup power supplies, environmental controls (Precision air conditioning, fire suppression, smoke detection, Water leak detection and humidity sensors), and security devices. Both Critical systems like IT Load UPS & HVAC should have N+N & N+1 redundant topology respectively. Environmental monitoring shall be done from IP based software.	

2.3	The detailed specifications of the intelligent integrated/inbuilt infrastructure, standalone system shall be in adherence to standard Data Centre guidelines thus shall be composed of multiple active power and cooling distribution paths, but only one path active.	
2.4	The complete Integrated Smart Rack solution must be CE certified or tested by third party agency for applicable industry standards i.e EN 62368-1: 2014. The Third-party agency should be following National Accreditation Board, BIS, TEC accreditation /Recognition.	
2.5	Critical Component's for Integrated Smart Racks Data Centre Solution i.e Rack, Cooling, UPS, intelligent rack PDU, monitoring system along with temperature & humidity sensor and wall mounted industrial grade AC units should be from same & single OEM for Seamless Integration & better Service Supports.	
3	**The Intelligent integrated Smart Rack DC Infrastructure shall have following components:**	
3.1	**In-Row closed loop Air-Conditioning**	
3.1.1	Data Center server and network racks should be equipped with In-row Variable capacity cooling units to provide closed loop precision cooling system which should be able to cool the equipment's uniformly right from 1st U to 42°' U of Rack.	
3.1.2	Each DX based Inrow Precision Air Cooling solution should deliver more than or equal to 40kW net sensible capacity@48°C Ambient Temperature, supply air temperature @22+2°C and return air temperature of 35°C. It is mandatory to submit OEM software selection output of the proposed unit. **Precision Air Conditioner should have following features:** • Cooling System should be DX (Variable capacity) type in N+I Topology. • The unit incorporates a high efficiency DC brushless compressor with a crankcase heater, filter dryer, moisture indicating sight glass, and an electronic expansion valve. • The compressor is equipped with an environment-friendly refrigerant (R410A), and a DC brushless type arrangement with variable capacity operation of 30% to 100%. • The unit is equipped with minimum 10 no. hot swappable EC fans. The fan speed is variable and can be automatically regulated by the highly intelligent controller through all modes of operation. The fans pull air through the coil and is located on the front side of the unit. Each Unit should be capable of handling up to 10200 CMH with a horizontal airflow pattern. • Each unit should have an inbuilt heater & humidifier. The capacity of the humidifier should be 1.5 kg/h and the capacity of reheating should be 6 kW. • Outdoor Unit with fan speed controller • Micro Processor should have capacity to store up to 1000 historical event records. • 7-inch HMI color screen or LCD screen with simple user interface operation. • The unit is equipped with two G4 rated air filters following with EU4, located within the cabinet, and accessible from the rear side of the unit. A filter clog alarm is also available as an option to alert clogging of the filter.	
3.2	**IT Rack & U Space**	
3.2.1	05 no IT racks with integrated hot & cold aisle containment. Integrated Smart rack solution should have below configuration: • 05 no. 42 U, 800 mm x 1200 mm with integrated hot & cold aisle containment of minimum 300 mm each.	

	• Integrated Smart racks should have a minimum of 206 U space available for IT equipment and network equipment.	
3.3	**Monitoring**	
3.3.1	Detailed Monitoring & Diagnostics through 1U rack mountable monitoring unit, with redundant power supplies & capable of single window monitoring of all the environmental parameters along with UPS & air conditioning through a single window dashboard over ethernet & Capable for sending Email Alerts.	
3.3.2	The monitoring unit should support IPMI2.0 protocol to enable feature to Access server Service Processor.	
3.3.3	The Monitoring unit should have a feature to enable graceful shutdown of the IT servers supporting IPMI Protocol.	
3.3.4	Capable for Email Alerts	
3.3.5	The Monitoring unit should support dual power input.	
3.4	**Other features:**	
3.4.1	The Intelligent integrated infrastructure would provide much functionality and some of the key functionalities are — Both Cold aisle & hot aisle containment, of minimum 300 mm each for airflow, Airtight Thermally insulated cabinet, remote Management.	
3.4.2	The rack-based Biometric access control system provided should be controlled by a common access control panel with control for both front as well as rear doors. IP-based Access control with user exclusive authentication.	
3.4.3	Critical Component's for Integrated Smart Racks Data Centre Solution, i.e Rack, Cooling, UPS, intelligent rack PDU, monitoring system along with temperature & humidity sensor, should be from same & single OEM for Seamless Integration & better Service Supports.	
3.4.4	Electrical Distribution board within Utility Cabinet to have fire detection & Novec 1230/ FK- 5-1-12 Based Fire Suppression system.	
3.4.5	Status based LED Lights within Smart Racks	
3.4.6	9 inch touch screen HMI — Graphical User Interface display should be mounted on the Integrated smart rack solution for local monitoring.	

Detailed Specification of Components:

3.5	**Inrow Precision Air Conditioning System**	
A	Design Requirements	
I	The unit shall be factory assembled environment control unit that can be floor mounted to provide maximum cooling capacity in minimum footprint. It is specifically designed for rack cooling from the front and rear of the unit. The cooling system of the unit is designed to ensure even air distribution to the entire face area of the coil. The unit can be installed between the racks or at the end of the row. The unit also modulates the cooling capacity, and the airflow based on requirements of the environment.	
II	The unit should be capable of handling up to 10200 CMH with a horizontal airflow pattern. The sensible cooling capacity of the unit should be more than or equal to 40 kW at 48°C ambient temperature. The unit is supplied with 318 V to 415 V, 3 Phase, 50 Hz/60 Hz power supply. The humidifier's capacity is 1.5 kg/h and the capacity of reheating is 6 kW.	
B	Product	
I	Cooling Circuit	
	The refrigeration circuit of the unit incorporates a high efficiency DC brushless compressor with a crankcase heater, filter dryer, moisture indicating sight glass, and an electronic expansion valve. The compressor is equipped with an environment-friendly refrigerant (R4l0A), and a DC brushless type arrangement with variable capacity operation of 30% to	

	100%. The compressor also has a suction gas cooled motor, vibration isolators, internal thermal overloads, automatic reset high-pressure switch, low pressure & high-pressure transducer, and a crankcase heater.	
	The unit should have a copper tubes evaporator coil of with hydrophilic painted aluminium fins followed with a condensate drain pan. The diameter of evaporator coil is 7 mm and face areas of >1.27 sqm and unit should have 3 rows of coil. The hydrophilic coating provides superior water carryover resistance.	
	The electronic expansion valve (EEV) controls the mass flow rate of the refrigerant within the refrigerant circuits at high speed with greater precision. EEV is suitable for DC brushless compressor as an expansion device, with green refrigerants (R4l0A). EEV provides a better control over superheating at the outlet of the evaporator, thereby ensures that compressor shall never be filled by liquid.	
II	Fan Section	
	The unit is equipped with 10 EC fans. The fan speed is variable and can be automatically regulated by the highly intelligent controller through all modes of operation. The fans pull air through the coil and is located on the front side of the unit. The EC fan has the characteristics of high efficiency, energy saving, space saving and hot swappable.	
III	Cabinet & Frame	
	The exterior steel panels are custom powder coated to protect against corrosion. The wall side panels are separated by the l5mm, 1.75 lb/ft3 insulation from the airstream. The unit is provided with levelling feet. The perforated inlet and outlet panels have 75% open area for better circulation of the air through the unit.	
IV	Air Filtration	
	The unit is equipped with two G4 rated air filters following with EU4, located within the cabinet, and accessible from the rear side of the unit. A filter clog alarm should be available to alert clogging of the filter.	
V	Refrigerant	
	The unit is designed for R410A, an environmentally friendly refrigerant.	
VI	Unit Controls	
	Microprocessor Controller	
	The unit should be controlled by the microprocessor-based intelligent controller board. The air conditioning unit is also configured with 7-inch HMI colour screen or LCD screen with simple user interface operation. The multi-level password protection feature can effectively prevent unauthorized operation. It also has additional features like power failure auto-restoration and high & low voltage protection. The operation status of the components can be available on the respective menus screen; the expert-level fault diagnosis system should automatically display the current fault information, facilitating easy maintenance. It should also store up to 1000 historical event records.	
	The controller allows setting and/or monitoring of the following space parameters: • Air inlet temperature • Air supply temperature • Return temperature setpoint • Supply temperature setpoint • Humidity (inlet) • Humidity setpoint • Suction pressure • Discharge pressure • Compressor output • Fan output • Heating status	

	• Humidifier status Supply voltage The example of available warnings/alarms: • High supply temperature • Low supply temperature • High return humidity • Low return humidity • Loss of airflow • Compressor low pressure • Compressor high pressure • Electrical heater high temperature (when applicable) • Clogged filter • Supply sensor failure • Humidifier problem • Rack sensor failure	
	Following features is incorporated in the controller: • Status Report of the latest 1000 alarm history of the unit • Input for remote on/off and voltage-free contacts for simple remote monitoring of low and high priority alarms such as: high/low temperature, high/low refrigerant pressure, fan/control failure, compressor/control failure, and others should be available.	
VII	**Condenser**	
	The condenser is designed with a fan speed controller and a set for R410A refrigerant usages, operates at 0 °C to 45°C ambient temperature. The condenser frame is made up of sturdy GI/MS structure and the electrical control box has IP54 protection.	
VIII	**Electrical Reheat** The unit is equipped with a Positive Temperature Coefficient (PTC) ceramic type electrical heater.	
IX	**Electrode Humidifier** The unit is equipped with a factory installed electrode humidifier, which includes humidifying cylinder kit and humidifying control board. The humidifying control board receives humidifying command from the main control board, which automatically controls the operation of the humidifying cylinder, and gives feedback alarms information of the humidifier to the main control board. The conductive rate of water required for electrode humidifying should be within the range of 125 us/cm to 1250 us/cm.	
X	**Condensate Pump**	
	Each unit should be provided with a factory installed condensate pump with a head capacity up to 10 m-head or up to 6 Al m-head.	

Uninterrupted Power Supply (UPS) System for Continuous Cooling

3.6	**Uninterrupted Power Supply (UPS) System for Continuous Cooling**	
a.	General Description:	
	Supply, Installation, testing and commissioning of true online, double conversion, high efficiency, high power factor Uninterruptible Power Systems (UPS) rated at 100 kVA with battery backup support for 15 minutes on rated load. UPS & backup batteries should be supplied with the necessary arrangements for proper mounting in the space allocated.	
b.	Configuration: 100kVA	
c.	**Detailed Technical specification**	
	Input	

	Nominal input voltage	380/400/415 Vac 4-wire plus ground	
	Input voltage range	323 to 478 Vac	
	Nominal input frequency	50/60 Hz	
	Input frequency range	45 to 55 Hz/55 to 65 Hz	
	Input current distortion with linear load (with filter)	3 to 10% with optional filter	
	Power factor (with filter)	0.88 to 0.97 with optional filter	
	Output		
	Nominal output voltage	380/400/415 Vac 4-wire plus ground	
	Output Power Factor	0.9	
	Frequency		
	Voltage stability	+/-1% (Steady state); +5% (Transient state)	
	Transient recovery time	20 milliseconds (max	
	Frequency stability	+/-0.1% (Synchronized with internal clock);+6% (max)(Synchronized with bypass)	
	Overload capability	101 to 110%, 60 minutes; 111 to 125%,10 minutes; 126 to 150%, 1 minute.	
	Voltage distortion with linear load	<1%	
	Voltage distortion with 100% Non-linear load	<5%	
	Permissible load unbalance	100%	
	Load handing capability without kVA derating	0.5 lagging to 0.9 lagging	
	Phase angle displacement accuracy 100% balanced load 100% unbalanced load	 +1° +1°	
	Standard & Conformity		
	General and safety requirements for UPS	IEC 62040-1	
	EMC requirements for UPS	IEC 62040-2	
	UPS Classification according to IEC 62040-3	VFI-SS-I I I	
	Communication Protocol	SNMP/ModBus / Jbus	
	Battery Backup	Minimum 15 min battery back @ Rated load via I2V SMF Batteries @ 0.9 pf	

3.7	**Racks & Accessories**	
a.	Rack Containment Frame should be of 42 U, 19" mounting type with standard Rack + Cold & Hot Aisle Containment. Both Cold aisle & hot aisle containment, of minimum 300 mm each, should be part of the rack frame.	
b.	Rack frame is, scalable and modular with safe load carrying capacity of 1000 Kg	
c.	Colour shade of Rack is RAL 7021	
d.	Base plinth with 100 mm height	
e.	Cable entry provision from top & bottom both side of rack	
f.	Cut outs with rubber/brush grommet on top and bottom cover of rack for cable entry	
g.	Vertical Cable manager on both LHS & RHS on rear side	

h.	Each rack shall have front glass door for complete 42U height visibility & rear steel split door integrated with common Biometric access control panel	
i.	Thermally insulated cold aisle chamber	
j.	Blanking panels to prevent air mixing	
k.	Fixed Shelf to be provided	
l.	Plastic Cable duct on vertical LH & RH section of racks for cable routing	
m.	Front Rack doors to be provided with Biometric Access Control with 02 nos. of Electromagnetic lock per door	
n.	Gas spring to be provided on front doors of racks	
o.	Status based LED light to be provided on each rack	
p.	Each rack enclosure should be physically separated through caged partition at cold & hot aisle to avoid unauthorized access from one rack to another	
	Intelligent rack PDU	
a.	Each IT rack to have minimum 02 no.63 A , three phase Intelligent PDU per Rack.	
b.	iPDU should have min. 30 outlet sockets. All 30 outlets of hybrid nature, which can be utilized as either Cl3 or Cl9 outlet. All outlets should provide high retention to avoid accidental dislodging of power cords. The IPDU hybrid outlets should meet electrical compliance and should be UL certified.	
c.	Monitoring parameters — The IPDU should have monitoring capability at the Strip level and Circuit/ Breaker monitoring.	
d.	The following monitoring parameter should be available at input level	
	a. Voltage (V)	
	b. Current (A)	
	c. Power factor	
	d. Active power (W/kW)	
	e. Apparent power (VA/kVA)	
	f. Energy consumption (kwh)	
e.	The metering accuracy should be +/- l% compliant to ANSI C12.l and IEC 62053-21 at 1% Accuracy Class Requirements for strip level	
f.	IPDU should have 12 numbers l6A magnetic circuit breakers for overcurrent protection in three phase PDU	
g.	The IPDU should have Colour coded outlets based on circuit Colour for easy identification of circuits for quick troubleshooting and ease in maintenance	
h.	The IPDU should support the daisy chain of minimum 40 units to reduce network port requirement and ensure continuous flow of data on network to monitoring tool/BMS/DCIM even a break in daisy chain occurs.	
i.	Network communication — PDU should have two Network Ports.	
	IPDU should support communication protocols including DHCP, HTTP, HTTPS, Ipv4, Ipv6, LDAP, NTP, RADIUS, SSH, SMTP, SSL, SNMP (vl, v2, v3), Syslog and TACACS+ or equivalent. Communication module should be hot- swappable, so that it can be replaced without powering off the PDU	
j.	IPDU should support encryption via TLS 1.2 or above for additional security.	
k.	IPDU should have features to support temperature, humidity, airflow, dew point, door position and flood detection sensors	
l.	The IPDU should support grouping of a minimum of 40 rPDU	
m.	The IPDU should be high temperature grade, operating temperature up to 60°C.	
n.	The IPDU shall have rotatable display, to easily read the displayed values when PDU is mounted upside down, based on the site requirement.	
o.	IPDU must support software-based mass firmware upgrades, backup and configuration.	

p.	IPDU should have USB support for firmware upgrade, backup, restored device configuration or expanding logging capacity via USB storage device	
q.	IPDU should have separate reset buttons for reset to factory defaults and separate button to reset IP only, if other configurations are not to be altered.	
r.	PDU should support configuration of user defined thresholds, reports and email alerts and send it automatically to the configured users automatically on the scheduled time intervals	
s.	The IPDU should have approvals form RoHS, CE marked, EN55032 /EN55024/ IEC 60950-1.	
t.	PDU should support integration with Power Management software/DCIM/Monitoring system for providing periodical data of power consumption.	
3.8	**Fire Safety & Security**	
a.	**Fire Alarm and Fire Suppression System** The integrated infrastructure solution should be designed as a complete stand-alone unit with security, fire detection and fire suppression systems. Each of the systems is inter-operable and inter-connected. Environmentally friendly NOVEC 1230/FK-5-1-12 agent is used to ensure that no harm to human beings and environment is caused. Following systems should be installed : • NOVEC 1230/FK-5-1-12 Clean Agent for fire suppression system. • Fire detection and alarm systems, with detectors and panel. • Protected area: The entire enclosed volume of the Intelligent Rack containment including electrical panel mounted in utility cabinet should be protected with fire detection and fire suppression system. • The NOVEC 1230/FK-5-1-12 system is designed and installed as per NFPA 2001-2012 Edition. SMPV, Petroleum and Safety Explosives Organization (PESO) approved cylinder filled with NOVEC 1230/FK-5-1-12 is installed in specially designed Modular rack.	
b.	**Biometric Based Access Control** The IP-based Access Control System shall be used to serve the objective of allowing access to authorized personnel only. The system deployed will be based on Biometric Technology. The front & rear rack doors will be provided with magnetic locks and will operate on fail-safe principle through one common Biometric access control system. The system would be designed and implemented to provide the following functionality: • Configurable system for user defined access • Built-in Real Time Clock (RTC), calendar; complete Database stored locally and shall be capable of operating offline on standalone mode. • Record, report and archive each and every activity (permission granted and / or rejected) with log formats • Fail safe operation in case of no-power condition and abnormal conditions such as fire, theft, intrusion, loss of access control, etc. • At the biometric reader, user presents the finger to the biometric reader which is unique to each employee. The pattern is read and compared with stored data to grant / deny access.	
3.9	**Monitoring**	
	Supply and installation 1U rack mountable monitoring system with Sensors & notification system for the Integrated Smart Rack Solution. The system shall continuously collect critical information from network connected devices such as Cooling Units, temperature & humidity sensors, Door sensors, Water Leak sensor and other dry contact monitoring. The solution should have Beacon, Buzzer-Sound and Flash Led Alarm. Based on pre-set parameters, automated email alerts should be sent to the intended recipients	
	Technical Specification for the monitoring unit:	
a.	Environmental Specification	

	Application site	Integrated Smart Rack Solution	
	Operating temperature	0‘C to +60‘C	
	Relative humidity	95%RH, no condensation	
	Use environment	The dust meets the indoor standard of the GR-63 without corrosive gases, flammable gases, oil mist, water vapor, dripping or salt, etc.	
	Power Distribution network	TT/TN	
	Protection level	IP20	
b.	Physical Specification		
	Main unit	l U Rack Mounted, with module extension design	
	Power	Support Dual power input AC l00Vac to 240Vac 50Hz/60Hz, <2A, Cl4 plug	
	Monitoring port	Main unit should be with AI/DI/DO/RS485/RS232 ports	
	Expansion slot	Should have capacity of adding additional 4 expansion slots to expand the monitoring access ability as per requirement	
	Expansion card	Should have capacity of adding Expansion card for AI/DI/DO/RS485/RS232 works with host expansion slot as per requirement	
	LAN Port	Dual LAN RJ-45 electral 10/100/l000Mbps Ethernet interface with different IP segment to achieve IP network redundancy	
	Fiber port	Should have feature with additional SFP module , if required, to support maximum l000Mbps optical Fiber communication, the port could assign a different IP segment address Vs LAN port	
c.	Certification		
	The monitoring unit gateway should meet CE claims, UL Certified, FCC Certified		
d.	The monitoring unit should be able to perform the following functions as per solution requirement:		
	Device monitoring: the data acquisition and processing of different intelligent devices, and control smart devices through the intelligent interface		
	Safety management: • Realize local door opening, log recording, etc. • Implement firefighting signal connection in the Smart Rack Solution		
	IT management: • Monitoring and management of IT device through IPMI • Monitor console output of IT device		
e.	Performance Specification		
	Environmental:		
	Temperature & Humidity sensor: By default, unit should support up to 32 sensors expandable up to 80 sensors with additional, if required.		
	Digital Input Sensor By default, unit should support up to 12 sensors expandable up to 44 sensors with additional cards, if required.		
	Additional Analog Input, Analog output, Digital output should be connected using the required expansion cards, if required.		

	Infrastructure Management	
	• Modbus 485 and/or SNMP Communications • Default of 32 devices in a monitoring module (Can be all Modbus 485, or all SNMP, or a Mix)	
3.10	**HMI — Smart Racks Interface mounted on Integrated Smart Rack Infrastructure for Local level monitoring**	
a.	• Smart Racks should have functionality to graphically monitor the passive infrastructure – • 9-inch-wide touch screen HMI display with a very user-friendly interface • It should be menu driven system, Thermal management, Power supply environmental quantities, alarms, logs, and provided a total of menu items, breakdown of the sub-menu item the next menu level, • First authorization on LCD, is only authorized once, authorized system will automatically skip the authorization page while booting. • System Configuration page includes integrated cabinet configuration. • Home page presents system function information (Such as Date & Time ex.), system performance parameters and critical system parameters	
b.	**System performance parameters** • Enclosures: thermal path average temperature, the IT load cabinet single cabinet (configured for an intelligent PDU). • Air conditioning: return air temperature, supply air temperature • All the components (Intelligent PDUs ext.) shall be graphically represented on HMI.	
c.	**Critical system parameters:** • UPS operation: AC mode/bypass mode/Battery mode/standby mode, The system load factor • HVAC Operation —Animated fan during Run & Compressor status display IT racks parameters — Temp. & Humidity Parameters are highlighted for normal & abnormal values	
d.	**Thermal Management:**	
	• Return air temperature profile cross-ordinate. • Cooling fan state to the operating state, the corresponding icon is animated; alarm flood state is, icon animations. Door status icon static display, the door opened and closed the door to a different style static icon.	
e.	**Supply & Distribution:**	
	• UPS page displays distribution parameters and real-time power system operating mode. • UPS working state: AC mode / bypass mode / Battery mode / standby mode. • The operating state of the system: Single /1 + l parallel / 2N double bus. • For each PDU distribution -PDU page displays the total current and power component. • when the PDU voltage value, the current value exceeds the set range, the system will generate a corresponding alarm; on the contrary, the alarm disappears	
f.	**Environmental Amount: (The amount of ambient acquisition)**	

	• acquisition and display status of the current environmental data amount of the rack, comprising: a real-time value of the respective collection point temperature and humidity sensors, front and rear door state, hot/cold aisles average temperature curve moisture profile. • When the air conditioning is working properly, hot and cold airflow patterns dynamic channel is turned on when the air conditioning is not working, dynamic airflow patterns hot and cold aisles disappear • Door status icon static display, the door opened and closed the door to a different style static icon. • When the passage of hot / cold temperature and humidity sensor measured value exceeds the set range, the system will generate a corresponding alarm; conversely, when the hot / cold aisles temperature and humidity sensor measurement range is set to fall the alarm disappears	
g.	**Warning — Alarm-Current Alarm:** • Displays the Current Alarms Page. • The current alarm is divided into emergency alarms, major alarms and general alarms. • When the current alarms and buzzers system in normal mode, the LCD buzzer will sound an alarm, and for 5 minutes, the duration of the latest alarm generation time from a timer In maintenance mode, the buzzer will not sound an alarm. After the lifting of maintenance mode, buzzer return to normal mode	
h.	**Alarm - historical alarm:** • Alarm History page provides a display system and screening history alarms. • LCD page provides only historical records up to 100 within the system one week. For longer or more the number of alarm history, Web pages can be viewed in alarm management	
4	**Warranty**	
	Warranty for the complete system shall be 03 years from the date completion of installation & commissioning and 3 years support	
5	**Maintenance & Support**	
i.	**After Sale Service** • Service shall be guaranteed by supplier during defect liability period/Warranty Period. • Bidders shall have back-to-back agreement with the product OEM to offer 24 x 7 services through their authorized service engineer for warranty period. • Product OEM shall provide warranty from the date of taking over of the equipment after the acceptance tests.. • Basic training and operational training to be provided after the successful installation of DC	

	• Quarterly PM to be carried out during the warranty period	

MINIMUM ELIGIBILITY CRITERIA FOR SERVER RACKS

The OEM should adhere & comply to the following minimum eligibility criteria for the bid:

a) Critical Component's for Integrated Smart Racks Data Centre Solution i.e Rack, Cooling, UPS, intelligent rack PDU, monitoring system along with temperature & humidity sensor should be from same & single OEM for Seamless Integration & better Service Supports.

b) The complete Integrated Smart Rack solution must be CE certified or tested by third party agency for applicable industry standards i.e EN 62368-1: 2014. The Third-party agency should be following National Accreditation Board, BIS, TEC accreditation / Recognition.

c) The Smart rack OEM should have at least 04 years of experience in executing similar works (Similar works means — "SITC of Integrated Smart Rack Infrastructure of minimum 06 rack configuration with Inrow cooling units") in Central/State/PSU Organizations. Completion Certificate, as proof of experience, signed by the concerned authorities to be submitted along with the bid.

d) The Smart Rack OEM must have executed minimum 05 Integrated Smart Rack Data Centre projects, with minimum 05 rack configuration in each project, during the last 3 years from the bid submission date in any reputed Govt/ PSU / Pvt. organizations. Completion Certificate signed by the concerned authorities to be submitted along with the bid.

e) OEM Service Support for Major Equipment's: Smart Rack OEM or Manufacturer should have its own service centre in Delhi /NCR.

f) Smart Rack OEM or Manufacturer should be ISO 9001: 2000, ISO 14001, ISO/IEC 27001:2013 and ISO 45001 certified.

g) Smart Rack OEM shall be present in Gartner Competitive Landscape Research Report for Edge in the Micro Modular Data Center Market as Leader in Data Center Facilities Specialist.

h) The Smart Rack OEM should have at least three qualified and experienced DC certified professionals like CDCP/CDCS/CDCE/ATD on their company payroll.

i) Smart rack OEM should have its own manufacturing facility in India for similar capacity of Rack, UPS & Precision air conditioning units for high availability of the proposed solution. Supporting document/undertaking regarding the same to be submitted along with the bid.

j) OEM or Manufacturer of the offered goods/ equipment's should be a company registered under the companies Act since last 10 years. Valid company registration certificate should be submitted.

Chapter- 4

General Instructions for Bidders

The Expression of Interest requires the submission of a detailed solution, Technical Requirements, Specifications, and Budgetary quote for the Solution mentioned in the tentative scope of work by the System Integartor

1. **Mandatory Site Survey/Visit & Pre-EOI Meeting**: All the interested parties are requested to go through the tentative Scope of Work detailed in Chapter 3 and mandatorily visit the site(At MayurVihar/Ayanagar New Delhi) during office working hours (at their own cost) before the Pre-EOI meeting scheduled on ____Jul 2025(10 Days from date of publication). *The visit will be scheduled for the parties and schedule of visit on D+5 to understand the modalities such as design, site preparation, supply, installation, testing, training, along with operations and maintenance of physical and IT Infrastructure for Integrated Technology Solution.*

2. Key dates(All dates timeline is till 1700 Hrs of the day. In case of holidays schedule would shift to the next working day

a.	Publication	D day
b.	Site Visit Data Center	D+5 (Tentative time 1400Hrs)
c.	Pre Bid Query	D+7 (Time 1700 HrsZ)
d.	Pre Bid Meeting (Hybrid Mode)	D+9/10(Time 1400 Hrs)
e.	Submission date	D+15 (Time 1700 Hrs)

3. Only the queries received on or within the date prior to the Pre-EOI meeting will be entertained and answered. All such clarifications, together with all details on which the clarification was sought, will be uploaded to the FITT portal and the tender section of FITT, IIT Delhi Website. Such clarifications shall form part of the EOI document.

4. Eligibility Criteria: FITT, IIT Delhi has set up minimum eligibility criteria for the bidding purpose. All interested parties must meet the criteria mentioned in chapter 4 before they apply for the bidding. The bidding parties meeting the criteria must enclose their supporting documents along with their technical proposal and budgetary quote, failing which their bids will be summarily rejected and will not be considered any further.

5. Submission of EoI: FITT,IIT Delhi invites online EoI in single packet bid (Technical Offer along with estimated Budgetary Quotation). The Technical Offer/Proposal shall include the proposed Bill of Material on the basis of a turnkey project (As per Annexure I . All the items/products/solutions required for the project should be suggested and included in the Bill of Material. The complete EoI shall be submitted within the stipulated date & time and to be sent to the address/email as mentioned.

After the due date and time, the proposal will not be considered. No opportunity shall be given to Bidder to revise the offer at any stage after the submission of the bids.

6. Any incomplete EoI received shall not be considered and will be summarily rejected in the very first instance without any recourse to the bidder and shall not be evaluated. All entries in the EoI should be legible and filled clearly, otherwise the proposal is likely to be rejected. If the space for furnishing information is insufficient, a separate sheet duly signed by the authorized signatory may be attached. The cuttings, if any, must be initialled by the authorized signatory.

7. Period of Validity of EoI: The proposals shall **remain valid till 120 days** from the date of opening of EoI. In exceptional circumstances, FITT, IIT Delhi may ask for extending the period of validity and such a request shall be binding on Bidders. FITTs request and the response to such a request by various bidders shall be in writing.

8. Evaluation of EoI & Call for Presentation: After the opening of the proposal, FITT, IIT Delhi will examine the credentials of the firms based on the submitted documents as per the **eligibility criteria detailed in Chapter 6** and other eligibility criteria as mentioned in Bid Document, to shortlist the vendors. In case FITT decides to seek further information/clarification, the same shall be provided by the bidder.

9. After evaluation of the eligibility criteria, the shortlisted vendors will be required to make a focused presentation on the company, expertise, experience in the relevant field, and products with the proposed solution to FITT, IIT Delhi. The date of the presentation will be informed to the shortlisted vendors in advance.

10. Following the presentations, based on the proposed acceptable solutions, FITT,IIT Delhi will finalize the actual requirement along with specifications and the RFP will be shared with the shortlisted SI.

11. It must be noted that this EOI is published for obtaining technical offers along with the budgetary quotation for the procurement of an Integrated Technology Solution. ***However, this EoI has been published without any financial commitment (Non-Committal EoI) from either side forwards any of the participating firms.***

12. The Competent Authority of FITT, IIT Delhi is not bound to accept the EOI if any technical discrepancies are found in the EOI. However, it reserves the right to accept/reject the EoI, and the decision of the authority in this regard shall be final and binding on the Bidder.

13. Participation in EoI will not be considered as a qualification of the bidder tender inquiry to be published later.

14. Amendment of Bid Document: At any time prior to the deadline for submission of proposals, FITT, IIT DELHI reserves the right to add/modify/delete any portion of this document by issuance of a Corrigendum, which would be published on the

FITT, IIT Delhi website. The Corrigendum shall be binding on all bidders and will form part of the bid documents.

15. FITT, IIT Delhi Right to reject any of all bids: The Competent Authority of FITT, IIT Delhi reserves the right to reject any bid and to annul the bidding process and reject all bids at any time or discontinue this EOI process, without assigning any reason, at any time. Any effort by a bidder or bidder's agent/consultant or representative, whosoever described, to influence the FITT, IIT Delhi in any way concerning scrutiny/consideration/evaluation of the bid shall entail rejection of the bid,

16 Eligibility Criteria

Parameter	S. No.	Criteria	Supporting Document
Organisational	(i)	Bidder should have valid PAN, GST registration as on bill submission date. .	Copy of PAN & GST registration duly attested by authorized bid signatory
	(ii)	The Bidder should have Registered Office/Head Office/Branch Office in India (Preferably Delhi/NCR.)	Valid proof of office in duly attested by the authorized bid signatory.
Financial	(iii)	Average Annual Turnover of the System Integartor (SI) should be minimum Rs. 35 crores during last three financial years	Copy of audited Balance Sheet and Profit & Loss account or CA certificate should be submitted. In case the audit is ongoing for FY 2023-24,provisional statements duly attested by CA/statutory auditor should be submitted.
	(iv)	Bidder should have a positive Profit Before Tax (PBT) or Networth in at least two of the last three financial years.	
Experience	(v)	a) A Company/Firm/LLP registered in India for a period of at least three (3) years before the bid submission date and; b) Minimum three years' experience in execution of similar works as on the last date of bid submission.	Copy of Certificate of Incorporation/ other relevant document duly attested by authorized bid signatory and Copy of Purchase Order along with execution proof showing minimum three years' experience
	(vi)	The bidder must have successfully completed similar work during last three financial years and up to bid submission date as per below criteria:	Documentary evidence should be submitted.

		(Similar work means handled Creation of datacentre, storage, compute , NW security…) (i) Three similar completed works costing not less than the amount equal to Rs. 6 crores; or (ii) Two similar completed works costing not less than the amount equal to Rs 8 crores; or (iii) One similar completed work costing not less than the amount equal to Rs. 15 crores.	
Obligatory	(vii)	Bidder must not stand declared ineligible/ blacklisted/ banned/ debarred by any PSU/ Ministry/ Govt. organization from participation in its Tender Processes.	Undertaking to be submitted on letterhead of the company duly signed by Authorized bid signatory, as per PFC format
Functional	(viii)	The Bidder should be OEM or Authorized Partner/ Distributor/ System Integrator of the OEM(s) of the offered product(s).	Bidder to submit documentary proof (MAF), specifically in reference to this bid, duly signed by Authorized bid signatory.
	(ix)	Minimum 10 technical resources should be on bidder's payroll as on date of bid submission in the category of Implementation of Server/ configuration domain.	Resumes duly certify by HR & attested by authorized bid signatory. and Proof of EPFO payments to the employees

Chapter- 5

Tentative Scope of Work of EOI

1. Supply, Installation, commissioning and supporting operations for items listed in **Annexure 1**

2. IT hardware items (Servers/NW components) have to be installed in the NCIIPC Tier 3 data centre. The key inputs to the data centre are as under:-

    a) The design capacity is 400 KVA with current load at 100KVA.
    b) Cooling is through floor ducts with PAC of 18 Tonnes X8 (at present only 4 are switched on)
    c) DG capacity is 1010KVA X 2
    d) UPS are 200KVA X 4.
    e) 60 X 48 U Racks (40 racks are available)The details are 42U/600 mm Width X 1200 mm Depth, PLN and AP8853

3. The SI would be involved in Establishing a compute facilties as per the approved NW defined in the RFP in the existing Tier-III Data Centre located in the NCIIPC premises.
4. Also the Datacentre is air gapped i.e. no direct access to the internet,hence Software etc need to be catered for in offline mode.

5. The scope of work shall include systems deployment, testing, bench marking defined as per ATP (Acceptance Test Procedure) document, supply, packing, transportation, scheduling of transportation, transit insurance, onsite training of Purchaser's representatives, delivery of equipment at Purchaser's premises, unloading, installation and commissioning of system, which include making it functional in secure manner, providing warranty services, and any other services related to the system. The Work involved for Incubation facility infrastructure at NCIIPC , Ayanagar, Mayur Vihar, New Delhi on Turnkey basis, including installation and commissioning are given below: -

    a) **AT AYANAGAR:** Establishment of Office Infrastructure to include Seating Capacity of 85 (Cubicles, Furniture, AC, 2 x Mini Conference Halls), Workstations (85 for LAN/ standalone)
    (Infra creation is a separate activity. The IT installation and NW will be in scope of SI)

    b) AT BANGLORE: Supply install and commission requisite hardware
    c) Requisite secure access provisions be catered for the teams to avail the services established in the datacentre Facility.

d) Ensure industry standard norms for Cyber Security and role-based access control for the above infrastructure through deployment of requisite Hardware and Software for secure access from workstations/ PCs.

e) Provide/install all requisite software (Including value-added programs and customizations) such as operating system, scheduler, compilers, cluster management tools, scientific libraries, and tools related to all servers as well as compilation and optimization of code on GPU servers. Customize/configure and optimize software/ applications to the requirement of the Purchaser.

f) Operation/ management of day-to-day functions of the infrastructure for the period of Grand Challenge (12 months from Acceptance). The SI has to provide all material with three years of warranty support and 3 years of product Support after Successful completion of Site Acceptance Test (SAT).

g) Training to eight officials of Purchaser on administration, configuration, troubleshooting, operation and maintenance of the infrastructure.

h) Onsite Product Support for the complete Infrastructure by the Seller for a period of six years(3+3).

6. Delivery:-

a) The SI shall transport/deliver goods to the nominated premises at New Delhi. FITT, IIT Delhi shall not pay separately for the transit insurance and it is the responsibility of the SI to ensure that goods arrive at the destination in good condition. SI is also required to clear the goods for exporter etc. On receipt of consignment, the Packing cases should be opened in the presence of the representative of the FITT, IIT Delhi , for checking visually and Transit Damages, if any, by the FITT, IIT Delhi .

b) Transit Damages, if any, should be reported by the SI to FITT, IIT Delhi within 30 days from the date of receipt of consignment failing which no claims will be entertained by FITT, IIT Delhi.

c) The contracted goods shall be insured by the SI in favour of the FITT, IIT Delhi on the terms and condition and insurance to the amount equal to 110% of value of on all risk basis up to the designated premises. In case of any Insurance claims, FITT, IIT Delhi may authorize the SI to claim the same. Unless applicable, no part shipment of goods would be permitted. Trans-shipment of goods would not be permitted. In case it becomes

inevitable to do so, the SI shall not arrange part supply without seeking prior written consent of FITT, IIT Delhi . SI will be required to communicate the following information invariably in advance before the shipment point of SI for any consignment:-

i. Name of the Carrier / Ship
ii. Name of Loading station and Country
iii. ETA at Purchaser's premises / port of Discharge
iv. Number of Packages and weight
v. Nomenclature and details of major equipment
vi. Special instructions, if any stores of sensitive nature requiring special attention

7. Joint Receipt Inspection (JRI) of delivered goods shall be conducted on arrival at the designated premises at New Delhi. FITT, IIT Delhi will invite the SI to attend the JRI and JRI shall be completed within 10 working days from the date of arrival of equipment at Purchaser's location. JRI will consist of: -
   a) Physical Inspection to confirm receipt of delivered goods in good condition.
   b) Quantitative checking to verify that the quantities of the delivered goods correspond to the quantities defined in this MoU and the invoices.
   c) Upon successful completion of JRI, proceedings of JRI and Acceptance Certificate will be signed by both the parties. In case the SI representative is not present, the JRI proceedings and Acceptance Certificate shall be signed by the FITT, IIT Delhi , representative only and the same shall be binding on the SI. Copy of JRI proceedings and Acceptance Certificate shall be dispatched to the SI within 30 days of completion of the JRI. In case of deficiencies in quantity and quality or defects, details of these shall be recorded in the JRI proceedings, Acceptance Certificate shall not be issued and claims raised. In case of claims, Acceptance Certificate shall be issued by FITT, IIT Delhi representative after all claims raised during JRI are settled.

8. The SI shall prepare a Site Acceptance Test (SAT) schedule & procedure. The FITT, IIT Delhi representatives will carry out SAT of the stores/equipment and accessories in order to check their compliance with specifications in accordance with its standard procedures. The SAT schedule & procedure after being formulated by the SI should be forwarded to FITT, IIT Delhi for vetting and approval. The schedule & procedure should state how the SI would demonstrate that the system(s) will meet the functional and performance requirements and at least shall comprise following: -

   a) Functional and parametric Test

   b) Test equipment used, calibration requirements

   c) Pass / Fail criteria

d) Expected duration

9. The SI shall provide Acceptance Test Procedure (ATP) to the FITT, IIT Delhi, as per timelines attached at Appendix-2. FITT, IIT Delhi will provide comments in writing within 30 days of the receipt of the same. Otherwise the SI procedure will be accepted as final.

10. Training

a) Onsite training to the representatives of FITT, IIT Delhi shall be provided as mentioned below. Complete information regarding material to be covered and type of background of the trainees required shall be intimated to FITT, IIT Delhi at least 21 days in advance: -

i. **Initial Training**: - Minimum Eight Scientists / Engineers/ officers/ Operational Technical staff to be trained for five working days before Installation of the system which would broadly cover basics of system configuration and troubleshooting.
ii. **OJT (On the Job Training)**: - Minimum Eight Scientists / Engineers/ officers/ Operational Technical staff to be trained for five working days on operation and maintenance of the system.

11. The SI will be required to furnish Performance Guarantee by way of Bank Guarantee through a commercial bank of India for **a sum equal to 5% of the Order value with respect to items. Performance Bank Guarantee should be valid up to 60 days beyond the date of successful completion of the Grand Challenge or 30th Nov 2026 (Whichever is later)**

12. Payment terms:-
a) Purchaser will pay 25% of the amount on confirmation of dispatch of stores/shipping.
b) Purchaser shall pay 50% amount of the cost to the Seller against delivery of infra items at site post successful JRI on submission of invoices to the Purchaser.
c) Balance 25% payment in shall be made on successful installation & commissioning of the incubation centre, Site Acceptance Test (SAT) and conduct of training on equipment.

Chapter –6

BOQ and Technical Bid- Eligibility Criteria (Annexure - I to VI)

Checklist for Technical Bid

Sr. No	Pre-qualification criteria	Documents to be provided	Attached (Y/N)	Pg No.
1	The prospective Bidder shall be an Indian entity registered and operating in India under the appropriate Laws of India.	Registration Certificate of Business.		
2	Bidder must have GST registration certificate issued by the Competent Authority	Attested copy of GST registration certificate.		
3	Bidder must have PAN/TAN/GIR card.	Attested copy of PAN/GIR/TAN Card		
4	List of items proposed to be supplied	Annexure- I [On the letterhead of the Bidder]		
5	Bidder's Details	Annexure- II [On the letterhead of the Bidder]		
6	Declaration of Bidder	Annexure- III [On the letterhead of the Bidder]		
7	Declaration of blacklisting/nonblack listing	Annexure- IV [On the letterhead of the Bidder]		
8	Financial Capability of Bidder	Annexure- V [On the letterhead of the Bidder]		
9	Details of the Firm's Experience of Similar Services	Annexure- VI [On the letterhead of the Bidder]		
10	OEM's Authorization Form	Annexure VII [On the letterhead of the OEM]		

The bidder is required to submit the self-attested photocopies of the following documents along with the Technical Bid, failing which their bids may be summarily/outrightly rejected and may not be considered:

Authorized Signatory (Signature In full): _____

Name and title of Signatory: _____
Stamp of the Company: _____

Annexure – I: *LIST OF ITEMS PROPOSED TO BE SUPPLIED*

DETAILS OF BILL OF MATERIAL HARDWARE. SOFTWARE AND OPERATIONS COST

(Cost is an estimate to arrive at the project Cost. This is not in any way related to award of PO. Shortlisted SI will be given the RFP for bidding for the Project)

SNo	**Description**	**Supplier/ make or Model/Version**	**Unit of Measurement**	**Number of Units** (estimated)%%	**Software Licenses recommended** Share details of OS, Virtualisation Software, VM , Database etc	
1	**1 Gbps Leased Line connection (1:1) with end point connectivity**					
2	GPU server NVIDIA H200 with Virtualisation software for NVIDIA (details to be mentioned in software table)			4 Node (32 GPU H200)	**Open Source SW** 1. OS : 2. Virtualisation SW 3. … 4. ……	
					Proprietary SW 1. 2 3.	
3	Inference Node Server			2		
4	Misc node consisting of			24		
5	SAN Storage			1		
5	HPC storage			1		
6	Network and Management Switches [$]					
	(a) IB Switch			2		
	(b) Data Centre NW Switch			2		

	(c) Management Switch			1/2		
	(d) Access Switch			2		
	(e) Any other switch recommended					
7	Incubation Centre Workstations (For Delhi and Banglore) + Five external HDD 1TB capacity			105+5 external HDD		
8	Incubation Center Conference Rooms Equipment's (LED Screen 75Inch and VoIP Equipment)			3* X conference room * One conference room at banglore		
9	Networking and connections within Data centre inclusive of connectors cables etc					
10	##Networking and Wiring for Incubation Centre (Estimated 10,000 Sq Feet for 90 Workstations)					
11	Cyber Security Suite					
	(a) Next-Generation Firewall					
	(b) Endpoint Detection and Response with sandboxing					
	(c) Host Intrusion prevention System					
	(d) Storage Security					
	(e) Security Information and Event Management (SIEM)					
12	Smart Racks Solution					
13	Warranty for 3 Years With Support for 3 years					
SOFTWARE REQUIRED (As per requirement of SI implementation plan) OPEN SOURCE ALSO TO BE MENTIONED						

Sno	**Description**	**Open Source OR Proprietary** (Mention Supplier and Model/Version)	**No of Licenses required**	**Justification for licenses**	Estimated Cost of	
1	**Virtualisation Licenses VMware vSphere Enterprise**		**12**			
2						
3						
4						
For Nodes (management Node, Control Node, Other Misc Nodes)						
1						
2						
3						
For Cyber Security						
1						
2						
3						
4						
OPERATIONAL COST FOR 24X7 upto Dec 12 Months from date of Installation						
	Description	**Justification**	**Estimated cost per month**	**Total Cost**		

1	**Manpower**					
2.	**Other costs**					

%% Vendor can suggest amended quantity as per his proposed plan
$ NOTE: For NW the Data centre would be connected to the incubation centre by Fiber and redundancy has to be catered for. Number of NW terminals estimated would be 48X3 i.e. 144 Nodes. No of switches estimated are 2 IB , 2 Data center, 1 Management and 2 Switches for Distribution
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.

ESTIMATED COST OF THE BOM

SI is requested to share the cost in the following categories to arrive at a budget cost

Category	Estimated Cost	Remarks by SI	Remarks by FITT
Compute Hardware including NW and Switches			Should include all Servers, NW switches , Connectors etc
Compute Software for Proprietary/Open source SW			Include SW cost like Virtualisation SW NVIDIA, VM Ware, Database etc
Smart racks with Accessories and installation			
Cyber Security HW			Cost of HW like NGFW etc
Cyber Security for Proprietary/Open source SW			
Incubation Centre HW			Workstations, Conference room equipment etc
Incubation Centre SW			OS, MS Office etc
Warranty Cost			Cost of 3 years+ any cost with 3 Years OS
Operation's cost			Cost of support upto 12 Months from date of Installation

Annexure II Bidder Details

[on the letterhead of the bidder]

1	Name of the Firm/ Company		
2	Offered Product Name, Make and Model* Item wise details in the table given below with estimated cost		
4	Name and Designation of Authorized Signatory		
5	Office Address of the Firm/ Communication Address:		
6	Phone No. / Mobile No:		
7	E-Mail ID:		
8	GST registration Number:		
9	PAN Number:		
10	Firm's Bank Account details	Bank Account No.:	
		Name of the Bank:	
		IFSC Code No:	
		Name of Branch:	
Particular Details of the Bidders Representative			

11	Contact Person: / Mobile No:	Name of Person:	
		Designation:	
		Tele / Mobile No:	
		E-Mail ID:	

Authorized Signatory (Signature In full): _____

Name and title of Signatory: _____

Stamp of the Company: _____

Item Wise details (SI can propose the Quantities or Change in Specifications as per the solution being offered)

Annexure III: DECLARATION

[On the letterhead of the Bidder]

I, _____ Son/Daughter/Wife of_____ Resident of _____

_____ Proprietor / Director / Authorized Signatory of the Company / Firm, mentioned above, is competent to sign this declaration and execute this EOI document;

I/We hereby certify that I/We have read the entire terms and conditions of the EOI documents from Page No. _____ to _____ (including all documents like annexure(s), etc.,). I/We shall abide hereby by the terms/conditions/clauses contained therein.

The information/documents furnished along with the above application are true and authentic to the best of my knowledge and belief. I/we are well aware of the fact that furnishing any false information / fabricated document would lead to rejection of my EOI at any stage besides liabilities towards prosecution under appropriate law.

The corrigendum(s) issued from time to time by your department/organization, too, have all been taken into consideration while submitting this declaration letter.

I/We hereby unconditionally accept the EOI conditions of the above-mentioned EOI document(s) in its total/entirety.

In case any provision of this EOI is found violated, then your department/organization shall, without prejudice to any other right or remedy, be at liberty to reject this EOI/bid.

Authorized Signatory (Signature In full): _____

Name and title of Signatory: _____

Stamp of the Company: _____

Annexure IV: DECLARATION REGARDING BLACKLISTING/NON-BLACKLISTING

CERTIFICATE [On the letterhead of the Bidder]

I /We, Proprietor / Partner (s) / Director (s) of M/s _____, hereby declare that the firm/ company, namely M/S _____, has not been blacklisted or debarred in the past by any Government Department/State Govt.//PSU/Municipal Corporation/other Govt. Bodies from taking part in Government EOIs as on the date of submission of proposals. Or

I / We, proprietor/partner (s) / Director (s) of M/S _____hereby declare that the firm/ company namely M/S_____ was blacklisted or debarred by any Government Department/State Govt.//PSU/Municipal Corporation/other Govt. Bodies from taking part in Government EOIs for a period of _____ years w.e.f _____The period over on _____And now the firm/ company is entitled to take part in Government EOI. In case the above information is found false, I/we am/are fully aware that the EOI/ contract will be rejected/cancelled by the FITT, IIT Delhi, and the EMD/Performance Bank Guarantee shall be forfeited. In addition to the above, FITT, IIT Delhi Will not be responsible for paying the bills for any completed/ partially completed work.

Signature: …….

Name: …….

Capacity in which as signed: ……

Name & address of the firm: …….

Seal of the firm should be affixed.

……

Dated: Signature of Bidder with seal.

In the case of a proprietorship firm, the certificate will be given by the proprietor, and in the case of a partnership firm, the certificate will be given by all the partners, and in the case of the limited company, by all the Directors of the company or company secretary on behalf of all directors.

Annexure- V FINANCIAL CAPABILITY OF BIDDER [On the letterhead of the Bidder]

Annual turnover details of the Bidder from [insert relevant details]

#	Financial Year	Turnover in Indian Rupees	Document Page No.
A	2021-2022		
B	2022-2023		
C	2023-2024		

*An audited balance sheet and profit & loss account statement for the bidder for each of the abovementioned financial years shall be submitted as supporting evidence.

1. Please affix the signature of the authorized signatory of the Bidder with name, designation, seal, and date here.

2. **Please affix the signature of the authorized signatory of the statutory auditor of the Bidder with name, designation, seal, and date here.**

Authorized Signatory

Name and title of Signatory:

(Signature in full):

Stamp of the Company:

Authorized Signature of Statutory Auditor:

Stamp of the firm

Annexure VI Details of works of similar* type executed by the Bidder

[On the letterhead of the Bidder]

Sl. No.	Name of the Company	Work Description	Ref. & Date of the order	Work Order Value	Contract Period	Work Status (if completed, provide the contact of the work assigning authority)	Page No

Authorized Signatory (Signature In full): _____

Name and title of Signatory: _____

Stamp of the Company: _____

Please Note: Copies of work orders should be attached with this information. In the absence of documentary evidence, the bid is liable to be rejected.

Annexure VII : OEM authorisation Letter for all products

(ON OEM LETTER HEAD)

[OEM's Official Letterhead - Including Logo, Name, Address, Contact Info]

[Date]

To: [Name of Purchasing Authority / Tender Committee / Relevant Department] [Address of Purchasing Authority] [City, State/Province, Zip/Postal Code]

Subject: OEM Authorization Letter for [Reseller/Partner Company Name] for [Tender Reference Number / Project Name, if applicable]

Dear Sir/Madam,

This letter hereby confirms and certifies that **[Full Legal Name of OEM Company]**, with its principal place of business at [OEM's Full Address], is the Original Equipment Manufacturer (OEM) of the [Specify Product/Product Line, e.g., "servers," "networking equipment," "video conferencing solutions," "software"] relevant to the aforementioned [Tender Reference Number / Project Name, if applicable].

We officially authorize **[Full Legal Name of Reseller/Partner Company]**, with its principal place of business at [Reseller/Partner's Full Address], to act as our **[Specify Role: e.g., "Authorized Reseller," "Authorized Partner," "Authorized Bidder," "Authorized Service Provider"]** for the purpose of [Clearly state the purpose, e.g., "submitting a proposal," "selling," "distributing," "providing technical support"] our [Specify Product/Product Line] products/solutions in connection with the [Tender Reference Number / Project Name, if applicable] issued by [Your Company/Organization Name, if known].

Specifically, this authorization extends to the following products/solutions:

- [List specific product models or general product categories, e.g.:]

- [Product Model 1]
- [Product Model 2]
- [Product Category, e.g., "All our X-Series Servers"]
- [Associated software and services]

We confirm that **[Full Legal Name of Reseller/Partner Company]** is fully authorized to provide our products and solutions. We, as the OEM, commit to providing the necessary support, technical information, warranty, and spare parts for the products supplied by **[Full Legal Name of Reseller/Partner Company]** for the duration specified in the tender/contract.

This authorization is valid from **[Start Date]** to **[End Date]** OR for the entire duration of the [Tender Reference Number / Project Name, if applicable], including any potential extensions or contract periods resulting from this tender.

We hereby attest that all information provided by **[Full Legal Name of Reseller/Partner Company]** regarding our products and their specifications, as submitted in response to the [Tender Reference Number / Project Name, if applicable], is accurate and has our full endorsement.

For any verification or further information regarding this authorization, please feel free to contact us using the details below.

Thank you for your time and consideration.

Authorized Signatory (Signature In full): _____

Name and title of Signatory: _____

Stamp of the Company: _____