

संख्या. पी-63013/231/01/2025/मोड-1/सीसुबल 325-36

भारत सरकार, गृह मंत्रालय
महानिदेशालय सीमा सुरक्षा बल
(रसद निदेशालय: आधुनिकीकरण सैल)
(Email-comdtord@bsf.nic.in)
(Fax: 011-24367683)

ब्लाक संख्या . 10,
सीजीओ काम्पलैक्स,
लोधी रोड, नई दिल्ली-03
दिनांक 11 फरवरी 2026

सेवा में,

महानिदेशक:- आसाम राईफलस (through LOAR), केन्द्रीय ओद्योगिक सुरक्षा बल,
केन्द्रीय रिजर्व पुलिस बल, भारतीय तिब्बत बोर्डर पुलिस, सशस्त्र सीमा बल,
राष्ट्रीय सुरक्षा गार्ड एवं पुलिस अनुसन्धान एवं विकास ब्योरो

विषय: अनुमोदित गुणात्मक आवश्यकता /परीक्षण निर्देशों का प्रेषण

तकनीकी विशेषज्ञों के उप समूह द्वारा किए गये सूत्रीकरण एवं महानिदेशक सीमा सुरक्षा बल द्वारा अनुमोदित "Smart Border Observation & Monitoring System" उपकरण के गुणात्मक आवश्यकता/परीक्षण निर्देशों को आपकी अग्रिम कार्यवाही हेतु प्रेषित किया जाता है।

संलग्न : उपरोक्तनुसार

आनन्द सिंह
(आनन्द सिंह तक्षक) 11/2/26
उप महानिरीक्षक (रसद)
11/02/2026

प्रतिलिपि :-

1. तकनीकी निदेशक
The Technical Director
राष्ट्रीय सूचना-विज्ञान केन्द्र, नोर्थ ब्लाक,
गृह मंत्रालय, नई दिल्ली
NIC, North Block, MHA
New Delhi (द्वारा ई-मेल)
(ई-मेल पता : mpsugandhi@nic.in)
: आपसे अनुरोध है कि उक्त उपकरण के गुणात्मक आवश्यकता /परीक्षण निर्देशों को गृह मंत्रालय की वैबसाईट (पुलिस आधुनिकीकरण संभाग) के गुणात्मक आवश्यकता पोर्टल में मशीनरी एवं उपकरण के साथ निगरानी उपकरण वर्ग के अर्न्तगत अपलोड करने का श्रम करें।
2. SO (IT), North Block, MHA
(Through E-mail)
(E-mail address: soit@nic.in)
: कृपया उपरोक्तानुसार कार्यवाही करने का श्रम करें।
3. Sh. Samarth Sharma,
Director Nodal Officer for MHA GeM,
3rd Floor, Jeevan Bharti Building
Conaught Lane, Janpath Cannaught
Place, N/ Delhi-110001
E-mail:directorcategory13@gem.gov.in
For info with request to upload the approved QRs & TDs of "Smart Border Observation & Monitoring System" on GeM Portal. Copy of QRs & TDs is attached with this letter.
4. तकनीकी विंग, सीमा सुरक्षा बल
: कृपया उक्त उपकरण के गुणात्मक आवश्यकता/परीक्षण निर्देशों को सीमा सुरक्षा बल की वैबसाईट पर अपलोड करने का श्रम करें।
5. संक्रिया निदेशालय (तकनीकी अनुभाग)
बल मुख्यालय सीमा सुरक्षा बल।
: आपके यूओ संख्या-21058 दिनांक 28.11.2025 के सन्दर्भ में अनुमोदित उपकरण के गुणात्मक आवश्यकता/परीक्षण निर्देशों को आपके सूचनार्थ एवं अग्रिम कार्यवाही हेतु प्रेषित जाता है।
6. फाईल।

QUALITATIVE REQUIREMENTS & TRIAL DIRECTIVES OF SMART BORDER OBSERVATION & MONITORING SYSTEM

Part-I

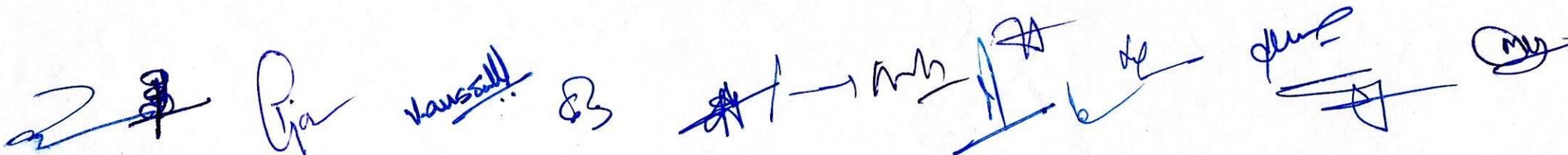
Nomenclature of Eqpt: SMART BORDER OBSERVATION & MONITORING SYSTEM

1. Trial/ technical evaluation of equipment will be conducted by a Board of Officers (B.O.O) in the presence of vendor or representative of firm to assess actual performance of the equipment.
2. All specifications/ parameters of equipment mentioned in the QRs will be checked by B.O.O during the trial by ascertaining/ verifying in the following ways:
 - (a) **PHYSICAL CHECK**: - In this category, specifications of the equipment will be checked by B.O.O. physically as per QRs/ TDs.
 - (b) **FUNCTIONAL CHECK**: - In this category, Vendor/ Supplier will show practically all features/ configurations to the board of officers during trial.
 - (c) **SUBMISSION OF CERTIFICATE**: - Specification which cannot be checked due to lack of testing facilities/ expertise, certificate(s) will be provided by the vendor, issued by a Government Authorized Laboratory/ International accredited laboratory or OEM as specified against the parameter, and will be acceptable by B.O.O. during trial.

Part-II

GENERAL INFORMATION

- i) The system at Bn level will enable central C2 with video analysis & management for deployed cameras along the border for generating alerts and analyzing incidents of intrusion detection creating virtual fencing, camera tampering and abandoned object detection. This will reduce human intensive efforts at monitoring stations.
- ii) Video Analytics Server (VA) will ingest live video streams directly from existing or new CCTV cameras using RTSP streams or through VMS/NVR. These streams will be processed in real time on the VA server, enabling immediate analysis and generation of alerts. Each alert generated will include detailed metadata such as camera location, timestamp, and other contextual information. This ensures accurate alerting, logging, and rapid response from the application and operational teams.

A series of handwritten signatures and initials in blue ink, including names like 'Pia', 'Kaus', and 'B3', along with various scribbles and marks.

Part -III

Qualitative Requirements and Trial Directives

1. VIDEO MANAGEMENT SOLUTION

Srl No.	Capability Required	Qualitative Requirements	Trial directives
1.1	User Interface	The system should be easy to install, learn, operate and manage. The VMS must have rich user interface that provides one click access, drag drop, menu, customizable GUI etc. to enhance operational efficiently in daily tasks and maintain. The VMS shall have ability to respond fast & shall be applicable to all processes, functions, features, and screens of a video management system.	BOO to check physically.
1.2	Scalability	The proposed video management system shall be able to support any no. of CCTV Cameras so as to accommodate any future expansion. System shall support viewing of video from multiple locations and by multiple users. The VMS shall support more than 500 or More cameras. The VMS shall have ability to receive and support recordings based on inputs or alarms, event management. Support for Standard protocols The VMS shall have ability to maintain independence from any one vendor & shall support open standard protocol i.e. ONVIF .	BOO to check physically.
1.3	On screen help and instructions	The system should provide help and assistance through help guide on same station.	BOO to check physically.
1.4	User management	User management with user roles & privileges right to view, update shall be available.	BOO to check physically.
1.5	Centrally controlled user management	Users, roles, rules, and privileges should be stored on the central VMS server allowing any authorized user to log into any workstation.	BOO to check physically.
1.6	Recording Server	The system shall not restrict the number of recording camera, Shall support dual streaming, shall support recording in all resolution at desired FPS, it should support video cum audio	BOO to check physically.

A collection of handwritten signatures and initials in blue ink, including names like 'Bin', 'Kausally', and various initials and symbols.

		recording. The system should Support for event based or schedule based recordings to optimize bandwidth and storage.	
1.7	Access Privileges	The VMS shall have ability to configure access privileges and other parameters for all users.	BOO to check physically.
1.8	Installation and updates	Wizard driven installation of software updates for VMS server and client machines. The VMS shall have ability to enforce access privileges (view /add /edit/ Remove) to device (s).	BOO to check physically.
1.9	Addition and removal of sensors	The VMS shall have ability to easily install, configure, modify, search and remove surveillance devices with automatic discovery of IP devices using external tool or in built options.	BOO to check physically.
1.10	Creation of Camera Groups	The VMS shall have ability to logically group device based on installation location & device type. The VMS shall have ability to search and view devices based on standard criteria like camera ID/Name, Location, Group, etc.	BOO to check physically.
1.11	Basic Recording Functions	Basic recording options (Full, Scheduled recoding, Motion detection recording, external/internal hardware or software events / trigger-based recording).	BOO to check physically.
1.12	PTZ Controls	When PTZ is deployed and enabled, system should offer a separate Control panel for PTZ operations. The control panel should include list of pre-sets, patterns, tours, eight directional & home positions and zoom-in & zoom-out buttons.	BOO to check physically.
1.13	Display Screens	All panes / tiles should indicate mode (live or recoded), source (camera name/location) and date/time and applied quality information (FPS, CODEC). A matrix view should support minimum 2x2, 3x3, 4x4 on small monitors and 9x9 formats on video wall and any number of multiple screen divisions.	BOO to check physically.
1.14	Video Replay	Replay facility with timeline control to display and play back recorded video for one or more cameras. Playback shall be possible on 1 or more cameras simultaneously for all cameras currently displayed in the Video Workspace. System should allow creating a still image from live or recorded feed and storing it into a workstation. The system should offer playback controls Play/Pause Forward playback Reverse playback Frame forward frame rewind.	BOO to check physically.

[Handwritten signatures]

Naussull

Par

[Handwritten signatures and notes]

[Handwritten signature]

1.15	Video Bookmark	The VMS shall have ability to bookmark / add-to-favourites in both live and playback modes. Bookmarks shall be created, searched, removed by the owner.	BOO to check physically.
1.16	Evidence export feature	The system should allow users to export audio/video evidence in open format for internal investigation or to share authentic proof to public authorities and outside agencies.	BOO to check physically. Firm to provide OEM certificate also in this regard.
1.17	Video Search	The VMS shall provide an advanced search of recorded video. The search shall be based on recording time, camera and recording details.	BOO to check physically.
1.18	Video Extract	The facility should be there to extract & save the video footages / images on CD, DVD, USB, External Storage etc.	BOO to check physically.
1.19	Loading layouts	Load selected layout from the saved layouts. Default Layout should automatically get launched when the controller boots up.	BOO to check physically.

2. VIDEO ANALYTICS SOLUTION

S. No.	Capability Required	Qualitative Requirement	Trail Directives
2.1	Unified AI Platform	The software offered shall be a unified AI Platform capable of running all video analytics use cases on a single system. It shall support all video analytics use-cases, traffic use-cases and AI on other sensors' data for this project.	The BOO to check physically and Firm to submit OEM certificate in this regard.
2.2	Cluster based Deployment	The software platform should run on a cluster of servers and compute-devices as per the proposed hardware sizing which can dynamically support any use-case without hard-coding or logging specifically into the server/compute device. This should allow one singular UI to run/deploy/update all the workload on the compute nodes in the cluster.	The BOO to check physically.
2.3	Seamless Application Deployment	The platform must support the addition and deployment of new applications across the camera infrastructure (subject to field of view and hardware compatibility). This process should be executable without any system downtime, allowing for real-time application uploads and license activation.	The BOO to check physically and Firm to submit OEM certificate in this regard.

2.4	Status of cameras/ Sensors	The user interface shall have a matrix to assign, start, stop and schedule any use case on any camera. The status of active and non-active use cases shall be clearly visible with colour coded information.	The BOO to check physically.
2.5	Modular and Scalable Architecture	The system should be designed with a modular architecture that supports scalability. In scenarios where there is an expansion in the number of cameras or the addition of servers, the platform must remain fully operational without requiring any software shutdown or interruption to services.	The BOO to check physically and Firm to submit OEM certificate in this regard.
2.6	Dynamic Dashboard Creation	The platform should have user-driven dashboards for data-visualization with widget based charts and graphs.	The BOO to check physically.
2.7	Map support	The platform should support GIS maps to show cameras, alerts search features and deploying of AI use-cases on the cameras from the map itself.	The BOO to check physically.
2.8	Geo-location based alert forwarding	The platform should support geo-location based alert forward to the QRTs deployed in field, so that they can take appropriate actions to the alerts within their pre-defined radius.	The BOO to check physically.
2.9	Real-time analytics processing	<p>The system should have real-time analytics processing with < 1-2 sec response for following incidents :-</p> <p>a) Intrusion Detection (smart Motion Detection)- The system detects whether a person/vehicle/animal has crossed a user defined line (virtual trip-line) or region in a specific direction. The alert will be classified as intrusion.</p> <p>b) Camera Health and Tampering – Alerts are generated when the view of the camera is either obstructed by an object or flashed by light or moved or blurred.</p> <p>c) Abandoned Object Detection - Raises an alert when an object is abandoned for more than set threshold time.</p>	The BOO to check physically and Firm to submit OEM certificate in this regard.

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

2.10	Accuracy	The system should have very less False positives/negatives. The overall accuracy of the system should be more than 90%.	The BOO to check physically.
2.11	Human in the Loop. AI Learning and Improvement	The system shall have an inbuilt reporting, annotation and labelling tool that allows a user to report, label and update the AI models with datasets based on user feedback from any mismatched or misreported alerts. The AI in video Analytics system shall be deterministic and non-hallucinating, ensuring outputs are strictly on validated models without speculations. There should be provision for Trg of model by user inputs.	The BOO to check physically and Firm to submit OEM certificate in this regard.
2.12	Alert and Event Views	The result of each of the use case shall be in the form of events that contain the screenshot with other metadata describing the event, such as detected objects, timestamp, camera/video that generated the event and all other metadata representing the event from different use cases. The User Interface shall have a grid and list view with all the events from different use cases, cameras etc.	The BOO to check physically and Firm to submit OEM certificate in this regard.
2.13	Multi-user Web Client	The User based access and interface of the system shall be a web-interface that can be accessed from any system in the local area network (LAN) or wide area network (WAN) with login credentials. It shall allow multiple users to log in at the same time, and receive real-time alerts and notifications.	The BOO to check physically and Firm to submit OEM certificate in this regard.
2.14	Live Video Interface	The User interface shall allow a user to view the live video stream from any camera with overlaid information of regions, objects, people and vehicles based on each of the use-case	The BOO to check physically.
2.15	Search parameters	The system shall allow a user to filter and retrieve all the events based on any combination of the following parameters, like time of the event, objects in the event and type of the use-case	The BOO to check physically and Firm to submit OEM certificate in this regard.
2.16	Video Tagging for Live events	To save the duplication of the video storage, the analytics should flag the video for the configurable duration of time pre and post event in the Video Management System. It should be possible for the operator to jump to the alert flag in the archived video for detailed investigation of the event.	The BOO to check physically.

A series of handwritten signatures and initials in blue ink are located at the bottom of the page. From left to right, they include: a large stylized signature, a signature that appears to be 'Pin', a signature that appears to be 'Kumar', a signature that appears to be 'PS', a signature that appears to be 'A', a signature that appears to be 'M', a signature that appears to be 'K', a signature that appears to be 'S', and a circled signature that appears to be 'M'.

2.17	VAPT Report	The unified AI based Video Intelligence Platform shall have a recent VAPT report conducted by a CERT-In empanelled auditor (within the last 12 months), or the OEM shall commit to complete the VAPT before Joint Receipt Inspection (JRI).	The BOO to check physically and Firm to submit OEM certificate in this regard.
------	-------------	---	--

3 VMS Server

Sno.	Item	Qualitative Requirements	Trial Directives
3.1	Chassis	1U/2U Rack Mountable.	The BOO to check physically.
3.2	CPU	Two numbers of 4th Generation Intel® Xeon® Scalable Processor 32 Core having 2.1 Ghz or Better.	The BOO to check physically and Firm to submit OEM certificate in this regard.
3.3	Chipset	Intel® C741 Chipset or better	The BOO to check physically and Firm to submit OEM certificate in this regard.
3.4	Memory	32DIMM slots. 512 GB Memory scalable upto 4.0 TB using DDR5 Registered DIMM (RDIMM) operating at 4800 MT/s.	The BOO to check physically and Firm to submit OEM certificate in this regard.
3.5	Bus Slots	Server should support upto eight PCI-Express 5.0 x16 slots. Additional two x8 or higher PCIe 5.0 slots.	The BOO to check physically and Firm to submit OEM certificate in this regard.
3.6	BOOT optimized storage	3 x 1.92 TB SATA SSD.	The BOO to check physically.
3.7	HDD Bays	8 SFF SAS/SATA/SSD/NVMe.	The BOO to check physically.
3.8	Controller	Server should support one of the 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.	The BOO to check physically and Firm to submit OEM certificate in this regard.
3.9	Networking features	Server should support below networking cards: 2 x 10Gb 2-port with SR SFP+.	The BOO to check physically.

2 *Ria*

Kanav

Handwritten signature

Handwritten signature

MS

3.10	Interfaces	Serial - 1 (Optional) USB support with Up to 5 total: 1 front, 2 rear, 2 internal. 1GbE Dedicated management port.	The BOO to check physically.
3.11	Power Supply	Should support hot plug redundant low halogen power supplies with minimum 94% efficiency.	The BOO to check physically and Firm to submit OEM certificate in this regard.
3.12	Fans	Redundant hot-plug system fans.	The BOO to check physically.
3.13	Industry Standard Compliance	ACPI 6.3 Compliant or better PCIe 5.0 Compliant or better WOL Support or better Microsoft® Logo certifications or better PXE Support or better Energy Star or better SMBIOS 3.2 or better UEFI 2.7 or better Redfish API or better IPMI 2.0 or better Secure Digital 4.0 or better Advanced Encryption Standard (AES) or better Triple Data Encrytion Standard (3DES) or better SNMP v3 or better TLS 1.2 or better DMTF Systems Management Architecture for Server Hardware Command Line Protocol (SMASH CLP) or better Active Directory v1.0 or better ASHRAE A3/A4 or better H-265 or better	The BOO to check physically and Firm to submit OEM certificate in this regard.

3.14	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 Configurable for PCI DSS compliance TPM (Trusted Platform Module) 2.0 option Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) 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	The BOO to check physically and Firm to submit OEM certificate in this regard
3.15	Operating Systems and Virtualization Software Support	Windows Server 2025 Standard Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) VMware ESXi. Canonical Ubuntu Oracle Linux and Oracle VM Citrix	The BOO to check physically and Firm to submit OEM certificate in this regard.
3.16	Provisioning	i) Should support tool to provision server using RESTful API to discover and deploy servers at scale ii) Provision one to many servers using own scripts to discover and deploy with	The BOO to check physically and Firm to submit OEM certificate in this regard.

A series of handwritten signatures and initials in blue ink are located at the bottom of the page. From left to right, they include: a stylized '2', a signature that appears to be 'Pim', the name 'Kanswill' with a checkmark, the initials 'ES', a signature that looks like 'dep', another signature 'MH', a signature 'A', a signature 'J', and a circled signature 'M'.

		Scripting Tool (STK) for Windows and Linux or Scripting Tools for Windows PowerShell.	
3.17	Firmware security	<p>i). 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</p> <p>ii). Should maintain repository for firmware and drivers recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery setup preloaded to rollback to factory tested secured firmware.</p>	The BOO to check physically and Firm to submit OEM certificate in this regard.
3.18	Virtualization Software	Server to be offered with Enterprise Virtualization software licences to be offered & configured with sever, Licences to be factored for 3 Year support & must be offered for all the cores – 64 Core offered with server. Virtualization software must be Enterprise Virtualization software supporting key features VM - Live Migration, High availability, dynamically schedule the placement of virtual machines, Storage Migration. Further in addition, it must integrate to external storage also.	The BOO to check physically and Firm to submit OEM certificate in this regard.
3.19	Embedded Remote Management and firmware security	<p>i) 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.</p> <p>ii) Server should have dedicated 1Gbps remote management port.</p> <p>iii) 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.</p> <p>iv) Server should support agentless management using the out-of-band remote management port.</p>	The BOO to check physically and Firm to submit OEM certificate in this regard.

A collection of handwritten signatures and initials in blue ink, including a large signature on the left, a signature that appears to be 'Kaus...' in the middle, and several other initials and signatures on the right, some with arrows pointing to specific parts of the table above.

v) 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.

vi) Two factor Authentication.

vii) Local or Directory-based user accounts with Role based access control.

viii) 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 and 3DES on browser. Should provide remote firmware update functionality. Should provide support for Java free graphical remote console.

ix) Should support managing multiple servers as one via Power Control Group Power Capping Group Firmware Update Group Configuration Group Virtual Media and Encrypted Virtual Media Group License Activation.

x) Should support RESTful API integration.

xi) System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support.

xii). 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.

xiii) One-button Secure Erase designed to decommission/repurpose servers.

xiv) NVMe wear level display.

Handwritten signature

Handwritten signature

Handwritten initials

Handwritten signature

Handwritten signature

Handwritten signature

Handwritten initials

		xv) Workload Performance Advisor - Provides server tuning recommendations to improve server performance.	
3.20	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 BOO to check physically and Firm to submit OEM certificate in this regard.
		The Dashboard minimum should display a health summary of the following: <ul style="list-style-type: none"> • Server Profiles • Server Hardware • Appliance alerts 	
		The Systems Management software should provide Role-based access control.	The BOO to check physically.
		Zero Touch Provisioning (ZTP) using SSDP with remote access.	The BOO to check physically and Firm to submit OEM certificate in this regard.
		Management software should support integration with popular virtualization platform management software like VMware vCenter & vRealize Operations, and Microsoft System Center & Admin Center.	The BOO to check physically and Firm to submit OEM certificate in this regard.
		Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD.	The BOO to check physically and Firm to submit OEM certificate in this regard.
		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 health, 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 private cloud).	The BOO to check physically and Firm to submit OEM certificate in this regard.
		Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.	The BOO to check physically and Firm to submit OEM certificate in this regard.

A collection of handwritten signatures and initials in blue ink, including a large signature on the left, a signature that appears to be 'Kauso...', and several other initials and scribbles scattered across the bottom of the page.

	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 BOO to check physically and Firm to submit OEM certificate in this regard.
	The Server Management Software should be of the same brand as of the server supplier.	The BOO to check physically and Firm to submit OEM certificate in this regard.

4. GPU SERVERS FOR VIDEO ANALYTICS SOLUTION

S/No.	Item	Qualitative Requirements	Trial Directives
4.1	Chassis	1U/2U Rack Mountable.	The BOO to check physically.
4.2	CPU	Two numbers of 4th Generation Intel® Xeon® Scalable Processor 32 Core having 2.1 Ghz or Better.	The BOO to check physically and Firm to submit OEM certificate in this regard.
4.3	Chipset	Intel® C741 Chipset or better.	The BOO to check physically and Firm to submit OEM certificate in this regard.
4.4	Memory	32DIMM slots. 512 GB Memory scalable upto 4.0 TB using DDR5 Registered DIMM (RDIMM) operating at 4800 MT/s	The BOO to check physically and Firm to submit OEM certificate in this regard
4.5	Graphic Card	1 Nos of NVIDIA L40S 48GB (CUDA Compliant) , PCIe Accelerator or Equivalent.	The BOO to check physically and Firm to submit OEM certificate in this regard.
4.6	Bus Slots	Server should support upto eight PCI-Express 5.0 x16 slots. Additional two x 8 or higher PCIe 5.0 slots.	The BOO to check physically and Firm to submit OEM certificate in this regard.
4.7	BOOT optimized storage	3 x 1.92 TB SATA SSD.	The BOO to check physically and Firm to submit OEM certificate in this regard.
4.8	HDD Bays	8 SFF SAS/SATA/SSD/NVMe.	The BOO to check physically and Firm to submit OEM certificate in this regard.
4.9	Controller	Server should support one of the below controllers, must support Mixed Mode which combines RAID and HBA mode operation simultaneously:	The BOO to check physically and Firm to submit OEM certificate in this regard.

		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.	
4.10	Networking features	Server should support below networking cards: 2 x 10Gb 2-port with SR SFP+.	The BOO to check physically and Firm to submit OEM certificate in this regard.
4.11	Interfaces	Serial-1(Optional) USB support with Up to 5 total: 1 front,2 rear & 2internal. 1GbE Dedicated management port.	The BOO to check physically.
4.12	Power Supply	Should support hot plug redundant low halogen power supplies with minimum 94% efficiency.	The BOO to check physically and Firm to submit OEM certificate in this regard.
4.13	Fans	Redundant hot-plug system fans.	The BOO to check physically.
4.14	Industry Standard Compliance	ACPI 6.3 Compliant or better PCIe 5.0 Compliant or better WOL Support or better Microsoft® Logo certifications or better PXE Support or better Energy Star or better SMBIOS 3.2 or better UEFI 2.7 or better Redfish API or better IPMI 2.0 or better Secure Digital 4.0 or better Advanced Encryption Standard (AES) or better Triple Data Encryption Standard (3DES) or better SNMP v3 or better TLS 1.2 or better	The BOO to check physically and Firm to submit OEM certificate in this regard.

[Handwritten signature]

Kausall

[Handwritten mark]

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

		DMTF Systems Management Architecture for Server Hardware Command Line Protocol (SMASH CLP) or better Active Directory v1.0 or better ASHRAE A3/A4 or better	
4.15	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 Configurable for PCI DSS compliance TPM (Trusted Platform Module) 2.0 option Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) 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	The BOO to check physically and Firm to submit OEM certificate in this regard.
4.16	Operating Systems and Virtualization Software Support	Windows Server 2025 Standard Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) VMware ESXi. Canonical Ubuntu Oracle Linux and Oracle VM Citrix	The BOO to check physically and Firm to submit OEM certificate in this regard.

4.17	Provisioning	<p>(i) Should support tool to provision server using RESTful API to discover and deploy servers at scale.</p> <p>(ii) 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.</p>	The BOO to check physically and Firm to submit OEM certificate in this regard.
4.18	Firmware security	<p>i). 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.</p> <p>ii). 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.</p>	The BOO to check physically and Firm to submit OEM certificate in this regard.
4.19	Embedded Remote Management and firmware security	<p>i). 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.</p> <p>ii). Server should have dedicated 1Gbps remote management port.</p> <p>iii). 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.</p> <p>iv) Server should support agentless management using the out-of-band remote management port.</p>	The BOO to check physically and Firm to submit OEM certificate in this regard.

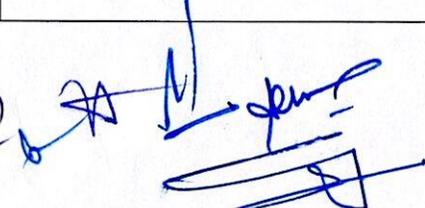
A collection of handwritten signatures and initials in blue ink, including a large signature on the left, a signature that appears to be 'Kauswell', and several other initials and scribbles scattered across the bottom of the page.

	<p>v. 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.</p> <p>vi). Two factor Authentication.</p> <p>vii). Local or Directory-based user accounts with Role based access control.</p> <p>viii). 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 and 3DES on browser. Should provide remote firmware update functionality .Should provide support for Java free graphical remote console.</p> <p>ix). 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.</p> <p>x). Should support RESTful API integration</p> <p>xi). System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support.</p> <p>xii). 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.</p>	
--	--	--










		<p>xiii). One-button Secure Erase designed to decommission/repurpose servers.</p> <p>xiv). NVMe wear level display.</p> <p>xv). Workload Performance Advisor - Provides server tuning recommendations to improve server performance.</p>	
4.20	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 BOO to check physically and Firm to submit OEM certificate in this regard.
		<p>The Dashboard minimum should display a health summary of the following:</p> <ul style="list-style-type: none"> • Server Profiles • Server Hardware • Appliance alerts 	The BOO to check physically and Firm to submit OEM certificate in this regard.
		The Systems Management software should provide Role-based access control.	The BOO to check physically and Firm to submit OEM certificate in this regard.
		Zero Touch Provisioning (ZTP) using SSDP with remote access.	The BOO to check physically and Firm to submit OEM certificate in this regard.
		Management software should support integration with popular virtualization platform management software like Vmware vCenter & vRealize Operations, and Microsoft System Center & Admin Center.	The BOO to check physically and Firm to submit OEM certificate in this regard.
		Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD.	The BOO to check physically and Firm to submit OEM certificate in this regard.
		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	The BOO to check physically and Firm to submit OEM certificate in this regard.

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

	contracts and status. The Portal should also provide a personalised dashboard to monitor device health, hardware events, and 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 private 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.	The BOO to check physically and Firm to submit OEM certificate in this regard.
	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 BOO to check physically and Firm to submit OEM certificate in this regard.

5. QRS/TECHNICAL SPECIFICATION OF STORAGE

S/ No.	Qualitative Requirements	Trail Directives
5.1	Offered Storage must have scale-up and scale-out architecture for SAN and NAS protocols asked, it must scale to 8 or more controllers for future expansion. It must support mixing of controllers within same generation and across generation of controller models, it must also support data in place upgrades for the Storage controllers to higher generation of controllers while data is intact in old media. Storage must be offered with purpose built single operating system supporting all of the block, file protocols and Object (S3) API asked.	The BOO to check physically and Firm to submit OEM certificate in this regard.
5.2	Offered Storage must support Symmetric or Asymmetric Active/Active architecture for block access, it also must support file shares to be accessible from all available controllers. Storage must support upto 10PB file share within a single namespace where data is spanning across 2 or more controllers and data is accessible from all of the controllers. Storage must be configured with minimum 2 or more 25/100 Gbps Interconnect ports per controller to ensure high speed inter-controller communication.	The BOO to check physically and Firm to submit OEM certificate in this regard.
5.3	Offered Storage must be supplied with 400 TiB (with 50 TIB in SSD and 350 TIB in NL SAS) of usable capacity after concurrent Triple drive failure protection and spare drives as per OEM's best practices.	The BOO to check physically and Firm to submit OEM certificate in this regard.

5.4	Offered Storage must be configured with minimum of 32 Cores per Controller. Storage must be configured with minimum 128GB DRAM based Global/Federated Cache/Memory per controller. Writes in the cache must be protected in the event of unplanned power outage by de-staging to persistent storage or battery backed cache.	The BOO to check physically and Firm to submit OEM certificate in this regard.
5.5	Array must be offered with minimum 8x32Gbps and 8x25Gbps Ethernet ports across controllers supporting asked protocols. Array must be supplied with 8 SAS ports with each port supporting 4x12Gbps SAS lanes.	The BOO to check physically and Firm to submit OEM certificate in this regard.
5.6	Offered Storage must support scalability minimum of 1440 Drives across offered controllers.	The BOO to check physically and Firm to submit OEM certificate in this regard.
5.7	Offered Storage must support minimum of 1000 Redirect on write snapshots per volume, Production SAN and NAS Volumes must be protected with point-in-time copies. Administrator must be able to setup a policy to take snapshots every 1 hour and retaining it for one month without any performance impact to host IO.	The BOO to check physically and Firm to submit OEM certificate in this regard.
5.8	Offered Storage must provide application consistent data protection within the data center (Snapshots & Thin clones) or by replicating to the remote data center. It must support VMware, MS SQL, Mongo DB, Oracle, MS Exchange, SAP HANA, SAP MaxDB, PostgreSQL, DB2 etc.	The BOO to check physically and Firm to submit OEM certificate in this regard.
5.9	The storage operating system must provide FC, iSCSI, pNFS, NFS (NFSv3, NFSv4, NFSv4.1), CIFS/SMB protocols natively to support heterogeneous application environment. In addition to the above, Object (S3 compatible) protocol should also be supported natively.	The BOO to check physically and Firm to submit OEM certificate in this regard.
5.10	Offered Storage must provide Inline as well as Post-Process deduplication, compression for both Block and File data. Data reduction must be maintained while tiering and replicating the data.	The BOO to check physically and Firm to submit OEM certificate in this regard.
5.11	The storage system should offer capability to identify and remediate ransomware attacks using autonomous ransomware protection within the controllers. The offered system should support ransomware and insider threat detection to protect data with early detection and actionable intelligence on ransomware and other malware incursions. Required HW and SW must be offered.	The BOO to check physically and Firm to submit OEM certificate in this regard.
5.12	Offered Storage must be configured with required Licenses to configure: (i) Synchronous and Asynchronous Replication between 2 DCs for both Block and File Protocols.	The BOO to check physically and Firm to submit OEM certificate in this regard.

A series of handwritten signatures and initials in blue ink are located at the bottom of the page, below the table. The signatures are stylized and include various marks such as 'Pia', 'Wlat', 'goc', 'A', 'key', 'MM', 'W', 'J', and 'Mg'.

	(ii) 3DC Replication with Zero RPO across 3 DCs where 2 Sites are within Metro Distance and 3rd Site can be >1000km away for both block and file Protocols. (iii) Replication solution must support bi-directional replication to minimum 3 Meity compliant public clouds, replication traffic must be encrypted during replication to public cloud.	
5.13	Offered Storage replication should be secured by end-to-end encryption and bandwidth optimization over a WAN link. All the necessary hardware & licenses should be quoted from day 1 in Highly available configuration.	The BOO to check physically and Firm to submit OEM certificate in this regard.
5.14	The proposed storage array must support data-at-rest encryption in compliance with FIPS 140-2 certification managed by On-board Key Manager or External Key Manager.	The BOO to check physically and Firm to submit OEM certificate in this regard
5.15	The storage system should offer high-performance compliance solution in accordance to various industry standards to meet regulations such as Securities and Exchange Commission (SEC) 17a-4, HIPAA, Financial Industry Regulatory Authority (FINRA), Commodity Futures Trading Commission (CFTC), and General Data Protection Regulation(GDPR).	The BOO to check physically and Firm to submit OEM certificate in this regard.
5.16	The storage should be configured to comply with SEC Rule 17a-4 for File data in order to protect the data with WORM protection.	The BOO to check physically and Firm to submit OEM certificate in this regard.
5.17	The storage system must offer management and monitoring layer supporting performance monitoring, utilization, provisioning, monitoring alerts, configuration and reporting around Data Protection, reporting File system analytics to analyze Capacity usage, File and directory counts, File activity trends, Active and inactive data identification and ageing of file data. Management UI must discover and monitor VMware infrastructure with the granularity of Data stores, VMs. it must support end to end topology view of VMware environment to the storage.	The BOO to check physically and Firm to submit OEM certificate in this regard.
5.18	Offered Storage must have capability to implement Quality of Service which must allow administrators to limit IOPS and throughput for certain Block Luns and File shares. Required HW and SW must be offered.	The BOO to check physically and Firm to submit OEM certificate in this regard.
5.19	Overall Security of Storage system should be based on Zero Trust Framework, which will broadly cover below functionalities:- • Controlling access to File and Block data.	The BOO to check physically and Firm to submit OEM certificate in this regard.

	<ul style="list-style-type: none"> • Secure multi-tenancy for all File and Block protocols and Object APIs. • Abnormal access patterns(Anomaly Detection & remediation). • Integration with Multifactor authentication solution. • Temper Proof snapshots. • Multi-admin validation where certain activities needs to be approved by more than 1 Administrators to secure from internal threats. • Encryption(At rest and in flight). • Monitoring and logging administrative access. • Role Based Access Control. 	
5.20	The system should provide capability to tier cold file and block data to Object storage within the Data Centre or to the object storage in the public cloud (AWS, Azure and Google) while preserving data efficiencies and single name space.	The BOO to check physically and Firm to submit OEM certificate in this regard.
5.21	Storage system must be offered in a No-Single-Point of Failure offering upto six 9s of availability with scale up and scale out architecture for all protocols asked .	The BOO to check physically and Firm to submit OEM certificate in this regard.
5.22	Offered Storage must provide Latest CSI driver for providing persistent storage to K8s environments, CSI driver must be a supported by the OEM.	The BOO to check physically and Firm to submit OEM certificate in this regard.

6. L-3 SWITCH

S No	Qualitative Requirements	Trial Directives
6.1	L3 Manageable switch should have minimum 24x 10G/1G SFP+/SFP ports and 2x 100G/40G QSFP28/QSFP+ ports.	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.2	Proposed switch should have a RJ-45 Serial console port.	The BOO to check physically.
6.3	The form factor of the proposed switch should be 1 RU Rack-Mount Appliance.	The BOO to check physically.
6.4	Switching capacity of the proposed switch should be minimum 800 Gbps.	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.5	Packet per second capacity of the switch should be minimum 1300 Mpps and the network latency should be ~1 Micro s.	The BOO to check physically and Firm to submit OEM certificate in this regard.

6.6	Proposed Switch should support minimum 64k MAC address storage and 8K multicast Routes.	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.7	Proposed switch should support 4K VLANs.	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.8	Proposed switches should have a redundant hot swappable power supply and FAN module.	The BOO to check physically.
6.9	The proposed switches should have IP conflict detection and notification.	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.10	The proposed switches should support 802.1X MAC-based mode: Wakeon-LAN.	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.11	The Proposed switches support Multiple ingress ACLs.	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.12	Should support Jumbo frames and link auto-negotiation.	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.13	Should support Spanning Tree Protocol MSTP native, and backwards compatible with STP, STP BPDU Guard and STP Root Guard.	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.14	Should support Edge Port / Port Fast.	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.15	IEEE 802.1AX Link Aggregation.	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.16	IEEE 802.1q VLAN tagging, Private VLAN, Voice VLAN.	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.17	Should support IEEE 802.3ad Link Aggregation with LACP with maximum 24 Link Aggregation Group size.	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.18	Should support virtual wire between two ports for troubleshooting.	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.19	should support Unicast/Multicast traffic balance over trunking port for dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac.	The BOO to check physically and Firm to submit OEM certificate in this regard.

A series of handwritten signatures and initials in blue ink are located at the bottom of the page. From left to right, they include: a signature that appears to be 'Pier', a signature that looks like 'K. Sabo', and several other initials and signatures, including one that looks like 'R. J.' and another that looks like 'M. J.'. There is also a circled signature on the far right.

6.20	Should Support TFTP, uRPF, Multi-stage load balancing and Priority-based flow control.	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.21	Should support 802.1x port-based, 802.1x MAC-based authentication, IEEE 802.1x MAC Access Bypass (MAB).	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.22	The proposed switch must support MACsec (IEEE 802.1AE) encryption to secure data on wired links. The solution should provide support for both Pre-Shared Key (PSK) mode and Dynamic Connectivity Association Key (CAK) mode (802.1X-based) to ensure flexibility in authentication and encryption for different deployment scenarios.	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.23	Should support IEEE 802.1x Guest and Fallback VLAN.	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.24	Should support IEEE 802.1x Dynamic VLAN Assignment.	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.25	Should support RADIUS accounting with CoA and disconnect messages.	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.26	Switch should support local user database and can integrate with, RADIUS, Radius CoA, TACACS+ servers.	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.27	should support LLDP, LLDP-MED, RMON group 1, Storm Control, Loop Guard, IGMP snooping, IP source guard, MLD snooping, MLD proxy, MLD querier and Dynamic ARP Inspection.	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.28	Should support Port mirroring, sFlow V5., RSPAN, Sticky MAC, TLS 1.3, OS image signature verification., IPv6 RA guard, ACL., Telnet,SSHv2, HTTP,HTTPS with IPv4 and IPv6 Management, SNMP v1, v2c and v3.	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.29	Proposed switch should be managed via both, GUI and CLI.	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.30	MUST support multiple configuration files with Dual-firmware image support.	The BOO to check physically and Firm to submit OEM certificate in this regard.

6.31	Should Support for HTTP REST APIs for Configuration and Monitoring.	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.32	Switch should support Policy-based routing, OSPF (IPv4/IPv6), BFD for OSPF (IPv4/IPv6), RIP (IPv4/IPv6), BFD for RIP (IPv4/IPv6), VRRP (IPv4/IPv6).	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.33	Switch should support BGP (IPv4/IPv6), BFD for BGP (IPv4/IPv6), IS-IS (IPv4/IPv6), PIM-SSM (IPv4) and MLAG.	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.34	Switches must be ready for centralized management from day one with the below key features to support. Bidder should provide all the required hardware and software resources and licenses from day one to achieve the below management features.	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.35	Power Required :100–240V AC, 50–60 Hz.	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.36	Operating Temperature : 0–50°C, Humidity: 10–90% non-condensing.	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.37	FCC, CE/EU, UL, RoHS2 and common criteria certified.	The BOO to check physically and Firm to submit OEM certificate in this regard.
6.38	The network switch should support an automation framework that allows administrators to define triggers and map them to automated actions. The triggers can include scheduled tasks, system events, or log-based conditions, and the actions may include running predefined scripts, enabling or disabling specific ports, performing configuration or log backups, initiating device reboots, or applying policy changes. This capability should enable automated enforcement of access policies, scheduled port control, regular maintenance tasks, and rapid incident response without requiring manual intervention.	The BOO to check physically and Firm to submit OEM certificate in this regard.

7. NGFW (Next Generation Fire Wall)

Srl No.	Item	Qualitative Requirement	Trial Directives
7.1	Hardware	The appliance-based security platform should provide firewall, Application Control, Antimalware/Antivirus, Web Filtering and IPS/IDS functionality in a single appliance from day one.	BOO to check physically.

[Handwritten signatures and initials in blue ink]

7.2		The appliance should have 8 x 10GE SFP+, 16 x GE RJ45, 6x1G SFP ports with dual redundant Power Supply from day one and dedicated management and HA port.	BOO to check physically.
7.3		The appliance hardware should be a multicore CPU architecture with a hardened 64-bit operating system.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.4		Proposed Firewall can be ASIC based in nature / open architecture based on multi-core CPU to protect & scale against dynamic latest security threats.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.5	Performance & Scalability	A Minimum Firewall application control throughput in real world/production environment/Application Mix – minimum 25 Gbps including Application-Identification/AVC/Application control and Logging enabled.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.6		Minimum NGFW Threat prevention throughput by enabling and measured with Application-ID/AVC, NGIPS, Anti-Virus, Anti Malware and logging security threat prevention features enabled – minimum 8 Gbps considering 100% HTTP with 64KB transaction size/ 1024 byte packet or Enterprise Traffic Mix.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.7		Firewall should support 10 Gbps of IPS throughput.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.8		The offered firewall must be a single appliance and not a cluster of appliances. The offered appliance should be provided with redundant Fan and redundant hot swappable power supplies.	The BOO to check physically and Firm to submit OEM certificate in this regard
7.9		Firewall should support at least 7.5 Million concurrent sessions or higher.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.10		Firewall should support at least 500 K connections per second or higher.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.11		Firewall should support 45 Gbps of IPSec throughput or higher and 8 Gbps of SSL Inspection Throughput.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.12		To help prevent tampering, the Appliance should have Trusted Platform Module (TPM) chip soldered on the motherboard to reduce the risk of data transaction	The BOO to check physically and Firm to submit OEM certificate in this regard.

A series of handwritten signatures and initials in blue ink are located at the bottom of the page. From left to right, there is a large signature, a smaller signature, the name 'Kasab' with a checkmark, and several other initials and signatures, including one that appears to be 'Raj' and another that looks like 'Sudhakar'.

		interceptions from attackers. This is used to protect the passwords and private keys against malicious software and phishing attacks. The dedicated module helps in generating, storing, and authenticating cryptographic keys.	
7.13		Firewall system shall be able to operate on either Transparent (bridge) mode to minimize interruption to existing network infrastructure or NAT/Route mode. Both modes can also be available concurrently using Virtual Contexts. Minimum 10 Virtual Firewall licenses to be provided with the solution from day one.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.14	Firewall Features	Firewall should support creating access-rules with IPv4 & IPv6 objects, user/groups, application, geolocation, url, zones, vlan, etc.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.15		Firewall should support manual NAT and Auto-NAT, static nat, dynamic nat, dynamic pat.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.16		Firewall should support NAT46, NAT64, NAT66 & DHCPv6 functionality from dayone.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.17		Firewall should support Static, OSPF, OSPFv3 and BGP.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.18		Firewall should support Multicast protocols like IGMP, PIM, etc.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.19		The proposed system shall have the ability to detect, log and take action against network traffic based on over 3500 application signatures.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.20		The application signatures shall be manual or automatically updated	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.21		The administrator shall be able to define application control list based on selectable application group and/or list and its corresponding actions.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.22		Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.	The BOO to check physically and Firm to submit OEM certificate in this regard.

7.23	Should support more than 18,000 (excluding custom signatures) IPS signatures or more. Should have a capabilities to easily import IPS signatures from the most common definition languages Snort or Suricata.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.24	The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reputation of IP addresses determined by the proposed security vendor.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.25	Solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.26	Should support DNS threat intelligence feeds to protect against threats	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.27	The Appliance OEM must have its own threat intelligence analysis center and should use the global footprint of security deployments for more comprehensive network protection.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.28	The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.29	Should be able to identify attacks based on Geo- location and define policy to block on the basis of Geo-location.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.30	The detection engine should support the capability of detecting variants of known threats, as well as new threats.	The BOO to check physically and Firm to submit OEM certificate in this regard
7.31	Firewall should have SDWAN functionality capable Path quality measurement based on (jitter, packet loss, latency).	The BOO to check physically and Firm to submit OEM certificate in this regard
7.32	Should support URL threat intelligence feeds to protect against threats.	The BOO to check physically and Firm to submit OEM certificate in this regard
7.33	WAN load balancing (weighted) algorithms by: volume/ sessions/ source-destination IP/ Source IP /spill over.	The BOO to check physically and Firm to submit OEM certificate in this regard.

7.34	The proposed system should be able to block, allow or monitor only using AV signatures and file blocking based on per firewall policy based or based on firewall authenticated user groups with configurable selection of the following services: HTTP, SMTP, SMTPs, POP3, IMAP, FTP etc.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.35	The proposed system should have integrated Web Content Filtering solution without external solution, devices or hardware modules.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.36	The proposed system shall be able to queries a real time database of over 110 million + rated websites categorized into 70+ unique content categories.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.37	The proposed solution should be able to enable or disable Web Filtering per firewall policy or based on firewall authenticated user groups for both HTTP and HTTPS traffic.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.38	The proposed system shall provide web content filtering features: a) which blocks web plug-ins such as ActiveX, Java Applet, and Cookies. b) Shall include Web URL block c) Shall include score based web keyword block d) Shall include Web Exempt List	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.39	Solution should be ready for the post-quantum threats to include Post Quantum Cryptography with NIST-approved algorithms like ML-KEM and emerging algorithms like BIKE, HQC, and Frodo to protect against emerging threats , including harvest-now, decrypt-later attacks.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.40	The proposed system should have integrated Traffic Shaping functionality.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.41	Ability to sanitize Microsoft Office documents and PDF files by stripping harmful active content (hyperlinks, embedded media, JavaScript, macros) while preserving textual content integrity.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.42	The proposed system should be able to block, allow or monitor only using AV signatures and file blocking based on per firewall policy based or based on	The BOO to check physically and Firm to submit OEM certificate in this regard.

		firewall authenticated user groups with configurable selection of the following services: a. HTTP, HTTPS b. SMTP, SMTPS c. POP3, POP3S d. IMAP, IMAPS e. FTP, FTPS	
7.43		IPS solution should have capability to protect against Denial of Service (DOS) and DDOS attacks. Should have flexibility to configure threshold values for each of the Anomaly. DOS and DDOS protection should be applied and attacks stopped before firewall policy look-ups.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.44	Management/OEM Criteria	OEM should not be blacklisted with in last 3 years in any of the government organisation.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.45		OEM should have local representative available in the region for any type of support or escalation.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.46		3 years license of Firewall, VPN (IPSEC), IPS, Application Control, URL filtering, Anti-Bot, APT, Gateway Antivirus etc, Antispam , Sandboxing, 24*7 Support should be quoted with the solution.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.47		All the feature functionalities and throughputs must be achieved from single box. Bids proposing N + 1 clustering or stacking solution shall be rejected.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.48		The proposed firewall family or its operation system must have EAL4 certified.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.49		The proposed firewall must be fully manageable through the organization's existing centralized management platform. If the proposed firewall is not compatible with the current management system, the bidder shall provide a dedicated firewall management solution capable of managing up to 200 firewalls, including all necessary licenses and components.	The BOO to check physically and Firm to submit OEM certificate in this regard.

7.50		In case bidder is providing dedicated Firewall Management solution. The proposed Firewall Management Platform must include an integrated AI-driven assistant capable of providing automated configuration guidance, diagnostic analysis, IoT device assessment, and generation of scripts/templates for network devices. The solution must support access for a minimum of three administrators, provide clear visibility of AI-resource/token consumption, and ensure that all sensitive information is masked or sanitized before being processed by the AI engine. The platform must also support AI-assisted secure-tunnel setup and automated troubleshooting for existing tunnels.	The BOO to check physically and Firm to submit OEM certificate in this regard.
7.51		Bidder shall offer separate/inbuilt on premise centralized reporting & logging solution from the same OEM whose Firewall are proposed. Logging & Reporting solution can be appliance or software based and should be able to accept logs from the proposed logging and reporting solution from day 1. Proposed logging solution should be able to ingest 100 GB/Day of Logs.	The BOO to check physically and Firm to submit OEM certificate in this regard.

[Handwritten signatures and initials in blue ink]

8. SMART RACK SOLUTION

S/ No.	Specification	Qualitative Requirements	Trial Directives
8.1	Modular Design	(i) Smart rack consists of 42HU x 1No. suitable for free standing installation. (ii) Provisioning of Smart for further extension.	To be Checked by BOO Physically.
8.2	Dimension (HXWxD) in mm	42U x 1 No.- 800 mm Wide x 2000mm Height x 1200mm Deep and 300 mm deep aisle containment at front side. Rack should have base frame of 100mm height for stability. Load bearing capacity of rack frame should be 1400 Kgs. and frame with welded structure. Rack should be made of CRCA sheet steel with minimum sixteen-folded frame with 1.5 mm thickness with surface finish Nano Coated, electro-dip coat primed to 20 microns and powder coated to 80 to 120 microns. Top cover and bottom cover should have cable entry provision. Rack front and rear door should have PU gasket. Each rack should have 2 Nos. vertical and 4 Nos. horizontal cable manager. Each rack should have 10 Nos. tool less banking frames of 1U size. Required total 10 KW cooling capacity with redundancy N+N inclusive both racks. Racks should have rodent repellent. Rack front door should have electronic keypad system. Rack rear door should be equipped with auto opening system. Rack should have air baffle plate. Racks should have water leak sensor. Rack should have provision to mount the cooling system inside in vertical form without consuming any u space within the rack side panel. Rack, cooling system, IPDU, Smoke detection, Front door access, Auto door opening system, monitoring and WLD are required from single OEM for better services.	The BOO to check physically and Firm to submit OEM certificate in this regard.
8.3	Rack door Access System	The Front door of smart rack should be fitted with High Security Electro-mechanical code combination lock of nine digit & Rear with auto door opening system.	To be Checked by BOO Physically.
8.4	Cooling System	Cooling System- 10 KW (N+N)	The BOO to check physically and Firm

[Handwritten signature]

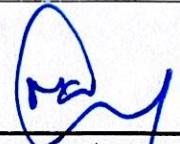
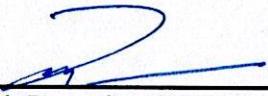
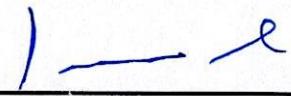
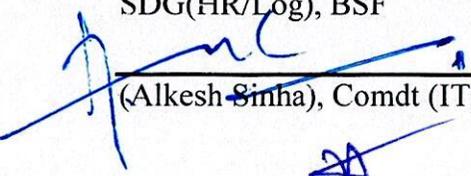
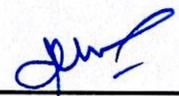
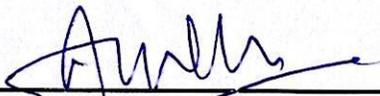
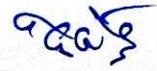
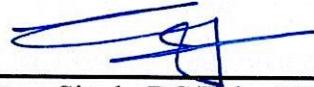
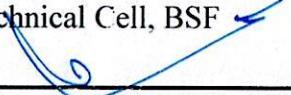
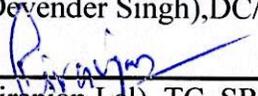
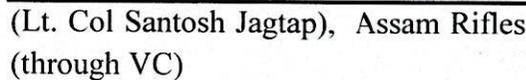
		<p>Harmonized modular components should ensure an energy-efficient dissipation of heat. The external unit (condenser) should be designed on the basis of latest technology. Cooling unit mount should be mount vertical to provide the uniform air flow inside the rack, Unit should not take any U space.</p> <p>Smart rack system should include:</p> <ol style="list-style-type: none"> 1. 2x Heat exchanger (evaporator) for placing on the inside of the system with 10 KW cooling capacity each. 2. 2x Condenser external unit works with R407C/410Arefrigerant. 3. DX control box to activate the evaporator. 4. LCD display, digital temperature display between 18 and 29°C. 5. Cooling system mount in vertical form to provide the uniform air flow in the rack. Cooling system should not occupy any U space in the rack. 6. Cooling unit frame dimension max 300mm x 2100mm height x1200 mm deep with additional 300 mm aisle containment. 	to submit OEM certificate in this regard.
8.5	Electrical Power Distribution System	<p>(i)Provisioning of structured power distribution system. The 3-Phase commercial conditioned 440V/50Hz power supply will be made available by the user at the Distribution panel along with MCCB.</p> <p>(ii)This Main Distribution panel will be used to distribute power to all power consuming devices used in Smart EDGE rack such as: UPS, Air-Conditioning system.</p>	The BOO to check physically and Firm to submit OEM certificate in this regard.
8.6	Power Distribution Units for Racks	<p>Vertical mount intelligent metered I PDU for Racks with industrial socket 32A/3P. Smart rack should have 2 Nos. I PDU.</p> <ul style="list-style-type: none"> • intelligent metered I PDU should have 24 Nos. IEC 13 and 6 Nos. IEC 19 sockets with 2.5 Mtr. connection cable with industrial sockets. • Smart rack should have 2 Nos. intelligent metered I PDU. 	The BOO to check physically and Firm to submit OEM certificate in this regard.
8.7	Monitoring (HMI display)	Provisioning of IP based monitoring Fault signals - Temp/ Humidity, WLD, smoke, UPS and Automatic rear Door Kit, Door access.	The BOO to check physically and Firm to submit OEM certificate in this regard.

Handwritten signatures and initials in blue ink at the bottom of the page.

3.8	Monitoring Technical specifications	<p>Monitoring unit should be an intelligent monitoring system with an Ethernet 10BaseT network connection.</p> <p>The basis of the CMC should be the processing unit (PU unit). Several input/output units (I/O unit) should be connected to one processing unit via a patch cable. This/these function module(s) should connect to the sensors via a standard plug connector. The sensors should be coded so that the function blocks recognise automatically which sensors are connected.</p> <ul style="list-style-type: none"> • Network interface: IEEE 802.3 10/100BaseT Full Duplex • Basic protocols: TCP/IP, SNMP V1.0, Telnet, FTP, http <p>Additional features: NTP, SSH, SSL, DHCP</p>	The BOO to check physically and Firm to submit OEM certificate in this regard.
8.9	Smoke detection and suppression system with hooter	<ul style="list-style-type: none"> • Smart rack should be fitted with smoke detection and suppression system with fire alarm panel, manual release and abort system. • Suppression medium- NOVEC/ FK 5-1-12. • Cylinder should be mount outside the rack. • Smart rack should have hooter. 	The BOO to check physically and Firm to submit OEM certificate in this regard
8.10	UPS System	<ul style="list-style-type: none"> • 10 KVA UPS system rack mount with 30 minutes backup with N+N redundancy. Common battery bank 30 minutes. • UPS and battery will be mount inside the utility rack. • Utility rack frame will be made of sixteen folded CRCA sheet steel and having dimension 600 mm wide x 2100 mm height x 1200 mm deep with 300 mm deep aisle. Utility rack frame load bearing capacity 1400 kgs and should have welded structure. 	The BOO to check physically and Firm to submit OEM certificate in this regard.
8.11	Services	<p>The Rack, smoke detection, Cooling system, IPDU, Front Door access, Rear auto door opening, WLD, monitoring system should be from one OEM for better SLA. OEM should have at least seven-year experience of smart rack in PSU/ Govt organisations.</p>	The BOO to check physically and Firm to submit OEM certificate in this regard.
8.12	Certification	Regulatory Standard, ISO 9001, 14001, 45001 and UL2416, ROHS, Tarde mark	The BOO to check physically and Firm

Handwritten signatures and initials in blue ink at the bottom of the page.

		certificate. With make in India and local content 70%.	to submit OEM certificate in this regard.
8.13	Installation & Training	(i) Installation of smart rack and the relevant components has to be carried out by qualified technicians/OEM engineer. (ii) 01 days onsite training to the user will be given by the vendor.	The BOO to check physically and Firm to submit OEM certificate in this regard.

			
(Mahesh Kumar Aggarwal), IPS, SDG(HR/Log), BSF	(Anish Prasad), IG(ICT), IPS, ICT Dte, BSF	(K L Puri), SP, BPR&D (through VC)	(N S Jamwal), Comdt. (Tech), BSF
			
(Alkesh Sinha), Comdt (IT), BSF	(S K Sastri), Comdt (C-Eqpt), BSF	(Mukesh Kumar), 2IC, SIW, BSF	(Anil Rajput), DC (Ops), Technical Cell, BSF
			
(Jayesh Patil), DC, CISE	(Devender Singh), DC/AIA, SSB	(Gurnam Singh), DC/Tele, ITBP	(Bharat Raj), DC(IT), BSF
			
(K Saha), Dy Director, DCPW	(Niranjn Lal), TC, SRG, NSG	(Lt. Col Santosh Jagtap), Assam Rifles (through VC)	(Aby Thomas), AC, CRPF
			
ASI(RM) Mukesh Kumar, SIW, BSF			

Approved/Not approved

approved

Director General
Border Security Force