Indian Institute of Technology KANPUR

KALYANPUR, KANPUR U.P

KANPUR -208016

Security Section

Tender No: Security/CCTV/IITK/2019/13 Dated 07.02.2020

Bid Submission Last Date 27.02.2020 (04:00 PM)

TENDER DOCUMENT

FOR

PURCHASE OF CCTV DEPLOYMENT

Supply, installation, testing and commissioning of CCTV surveillance equipment (Hardware and software)

BID DOCUMENT

Online bids (Technical & Financial) from eligible bidders which are valid for a period of 120 days from the date of Technical Bid opening (i.e 28.02.2020) are invited for and on behalf of the Assistant Registrar, IIT Kanpur for "**CCTV Deployment".**

Name of Work	**Supply, installation, testing and commissioning of CCTV surveillance equipment (Hardware and software)**
Date of Publishing	**07.02.2020 (17:00 hrs)**
Clarification Start Date and Time	07.02.2020 (17:00 hrs)
Clarification End Date and Time	27.02.2020 (16:00 hrs)
Queries (if any)	No queries will be entertained after clarification end date and time
Bid Submission Start Date	**07.02.2020 (17:00 hrs)**
Last Date and time of uploading of Bids	27.02.2020 (16:00 hrs)3 weeks from publication
EMD amount	**Rs. 1,00,000/- (Rupees One Lakh)** **In favour of "REGISTRAR, IIT KANPUR" payable at Kanpur**
Last Date and time of submitting , EMD and other documents	28.02.2020 (12:00 hrs)
Date and time of opening of Technical Bids	28.02.2020 (16:00 hrs)
Date and time of opening of Financial Bids	Will be separately notified for Technically shortlisted/qualified bidders

Interested parties may view and download the tender document containing the detailed terms & conditions from the website http://eprocure.gov.in/eprocure/app

(The bids have to be submitted online in electronic form on www.eprocure.gov.in only. No physical bids will be accepted.)

INDIAN INSTITUTE OF TECHNOLOGY, KANPUR

Tender Notice

E-tender /Online bids are invited for reputed firms from eligible bidders for the "**Purchase of CCTV Deployment {(Supply, installation, testing and commissioning of CCTV surveillance equipment (Hardware and software)}"**.

The scanned Demand draft for **Rs/- 1,00,000/ (Rs/-.One Lakh only)** towards Bid Security/ EMD in favour of **Registrar IIT Kanpur** payable at **Kanpur** must reach to the **Security Officer, Security Section, Indian Institute of Technology Kanpur, Kanpur (UP), 208016 India** latest by **12:00hrs 28.02.2020.**

Please note all bid related documents scanned copy is to be submitted on the online portal, only Demand draft has to physical reach the aforementioned address.

The tender document along with other details may be downloaded from the CPP Portal: http://eprocure.gov.in/eprocure/app

IIT, Kanpur reserves the right to accept or reject any or all the tenders without assigning any reasons thereof.

Sd/-
In Charge CCTV Survellance

Sd/-
Security Officer (Acting), IIT Kanpur

Date: 07th Feb, 2020

Sd/-
Chairman SAEC
IIT Kanpur

INSTRUCTION FOR ONLINE BID SUBMISSION

The bidders are required to submit soft copies of their bids electronically on the Central Public Procurement (CPP) Portal ie http://eprocure.gov.in/eprocure/app , using valid Digital Signature Certificates. The instructions given below are meant to assist the bidders in registering on the CPP Portal, prepare their bids in accordance with the requirements and submitting their bids online on the CPP Portal.

REGISTRATION

(i) Bidders are required to enrol on the e-Procurement module of the Central Public Procurement Portal (URL:https://eprocure.gov.in/eprocure/app)by clicking on the link "Online Bidder Enrolment" option available on the home page. **Enrolment on the CPP Portal is free of charge.**

(ii) During enrolment/ registration, the bidders should provide the correct/ true information including valid email-id & mobile no. All the correspondence shall be made directly with the contractors/ bidders through email-id provided.

(iii) As part of the enrolment process, the bidders will be required to choose a unique username and assign a password for their accounts.

(iv) For e-tendering possession of valid Digital Signature Certificate (Class II or Class III Certificates with signing key usage) is mandatory which can be obtained from SIFY /n-Code/e-Mudra or any Certifying Authority recognized by CCA India on e-Token/ Smart Card.

(v) Upon enrolment on CPP Portal for e-tendering, the bidders shall register their valid Digital Signature Certificate with their profile.

(vi) Only one valid DSC should be registered by a bidder. Bidders are responsible to ensure that they do not lend their DSCs to others which may lead to misuse and should ensure safety of the same.

(vii) Bidders can than log into the site through the secured login by entering their user ID/ password and the password of the DSC/ e-Token.

SEARCHING FOR TENDER DOCUMENTS

1) There are various search options built in the CPP Portal to facilitate bidders to search active tenders by several parameters. These parameters could include Tender ID, organization name, location, date, value, etc. There is also an option of advanced search for tenders, wherein the bidders may combine a number of search parameters such as organization name, form of contract, location, date, other keywords, etc., to search for a tender published on the CPP Portal.

2) Once the bidders have selected the tenders they are interested in, they may download the required documents / tender schedules. These tenders can be moved to the respective 'My Tenders' folder. This would enable the CPP Portal to intimate the bidders through SMS / e-mail in case there is any corrigendum issued to the tender document.

3) The bidder should make a note of the unique Tender ID assigned to each tender, in case they want to obtain any clarification / help from the Helpdesk.

PREPARATION OF BIDS:

(i) For preparation of bid Bidders shall search the tender from published tender list available on site and download the complete tender document and should take into account corrigendum if any published before submitting their bids.

After selecting the tender document same shall be moved to the 'My favourite' folder of bidders account from where bidder can view all the details of the tender document.

(ii) Bidder shall go through the tender document carefully to understand the documents required to be submitted as part of the bid. Bidders shall note the number of covers in which the bid documents have to be submitted, the number of documents – including the names and content of each of the document that need to be submitted. Any deviations from these may lead to rejection of the bid.

(iii) Any pre-bid clarifications if required, then same may be obtained online through the tender site, or through the contact details given in the tender document.

(iv) Bidders should get ready in advance the bid documents in the required format (PDF/xls/rar/dwf/jpg formats) to be submitted as indicated in the tender document/schedule. **Bid documents may be scanned with 100 dpi with black and white option which helps in reducing size of the scanned document.**

(v) Bidders can update well in advance, the documents such as experience certificates, annual report, PAN, EPF &

other details etc., under "My Space/ Other Important Document" option, which can be submitted as per tender requirements. This will facilitate the bid submission process faster by reducing upload time of bids.

(vi) Any information/ material/ document supplied along with this tender or after placement order should not be disclosed or copied.

(vii) IITK may accept or reject any/ all tenders including the lowest tender without assigning any reasons whatsoever.

(viii) Clarification: For any clarification: For any clarification: Please contact Security, IIT Kanpur (secunit@iitk.ac.in)

SUBMISSION OF BIDS:

(i) Interested authorized dealers/ distributors, who are willing to meet the stated requirement, are requested to kindly submit their competitive bids/ offers through e-procurement system of CPPP of GoI.

(ii) Bidder should log into the site well in advance for bid submission so that he/ she upload the bid in time i.e. on or before the bid submission time. Bidder will be responsible for any delay.

(iii) While submitting the bids online, the bidder shall read the terms & conditions (of CPP portal) and accepts the same in order to proceed further to submit their bid.

(iv) Bidders shall select the payment option as offline to pay the EMD and enter details of the DD/BC/BG/others.

(v) Bidder shall digitally sign and upload the required bid documents one by one as indicated in the tender document.

(vi) Bidders shall note that the very act of using DSC for downloading the tender document and uploading their offers is deemed to be a confirmation that they have read all sections and pages of the tender document without any exception and have understood the complete tender document and are clear about the requirements of the tender document.

(vii) Bid documents may be scanned with 100 dpi with black and white option which helps in reducing size of the scanned document. For the file size of less than 1 MB, the transaction uploading time will be very fast.

(viii) **If price quotes are required in XLS format, utmost care shall be taken for uploading Schedule of quantities & Prices and any change/ modification of the price schedule shall render it unfit for bidding.**

Bidders shall download the Schedule of Quantities & Prices i.e. Schedule-A, in XLS format and save it without changing the name of the file. Bidder shall quote their rate in figures in the appropriate cells, thereafter save and upload the file in financial bid cover (Price bid) only.

The bidders are cautioned that uploading of financial bid elsewhere i.e. other than in cover 2 will result in rejection of the tender.

(ix) Bidders shall submit their bids through online e-tendering system to the Tender Inviting Authority (TIA) well before the bid submission end date & time (as per Server System Clock). **The TIA will not be held responsible for any sort of delay or the difficulties faced during the submission of bids online by the bidders at the eleventh hour**.

(x) After the bid submission **(i.e. after Clicking "Freeze Bid Submission" i**n the portal), the bidders shall **take print out of system generated acknowledgement** number and keep it as a record of evidence for online submission of bid, which will also act as an entry pass to participate in the bid opening.

(xi) Bidders should follow the server time being displayed on bidder's dashboard at the top of the tender site, which shall be considered valid for all actions of requesting, bid submission, bid opening etc., in the e-tender system.

(xii) All the documents being submitted by the bidders would be encrypted using PKI (Public Key Infrastructure) encryption techniques to ensure the secrecy of the data. The data entered cannot be viewed by unauthorized persons until the time of bid opening. The confidentiality of the bids is maintained using the secured Socket Layer 128 bit encryption technology.

(xiii) The successful bidder should submit Order Acceptance within 7 days from the date of order.

(xiv) If an Indian agent is involved, the following documents must be enclosed:

a. Foreign principal's preforma invoice indicating the Commission payable to the Indian

b. Agent and nature of after sales service to be rendered by the Indian Agent.

c. Copy of the agency agreement with the foreign principal and the precise relationship between them and their mutual interest in the business.

d. The enlistment of the Indian agent with Director General of Supplies & Disposals under the Compulsory Registration Scheme of Ministry of Finance.

(xv) Conditional offers/ quotations shall not be accepted and are liable for rejection

(xvi) A scanned copy of the certificate on company letterhead, stating that the bidder hasn't been blacklisted by any institution/ organization/ society/ company of the Central / State Government ministry/ department, or its public sector organizations during the last three years, with company stamp and signed by authorized signatory should also be uploaded.

(xvii) The broad configuration / specification of the proposed purchase / work is given. Bidders are required to keep their proposal strictly as per the specification prescribed.

ASSISTANCE TO BIDDERS:

(i) Any queries relating to the tender document and the terms and conditions contained therein should be addressed to the Tender Inviting Authority for a tender or the relevant contract person indicated in the tender. The contact email for the helpdesk is **secunit@iitk.ac.in** between 10:30 hrs to 17:00 hrs.

(ii) Any queries relating to the process of online bid submission or queries relating to CPP Portal in general may be directed to the 24X7 CPP Portal Helpdesk. The 24 x 7 Help Desk Number 0120-4200462, 0120-4001002 and 0120-4001005. The helpdesk email id is **support-eproc@nic.in**

INSTRUCTION FOR e-PROCUREMENT

1. **PREPARATION AND SUBMISSION OF BIDS :**

   a. The detailed tender documents may be downloaded from http://eprocure.gov.in/eprocure/app till the last date of submission of tender. The Tender may be submitted online through CPP Portal http://eprocure.gov.in/eprocure/app

   b. The bidder should submit the bid online in two parts viz. Technical Bid and Financial Bid. Technical Bid should be upload online in cover 1and Financial Bid in ".Xls" should be upload online in cover-2

   SUBMISSION OF THE BID : All interested eligible bidders are requested to submit their bids online on CPP Portal: http://eprocure.gov.in/eprocure/app as per the criteria given in this document:

   a. Technical Bid should be upload online in cover-1.

   b. Financial Bid should be upload online in cover-2

   Both Technical and Financial Bid covers should be placed online on the CPP Portal (http://eprocure.gov.in/eprocure/app).

2. **TECHNICAL BID:** Signed and Scanned copies of the Technical bid documents as under must be submitted online on CPP Portal: http://eprocure.gov.in/eprocure/app .

   List of Documents to be scanned and uploaded (Under Cover-1) within the period of bid submission:-

   i. Scanned copy of Eligibility Criteria of OEM and Bidder as per Annexure-1

   ii. Scanned copy of Compliance sheet as per Annexure-2.

   iii. Scanned copy of Organization Declaration Sheet as per Annexure-3

   iv. Scanned copy of Technical supporting documents in support of all claims.

   v. Scanned copy of other documents mentioned in tender document (if any).

   Please note that no indication of the rates/amounts be made in any of the documents submitted with the TC-BID.

3. **Financial Bid**

   a. The currency of all quoted rates shall be Indian Rupees. All payment shall be made in Indian Rupees.

b. In preparing the financial bids, bidders are expected to take into account the requirements and conditions laid down in this Tender document. The financial bids should be uploaded online as per the specified **".Xls"** format i.e. Price Biin Excel sheet attached as **'.Xls'** with the tender and based on the scope of work, service conditions and other terms of the Tender document. It should include all costs associated with the Terms of Reference/Scope of Work of the assignment.

c. The Financial Proposal should be inclusive of all applicable taxes, duties, fees, levies, and other charges imposed under the applicable laws. The rates quoted in the Tender are inclusive of all applicable taxes, duties etc. **except service tax.** The service tax component shall be re-immersible by the department after receipt of paid challans etc. if applicable.

4. **Last Date for Submission of Tender:**

a. Online bids complete in all respects, must be submitted on or before the last date and time specified in the schedule of events.

b. The IIT, Kanpur may, at its own discretion, alter/extend the last date for submission of tenders.

5. **Bid Validity**

a. All the Bids must be valid for a period of 120 days from the last date of submission of the tender for execution of Contract. However, the quoted rates should be valid for the initial/ extended period of the Contract from the effective date of the Contract. No request will be considered for price revision during the original Contract period.

b. A bid valid for a shorter period shall be declared as non-responsive.

c. In exceptional circumstances, prior to expiry of the original time limit, the IIT may request the bidders to extend the period of validity for a specified additional period beyond the original validity of 120 days. The request and the bidders' responses shall be made in writing. The bidders, not agreeing for such extensions will be allowed to withdraw their bids without forfeiture of their Bid Security.

6. **Modification / Substitution/ Withdrawal of bids:**

a. No Bid shall be modified, substituted or withdrawn by the Bidder after the Bid's due Date.

b. Any alteration/ modification in the Bid or additional information supplied subsequent to the Bid's due Date, unless the same has been expressly sought for by the Authority, shall be disregarded.

7. **Rejection of the Bid**: The bid submitted shall become invalid and tender fee shall not be refunded if:-

a. The bidder is found ineligible.
b. The bidder does not upload all the documents as stipulated in the bid document.

Tender Document

Security Section
Indian Institute of Technology Kanpur
Kanpur (UP) 208016 India

Enquiry Date: 07.02.2020
Enquiry No. Security/CCTV/IITK/2019/13

A. Online quotations are invited for Supply, Installation and Testing of CCTV Deployment. The technical specifications are described below:

Management and Failover Servers (2 Nos.)		
Item	**Description of Requirement**	
Chassis	Rack mount server with 2U form factor.	
CPU	2 x Intel 4114 Xeon Silver (10 core, 2.20 GHz, 13.75 MB L3 Cache, 85 Watt TDP) processor, C621 Series Chipset	
Memory	2x32 GB Advanced ECC DDR4 2666 MT/s RAM with 24 RDIMM slots Support upto 512 GB.	
Memory Protection	Advanced ECC with multi-bit error protection, Online spare, mirrored memory and fast fault tolerance	
HDD Bays	Minimum 8 number of drive bay	
Hard disk drive	SFF Hot-swap 2x 600 GB, 10 K hot plug SAS Disks.	
Controller	RAID controller with 2GB NV flash Cache, minimum 12Gb/s SAS per lane transfer rate, RAID 0, 1, 5, 6, 10, 50, 60 support.	
Networking features	Shall have minimum of 4 x 1Gb, 4 x 10Gbps ISCSI and 4 x 10Gbps IP (Ports for file operations) host ports for connectivity to servers Minimum two number of gigabit NIC on separate controller with TCP/IP offload engine, WoL, PXE support.	
Interfaces	Integrated VGA, minimum 4 USB ports supporting USB 3.1. Fully functional dedicated management Ethernet port (latest IPMI v2.x) with remote console access over LAN, email alerts, hardware monitoring (pre-failure alert) etc.	
Power Supply	Efficient (minimum 93%) hot plug dual redundant power supply with N+1 configuration.	
Fans	Redundant hot-plug system fans	
Operating Systems and Virtualization Software Support	All hardware must fully support latest CentOS, RHEL, Ubuntu, Open Suse and windows server operating system.	
Industry Standard Compliance	ACPI 6.1 Compliant PCIe 3.0 Compliant PXE Support Energy Star ASHRAE A3/A4 UEFI 2.6 SMBIOS Redfish API SNMP v3 TLS 1.2 DMTF Systems Management Architecture	
Warranty	Five years on-site comprehensive warranty from OEM.	

Video Analytics Servers (2 Nos.)	
Item	**Description of Requirement**
Chassis	Rack mount server with 2U form factor.
CPU	2 x Intel 4114 Xeon Silver (10 core, 2.20 GHz, 13.75 MB L3 Cache, 85 Watt TDP) processor, C621 Series Chipset
Memory	2x32 GB Advanced ECC DDR4 2666 MT/s RAM with 24 RDIMM slots Support upto 512 GB.
Memory Protection	Advanced ECC with multi-bit error protection, Online spare, mirrored memory and fast fault tolerance
HDD Bays	Minimum 8 number of drive bay
Hard disk drive	SFF Hot-swap 2x 600 GB, 10 K hot plug SAS Disks.
Controller	RAID controller with 2GB NV flash Cache, minimum 12Gb/s SAS per lane transfer rate, RAID 0, 1, 5, 6, 10, 50, 60 support.
Networking features	Shall have minimum of 4 x 1Gb, 4 x 10Gbps ISCSI and 4 x 10Gbps IP (Ports for file operations) host ports for connectivity to servers Minimum two number of gigabit NIC on separate controller with TCP/IP offload engine, WoL, PXE support.
Interfaces	Integrated VGA, minimum 4 USB ports supporting USB 3.1. Fully functional dedicated management Ethernet port (latest IPMI v2.x) with remote console access over LAN, email alerts, hardware monitoring (pre-failure alert) etc.
Power Supply	Efficient (minimum 93%) hot plug dual redundant power supply with N+1 configuration.
Fans	Redundant hot-plug system fans
Operating Systems and Virtualization Software Support	All hardware must fully support latest CentOS, RHEL, Ubuntu, Open Suse and windows server operating system.
GPU support	2 x NVIDIA Quadro P4000 Graphics Accelerator
Industry Standard Compliance	ACPI 6.1 Compliant PCIe 3.0 Compliant PXE Support Energy Star ASHRAE A3/A4 UEFI 2.6 SMBIOS Redfish API SNMP v3 TLS 1.2 DMTF Systems Management Architecture
Warranty	Five years on-site comprehensive warranty from OEM.	

Unified Storage (1 No.)		
S. No.	**Parameter**	**Description of requirement**
1.	Converge / Unified Storage	Offered Storage array shall be a true converge / unified storage with a single Microcode / operating system instead of running different Microcode / Operating system / Controllers for File, block and object services respectively.
2.	Operating System	The storage array should support industry-leading Operating System platforms including: Windows, Linux.
3.	Capacity & Scalability	The Storage Array shall be offered with **40 x 8TB NL-SAS drives**.
		Offered storage array should be future extendable up-to 1000 TB.
4.	Disk Drive Type	NL-SAS drives, 7000 RPM or higher
5.	Cache	1. Offered Storage Array shall be given with Minimum of 64GB cache in a single unit and shall be scalable to 128GB without any controller change.
		2. Cache shall be completely dynamic for read and write operations and vendor shall not offer any additional card / module for write cache operations.
		3. Cache shall be used only for Data and Control information. OS overhead shall not be done inside cache.
		4. Offered Storage array shall also have additional support for Flash Cache using SSD / Flash drives. Both File services as well as Block operations shall be able to utilize flash cache. Minimum of 1TB Flash cache shall be supported.
		5. If Flash cache is not supported inside the storage array then vendor shall ensure that offered storage array shall be scalable to minimum of 256GB DRAM cache without any replacement or upgrade of controllers.
6.	Processing Power	Offered Storage architecture shall be such that there shall be no load on the storage CPU during Raid Parity calculations.
7.	Architecture	Controllers shall be **true active-active** so that a single logical unit can be shared across all offered controllers in symmetrical fashion, while supporting all the major functionalities like Thin Provisioning, Data Tiering etc.
8.	No Single point of Failure	Offered Storage Array shall be configured in a No Single Point of configuration including Array Controller card, Cache memory, FAN, Power supply etc.
		Controller should be scalable to four controllers within same Storage Array.
9.	Raid Support, Virtualization	1. Offered Storage Subsystem shall support Raid 1, 5 and Raid 6.
		2. Offered storage array shall have native virtualization support so that Raid 1. Raid 5, Raid 6 can be carved out from a logical space instead of dedicating separate physical disks for each application.
		3. Every supplied disk shall be able to participate into multiple and different raid sets simultaneously.
		4. In case vendor doesn't have above functionality, then 20% additional raw capacity shall be provided for each type of disk to balance out the capacity utilization.
10.	Monitoring and Analytics	1. Offered storage shall have cloud enabled monitoring and analytics engine for proactive Storage management. All required licenses for same shall be included in the offer.
		2. Cloud Enabled Monitoring and analytics engine shall have capability to provide following: a. Providing Firmware upgrade and patch upgrade recommendations proactively. b. Providing historical capacity and performance trend analysis. c. Shall provide history of support cases logged with Support team under different column like Critical, Normal and low severity along with closed

		cases. Cloud monitoring tool shall be able to provide the complete month-wise breakup. d. A Complete connectivity map starting from controller to back-end disks. Shall be able to provide a dashboard covering various critical and aspects of Total Capacity, overall health score of array. De-duplication and compression ratio, over-all front-end performance etc.
11.	Data Protection	In-case of Power failure, Storage array shall have de-staged feature to avoid any data loss.
12.	Protocols	Offered Storage array shall support all well-known protocols like FC, ISCSI, FCOE, Ethernet, SMB 3.0, NFS V4, FTP/FTPS etc.
13.	Host and Back-end Ports	1. Offered Storage shall have minimum of 4 x 10Gbps ISCSI and 4 x 10Gbps IP (Ports for file operations) host ports for connectivity to servers. All types of ports shall be 100% scalable.
		2. Offered storage shall have two additional IP ports for the storage based replication.
		3. Offered storage shall support 32Gbps FC front-end ports also, if required in future.
14.	Global Hot Spare	1. Offered Storage Array shall support distributed Global hot Spare for offered Disk drives.
		2. Global hot spare configuring as per industry practice.
		3. It shall provide at-least two hot spare disk per appliance
15.	Performance and Quality of Service	1. Shall have capability to use more than 30 drives per array group or raid group for better performance.
		2. Offered storage array shall support quality of service for critical applications so that appropriate and required response time can be defined for application logical units at storage. It shall be possible to define different service / response time for different application logical units.
		3. Quality of service engine shall allow to define minimum and maximum cap for required IOPS / bandwidth for a given logical units of application running at storage array.
		4. It shall be possible to change the quality of service Response time (In both milliseconds as well as Sub-milliseconds), IOPS, bandwidth specification on basis of real time.
16.	Maintenance	Offered storage shall support online non-disruptive firmware upgrade for both Controller and disk drives.
17.	Snapshot / Point in time copy / Clone	1. Offered Storage shall have support to make the snapshot and full copy (Clone) on the thin volumes if original volume is created on thick or vice-versa.
		2. The storage array should have support for both controller-based as well as file system based snapshots functionality (At-least 1024 copies for a given volume or a file store).
18.	Quota Management and Antivirus Scanning	1. For file services operations, offered storage shall support both user level as well as file level hard and soft quota.
		2. For file services operations, offered storage shall support integration with industry leading antivirus vendors like Symantec, Trend Micro and MacAfee.
19.	Storage Array Configuration & Management Software	1. Vendor shall provide Storage Array configuration and Management software.
		2. Software shall be able to manage more than one array of same family.
20.	Storage Tiering	1. Offered storage shall support dynamic migration of Volume from one Raid set to another set while keeping the application online.
		2. For effective data tiering, Storage subsystem shall support automatically Policy based Sub-Lun Data Migration from one Set of drive Tier to another set of drive tier.

21.	Remote Replication	1. The storage array should support hardware based data replication at the array controller level across all models of the offered family.
		2. Replication shall support incremental replication after resumption from Link Failure or failback situations.
22.	File Level retention and immutability	1. For file services operation, offered storage shall support file protection against accidental, premature, malicious deletion and modification of data using file locking mechanism of WORM and Legal hold.
		2. Apply of legal hold shall ensure that File cannot be moved, modified, or deleted regardless of the retention period
23.	Licenses	Storage subsystem shall be supplied with Thin provisioning, Snapshot, Clone, Performance Monitoring, Online Raid Migration, Online Volume conversion (thin to thin compressed, thin to thin de-dup etc.), Quality of services, Sub-LUN data tiering, Flash cache, and File services on day 1 for the maximum supported capacity of array.
24.	Investment Protection	1. Offered storage array shall support data in place upgrade for higher models within the same offered series.
		2. Data in place shall also allow addition of more controllers in the given array without any federation technology.
		3. The proposed Storage should be none disruptively upgraded to 10G Ethernet, FC and FCoE protocols in future and managed by the same Unified Storage Management Software.
		4. Storage System quoted by the OEM should be in the Leaders Quadrant in the latest Gartner Magic Quadrant for Midrange and High End Modular Storage Arrays Report.
25.	Regulatory Model	The device should have the following certifications - FCC Class A or CE Mark for immunity against electromagnetic emissions
26.	Safety and Quality Standards	The device should have the following quality and safety standard certifications - CAN/ CSAC22.2-60950/UL60950.

Video Management System (100 cameras)	
S. No	**Technical Specification**
1.0	**VMS General Requirements**
1.1	The VMS shall be based on a true open and Cloud ready architecture that shall allow the use of non-proprietary workstation and server hardware, non-proprietary network infrastructure and non-proprietary storage. The VMS application provider must support at least 50 + brands of Cameras and the list of integrations must be listed on the global web site of the application provider.
1.2	The VMS shall integrate cameras using dedicated driver or using the industry standards ONVIF Profile S and Profile G. The same must be listed on the ONVIF website.
1.3	The Security application shall offer a complete and scalable video surveillance solution which allows cameras to be added on a unit-by-unit basis. The database shall support more than 50000 cameras / IP end points in a single Hardware machine.
1.4	The Proposed VMS Solution Shall support native Fail over with in application with no dependency on any external application for both hardware and application redundancy. Solutions with external clustering like Windows, NEC etc should not be proposed. The native fail over architecture must be for both management and recording servers.
1.5	Should record H.265, MPEG4 or MJPEG in at minimum 25 fps
1.6	Should be capable of doing the recordings in NAS, SAN, iSCSI, network drive – defining different drives for each individual camera.
1.7	Option to record at low frame rate on no motion and high frame rate on Motion
1.8	Option to define multiple recording paths
1.9	Export recordings in mp4, avi, asf formats etc. Must be playable in any operating system- Windows, any flavor of Linux, Unix or Apple MAC
1.10	Option for Windows-Pop Up, Email, Sound Alarm, SMS etc on recording or video loss
1.11	Image Enhancement on recorded videos. The image enhancement should be able to enhance videos of fog, rain, low light conditions etc.
1.12	The user should be informed via email and video popup on low disk space event.
1.13	Automatic Archiving after set number of days and automatic recording deletion after disk full, along-with triggering email to the user.
1.14	Should have adaptive streaming – Option to switch stream from lower stream to higher stream and vice-versa on full screen.
1.15	Both live and zoomed picture should be visible simultaneously while zooming.
1.16	The Application shall offer a plug and play type hardware discovery service with the following functionalities:
1.	Automatically discover Video surveillance units as they are attached to the network.
2.	Discover Surveillance units on different network segments, including the Internet, and across routers with or without network address translation (NAT) capabilities.
3.	The Application shall have the capacity to configure the key frame interval (I-frame) in seconds or number of frames.
4.	The Application shall allow for multiple recording schedules to be assigned to a single camera.
5.	The Application shall support Direct Multicast from Camera. For network topologies that restrict the Application from sending multicast UDP streams, the application shall redirect audio/video streams to active viewing clients on the network using multicast UDP directly from cameras and the architecture should not use Multicast streaming via recording servers or any other servers and increase the overall compute capacity of Recording servers.

6.	The Application shall allow important video sequences to be protected against normal disk cleanup routines.
7.	The application shall have the following options when protecting a video sequence: Until a specified date, for a specified number of days, indefinitely (until the protection is explicitly removed for evidence).
8.	The application shall support edge recording capabilities with ability to playback the video recorded at different speeds and ability to offload the video recorded on the application server on schedule, on event, or manually to store it on the recording server.
9.	The proposed software shall be scalable to support live viewing and automatic transfer of video recorded to the cloud on demand basis from the same VMs user interface, based on the age of the video for future scalability and the hosted Cloud Platform must be among the approved vendors as per the MeiTY approved GI Cloud initiative from Govt of India. The proposed application must provide a single interface to monitor, collaborate and action for both on premises and cloud devices like cameras, ANPR devices etc.
10.	The Application shall be capable to handle both IP v4 and IP v6 Unicast and Multicast traffic with both PIM - SM and PIM - DM support.
11.	The application management server should not have any limitation on the no of recording servers added on one single management / fail over server. Any limitations must be clearly specified by the bidder.
12.	There should not be any dependency on the end point MAC address for licensing for ease of operations.
13.	The application vendor must be a Gold partner of the proposed OS vendor for seamless integration and higher level of support commitment.
2.0	**Fail-over Server**
2.1	The Fail over and Fall back management and recording Server shall be on hot standby, ready to take over during the primary management server fails.
2.2	No manual action from the user shall be required.
2.3	The fail over time should not be beyond 30 seconds and there should not be any loss in the Live video and recorded video.
2.4	The Standby VMS server shall support disaster recovery scenarios where a server can be in another geographic area (or building) and only take over if Primary server becomes offline.
2.5	The Standby Server shall support real-time synchronization of the configuration databases for high reliability.
3.0	**Client Interface**
3.1	The Monitoring UI shall support the role of a Unified Security Interface that can monitor various Video, ALPR, and other system events and alarms, as well as view live and recorded video.
3.2	**User workspace customization:**
1.	The user shall have full control over the user workspace through a variety of user-selectable customization options. Administrators shall also be able to limit what users and operators can modify in their workspace through privileges.
2.	Once customized, the user shall be able to save his or her workspace.
3.	The user workspace shall be accessible by a specific user from any client application on the network.
4.	Display tile patterns shall be customizable.
5.	Event or alarm lists shall span anywhere from a portion of the screen up to the entire screen and shall be resizable by the user. The length of event or alarm lists shall be user-defined. Scroll bars shall enable the user to navigate through lengthy lists of events and alarms.

6.	The Monitoring UI shall support multiple display tile patterns (e.g. 1 display tile (1x1 matrix), 16 tiles (8x8 matrix), and multiple additional variations).		
7.	Additional customization options include: show/hide window panes, show/hide menus/toolbars, show/hide overlaid information on video, resize different window panes, and choice of tile display pattern on a per task basis.		
8.	The Monitoring UI shall provide an interface to support the following tasks and activities common to Various systems		
9.	Monitoring the events from a live security system		
10.	Generating reports, including custom reports.		
11.	Monitoring and acknowledging alarms.		
12.	Creating and editing incidents and generating incident reports.		
13.	Displaying dynamic graphical maps and floor plans as well as executing actions from dynamic graphical maps and floor plans Unified with UC&C.		
14.	The live video viewing capabilities of the Monitoring UI shall include:		
A.	The ability to display all cameras attached to the system both Public, Collaborative monitoring and Cloud based entities.		
B.	The ability to drag and drop a camera into a display tile for live viewing.		
C.	The ability to drag and drop a camera from a map into a display tile for live viewing.		
D.	Support for digital zoom on live camera video streams.		
E.	The ability for audio communication with video units with audio input and output.		
F.	The ability to control pan-tilt-zoom, iris, focus, and presets.		
G.	The ability to bookmark important events for later retrieval on any archiving camera and to uniquely name each bookmark in order to facilitate future searches.		
H.	The ability to start/stop recording on any camera in the system that is configured to allow manual recording by clicking on a single button.		
I.	The ability to activate or de-activate viewing of all system events as they occur.		
J.	The ability to switch to instant replay of the video for any archiving camera with the simple click of button.		
K.	The ability to take snapshots of live video and be able to save or print the snapshots.		
L.	The ability to browse through a list of all bookmarks created on the system and selects any bookmarked event for viewing.		
M.	Tools for exporting video and a self-contained video player on various media such as USB keys, CD/DVD-ROM and Proposed Evidence management and Collaboration system. This video player shall be easy to use without training and shall still support reviewing video metadata.		
N.	Tools for exporting video sequences in standard video formats, such as AVI, ASF, MP4 etc		
O.	The ability to encrypt exported video files with industry standard encryption.		
P.	A tool building and exporting a set of videos into a single container. This tool shall allow the operator to build sequences of video to create a storyboard and allow the export of synchronous cameras.		
4.0	**Cyber Security Requirements:**		
4.1	The VMS shall support only secured media stream requests, unless explicitly configured otherwise. Secured media stream requests shall be secured with strong certificate-based authentication leveraging RTSPS (aka RTSP over TLS). Client authentication for media stream requests is claims-based and may use a limited lifetime security token.		
4.2	The VMS shall offer the ability to encrypt the media stream, including video, audio, and metadata with authenticated encryption. Media stream encryption shall be done at rest and in transit and be a certificate-based AES 128-bit encryption.		
4.3	The VMS shall allow encryption to be set on a per camera basis for all or some of the cameras.		

4.4	Provide up to 20 different certificates for different groups of users who have been granted access to decrypted streams.
4.5	Use Secure RTP (SRTP) to encrypt the payload of a media stream in transit and allow multicast and unicast of the encrypted stream.
4.6	Use a random encryption key and change periodically.
4.7	Allow encrypted streams to be exported.
4.8	The VMS shall support end to end encrypted streams with cameras supporting Secure RTP (SRTP) both in unicast and multicast from the camera.
4.9	The Application shall support digitally sign recorded video using 248-bit RSA public/private key cryptography.
4.10	The Application shall protect archived audio/video files and the system database against network access and non-administrative user access.
4.11	Media encryption shall support with latest industry standards - AES-128.
4.12	The application must support encryptions at the rest and not only on the exported videos footage
4.13	The proposed VMS platform must be UL 2900-2-3 Level 3 Cybersecurity certification
5.0	**Mobile App interface**
5.1	The VMS shall support mobile apps for various off-the-shelf devices. The mobile apps shall communicate with the Mobile Server of the VMS over any Wi-Fi or cellular network connection.
5.2	All communication between the mobile apps and central server shall be based on standard TCP/IP protocol and shall use the TLS encryption with digital certificates to secure the communication channel.
5.3	Ability to view live video on Windows, iOS and Android Phones or devices with and without installing proprietary Apps.
5.4	Ability to receive alerts/notifications on Mobile phones with and without SMS using Push Technology
5.5	Functionalities: Core a. The mobile app should a COTS based app from the VMS provider being made available from the day 1 and must be easily be downloadable from IOS and Android stores online. b. Ability to display a geographic map with VMS entities geo-located on the map. c. Ability to view any camera configured on the map. d. Ability to search cameras or location on the map. e. Ability to view live and recorded video from the cameras of the central recording server. f. Ability to display live and recorded video side-by-side for a specific camera. g. Ability to perform digital zoom on cameras. h. Ability to perform actions on cameras such as add a bookmark, control a PTZ, control the iris/focus function, save a snapshot, start/stop recording. i. Ability to use the camera of the smartphone and stream a live video feed to a video recorder in the system. Ability to locate the mobile app user on map and provisioning to message and collaborate in real time with the central command centre or field staff.
5.6	It shall be possible to extend to the widgets of a dashboard using the SDK. This will provide the ability to develop custom widgets to the system.
5.7	The VMS shall support the following actions on a dashboard: print dashboard, export dashboard to PNG file, and automatically email a report based on a schedule and a list of one or more recipients.
5.8	Camera Integrity Monitor: The VMS shall have native module for monitoring the camera integrity. It should raise alarm if there is change in view, Blurr, Tampering in the camera.

Video Analytics and Licenses (25 Nos.)	
6.1	All below mentioned analytics will comprise as a single Video Analytic License: **1.** Perimeter Trip Wire, Crossing Virtual Line **2.** Object Counting or people/vehicle counting Analytics **3.** Stopped Vehicle Detection for longer span of time – parked at no parking zone. **4.** Crowd Counting & Detection **5.** Intrusion detection on scheduled time intervals **6.** Abandoned Baggage Detection **7.** Missing Object Detection and Selection **8.** Camera Tempering Detection for Camera Blurred video or blocking Speed Violation
6.2	Analytics have to be applied on the above VMS at every possible configuration and at every video formats, without any deviation.
6.3	Real time and Offline analytics option should be available.
6.4	Offline analytics can be run in batch mode in the folder and sub folders –considering every file.
6.5	Define minimum 20 shapes, lines or zone in single camera for video analytics
6.6	Video Analytics can be configured on day/night, daily, weekly or according to users specified date and time
6.7	Reporting feature of analytics should be available for all possible events.
6.8	All the video analytics if come with the camera directly- should be supported directly by the VMS and **no separate video analytic license required for such cases.**

180 Degree Camera (10 Nos.)		
Sr. No	**Camera Characteristics**	**Minimum Specifications**
1.	Imaging Device	1/3.2 inch
2.	Imager Type	CMOS
3.	Imager Readout	Progressive Scan
4.	Sensor	Minimum 4 no's or better
5.	Resolution	12 MP
6.	Image Processing	Minimum 4 no's or better
7.	Signal to Noise Ratio	>50 dB
8.	Sensitivity	Color@0.2 Lux, B/W@.14 Lux
9.	Day Night Capabilities	Yes
10.	Mechanical IR Cut Filter	Yes
11.	Wide Dynamic Range	120 db or better
12.	Lens	4.8 mm
13.	Video Streams	Set of streams to deliver full resolution views
14.	Frame Per Second	up to 30 fps
15.	Video Encoding	H.264 and H.265
16.	Field of View	180º horizontal, 41º vertical
17.	Video Analytics	➢ **Abandoned Object:** Detects objects placed within a defined zone and triggers an alarm if the object remains in the zone longer than the user-defined time allows. An airport terminal is a typical installation for this behaviour. This behaviour can also detect objects left behind at an ATM, signalling possible card skimming. ➢ **Adaptive Motion Detection:** Detects and tracks objects that enter scene and then triggers an alarm when the objects enter a user-defined zone. This behaviour is primarily used in outdoor environments with light traffic to reduce the number of false alarms caused by environmental changes. ➢ **Camera Sabotage:** Detects contrast changes in the field of view. An alarm is triggered if the lens is obstructed by spray paint, a cloth, or a lens cap. Any unauthorized repositioning of the camera also triggers an alarm. ➢ **Directional Motion:** Generates an alarm in a high traffic area when a person or object moves in a specified direction. Typical installations for this behaviour include an airport gate or tunnel where cameras can detect objects moving in the opposite direction of the normal flow of traffic or an individual entering through an exit door. ➢ **Loitering Detection:** Identifies when people or vehicles remain in a defined zone longer than the user-defined time allows. This behaviour is effective in real-time notification of suspicious behaviour around ATMs, stairwells, and school grounds. ➢ **Object Counting:** Counts the number of objects that enter a defined zone. This behaviour can be used to count the number of people at a store entrance/exit or inside a store where the traffic is light. This behaviour is based on tracking and does not count people in a crowded setting. ➢ **Object Removal:** Triggers an alarm if an object is removed from a user-defined zone. This behaviour is ideal for customers who want to detect the removal of high value objects, such as painting from a wall or a statue from a pedestal. ➢ **Stopped Vehicle:** Detects vehicles stopped near a sensitive area longer than the user-defined time allows. This behaviour is idea for drop-offs, parking enforcement, suspicious parking, traffic lane breakdowns, and vehicles waiting at gates.

18.	Supported Protocols	TCP/IP, UDP/IP (Unicast, Multicast IGMP), UPnP, DNS, DHCP, RTP, RTSP, NTP, SNMP v2c/v3, QoS, HTTP, HTTPS, LDAP (client), SSH, SSL, SMTP, FTP, ARP, ICMP, and 802.1x (EAP)
19.	Users	➢ **Unicast:** Up to 20 simultaneous depending on the resolution settings, and frame rate ➢ **Multicast:** Unlimited H.264 and H.265
20.	Streaming	Bi-directional: Full or half duplex
21.	Window Blanking	32
22.	Temperature	–40º to 50ºC
23.	Humidity	10 to 95%, RH condensing
24.	Impact resistance	IK10
25.	Ingress Protection	IP66 & Type 4X
26.	Certification	➢ CE, Class A ➢ FCC Part 15 Class A ➢ ICES-003, Class A ➢ UL/cUL Listed ➢ C-Tick ➢ NEMA Type 4X, and IP66 rating (Environmental Vandal) ➢ RoHS, Lead Free, REACH ➢ NTCIP 1205 ➢ IEC 62676 image quality measurement
27.	ONVIF	S,G & Q

Bullet Camera (15 Nos)		
Sr. No	**Specification**	**Description**
1.	Image sensor	1/2.8" Progressive scan CMOS sensor with WDR.
2.	Resolution	3 Mega Pixel ; 2048 X 1536 @ 30FPS
3.	Lens	5-50 mm Autofocus motorized remote zoom lens
4.	Angle of View	H:90°~ 31°; V: 66° ~ 24°; D: 120°~ 38°
5.	Minimum Illumination	Colour- 0.104 Lux @ 30IRE, B/W -0.05lux; 0Lux with IR ON
6.	IR Illumination	Inbuilt Adaptive IR up to 80 mtr range
7.	Signal to Noise Ratio	>=50dB, Back light compensation ON/OFF selectable.
8.	Compression	H.265, H.264 High & Main profiles; and MJPEG
9.	Wide Dynamic Range	up to 120db as per IEC 62676
10.	3D Digital Noise Reduction	Yes (ON/OFF selectable)
11.	Day/Night Camera	Auto day/night configuration.
12.	Window Blanking	8 configurable windows
13.	Video Stream	Up to three simultaneous streams, the second and the third stream are variable based on the setup of the primary stream
14.	Smart Compression	Yes, to lower bandwidth and storage requirements by up to 70%.
15.	Shutter speed	1/10,000 sec ~ 1 sec
16.	Edge based analytics	Object Counting, Motion detection, Intrusion Detection , camera sabotage, Audio Detection, Adaptive Motion, Object Removal, Directional Motion
17.	Audio	Bi-directional , G.711 A-law/G.711 U-law
18.	Streaming	Camera should support uncast and multicast streams.
19.	Web interface	Camera should have web interface to configure and control.
20.	Text superimposing	Super imposing the title and date & time on the video.
21.	Alarm input	One alarm input & One alarm output.
22.	Edge Storage	Provision for 128GB SD Card.
23.	Ethernet, Network protocols	TCP/IP, UDP/IP (Unicast, Multicast IGMP), UPnP, DNS, DHCP, RTP, RTSP, NTP, IPv4, IPv6, SNMP v2c/v3, QoS, HTTP, HTTPS, SSH, SSL, SMTP, FTP, 802.1x (EAP), and NTCIP 1205,ARP, DDNS, ICMP, IGMP, RTCP, SFTP, SIP, TLS/TTLS, WS-discovery
24.	Discovery interface	OEM interface to detect the cameras automatically and configure network settings.
25.	Housing	Vandal resistant Aluminium enclosure with polycarbonate window
26.	Power requirement	PoE , 24VAC & 2VDC
27.	Power Consumption	Up to 25W
28.	Environmental Protection	Type 4X and IP66/67 rated enclosure
29.	Vandal Proof Certification	IK10
30.	Operating Temperature	-40 to 60 C Degrees.
31.	Operating Humidity	5 to 95% RH non-condensing.
32.	ONVIF Compliance	ONVIF Profile S , Profile G conformant, Profile Q conformant & Profile T conformant
33.	Regulatory Approvals	➢ CE - EN 55032 (Class A), EN 50130-4, EN 60950-1 ➢ FCC (Class A) - 47 CFR Part 15 ➢ UL and cUL Listed - UL 60950-1, CAN/CSA-C22.2 No. 60950-1-07 ➢ UL/IEC 60950-22 ➢ ICES-003 (Class A)
34.	Shock and vibration resistance	IEC 60068:2-6 and 2-27

Sr. No	Mandatory Conditions
1.	All the Items will have to be supplied by the same bidder.
2.	The Servers and Storage should be of the same make.
3.	All the camera brands mentioned are mandatory to be compatible with the mentioned VMS Software Application/Analytics for CCTV/Video-Surveillance.
4.	The prices of cameras, License for VMS and Video Analytics - should be valid for 02 years from the issue of Purchase Order.
5.	One week training/knowledge transfer for all the items (software & hardware) of entire system supplied.
6.	All the documents to be submitted for operation, troubleshooting and maintenance of the entire system supplied

B. Clarification:

For any clarification: Please contact Security, IIT Kanpur (secunit@iitk.ac.in)

C. Final Decision Making Authority:

The decision of the Director, IIT Kanpur will be binding on all bidders.

D. Disclaimer:

1. Information disclosed under and in accordance with the tender document will not constitute as an offer, also the acceptance of responses to this tender cannot be considered as a binding contract.
2. Applicants are solely responsible for all expenses associated with responding to this tender.
3. IITK reserves the right to annul the tender process at any time, without thereby incurring any liability to the affected bidders or specifying the grounds for the action.

E. Legal

1. If any dispute, difference, question of disagreement or matter, whatsoever, before or after completion or abandonment of work, hereafter arises between the parties, as to the meaning, operation or effect of the contract or out of or relating to the contract or breach thereof, the same shall be referred to a Sole Arbitrator to be appointed by the Director of the Institute at the time of dispute.
   a. The venue of the arbitration shall be at Kanpur.
   b. Subject to as aforesaid, the provisions of the Arbitration and Conciliation Act. 1996 and any statutory modifications or re-enactment thereof and rules made there-under and for the time being in force, shall apply to the arbitration proceedings under this clause.

2. The contract shall be governed by and construed according to the laws in force in India. The Parties shall hereby submit to the jurisdiction of the courts situated at Kanpur.

Terms and Conditions Governing the Contract

1. The rates are to be quoted by the bidders in Indian Rupees only and payment shall be made to successful bidders in Indian Rupees only. Any statutory applicable taxes such as applicable Tax, etc. should be mentioned separately in the Financial Bid. However, quote should be inclusive of all other levies, statutory taxes and charges such as Octroi, Packaging & Forwarding charges etc. and should be delivered at the premises. All prices shall be fixed and shall not be subject to escalation of any description. The rates must be quoted strictly as per the 'Financial Bid Format' provided.

2. The time of delivery including testing and handing over in satisfactory condition is the essence of the contract and the shipment should be effected as per the schedule. In the event of part supply, IITK shall withhold the entire payment until the whole of the supply as per the order is delivered. In case the delivery schedule is not stipulated as essential criteria, Contractor may indicate the period of delivery required for them.

3. If the completion of systems/ components is delayed for reasons of force majeure such as acts of God, Acts of Public enemy, acts of Government, fires, floods, epidemics, quarantine restrictions, illegal strikes and freight embargoes, the Contractor shall within 3 days from the date of such occurrence, give notice to IITK in writing of his claim for extension of delivery period. IITK on receipt of such notice may agree to extend the Contract delivery date as may be reasonable but without prejudice to other terms and conditions of the contract. Unless the extended delivery period is agreed by IITK in writing, contractor cannot claim the extension of delivery time as a matter of right. IITK shall have the right to either cancel/ extend the order validity/ levy LD as appropriate.

4. If the Contractor shall fail to deliver the systems/ components within the time specified in the Contract, IITK shall recover from the Contractor as liquidated damages a sum of 0.5% of the contract price of the undelivered systems /components for each week of delay (or) part thereof. The total liquidated damages shall not exceed 5% of the contract price of the unit or units so delayed. Systems/ components will be deemed to have been delivered only when all essential components parts are also delivered. If any essential components are not delivered in time, the entire system / components will be considered as delayed until such time the missing parts are delivered.

5. In general, all supplies are to be delivered as per the schedule of the contract only. In exceptional circumstances, part supply of the items may be accepted upon the recommendation of end-user. However, payment will be effected as stipulated in order/ contract.

6. The Goods supplied under the Contract shall be fully insured against loss or damage incidental to manufacture or acquisition, transportation, storage and delivery.

7. If the contractor fails to deliver the stores or any instalment thereof within the period fixed for such delivery or at any time repudiates the contract before expiry of such period, IITK is entitled to cancel the contract and source purchases from third parties the stores not delivered at the risk and cost of the defaulting contractor.

8. The Contractor warrants that the Goods supplied under this Contract are new, unused, of the most recent or current models and those they incorporate all recent improvements in design and materials unless provided otherwise in the Contract. The Contractor further warrants that all Goods supplied under this Contract shall have no defect arising from design, materials or workmanship (except when the design and/ or material is required by IITK's Specifications) or from any act or omission of the Contractor, that may develop under normal use of the supplied Goods in the conditions prevailing in the country of final destination.

9. **Bidders shall select the payment option as offline to pay the EMD and enter details of the DD/BC/BG/others.**

10. **Deadline for delivery and installation is 60 days from the issue of P.O.**. As per standard terms, 70% payment will be made against after Installation, Commissioning, Testing and installation acceptance; and rest 30% after 03 months of successful observation period.

11. The price shall include but not limited to:

   a. Costs of goods / services covered in this contract.
   b. Taxes and duties

c. Transportation and packing cost
d. Cost of Installation, testing, commissioning and handing over of goods

The Bidder shall indicate on the appropriate price schedule form, the unit prices and total bid prices of the goods he proposes to supply under the contract strictly as per price bid format of tender.

12. **Total duration for delivery and installation is 60 days from the issue of P.O. The supplier is also required to do the installation and demonstration of the equipment within this time; otherwise the penalty clause will be the 0.5% of the total PO value, on weekly basis.**

    In case of any damage to equipment and supplies during the carriage of supplies from the origin of equipment to the installation site, the supplier has to replace it with new equipment/supplies immediately at his own risk. Supplier will settle his claim with the insurance company as per his convenience. IIT Kanpur will not be liable to any type of losses in any form.

13. **Downtime:** During the warranty period, not more than 1% downtime will be permissible. For every day exceeding permissible downtime, penalty of 1/365 of the 1% FOB value will be imposed. Downtime will be counted from the date and time of the filing of complaint with in the business hours.

14. The Bidder shall have to submit a copy of GST Registration certificate along with quotation (if applicable) for claiming the above.

15. In respect of GST as per notification No.45/2017 central tax (Rate) dated 14.11.2017 and Notification No. 47/2017-Integrated Tax (Rate) dated 14.11.2017 and G.O.(MS) No.161 CT&RD dated 14.11.2017. The GST is payable by IITK at 5% only against the tariff rate. Necessary exemption certificate will be issued by IITK for claiming the benefit of exemption. In respect of Import, the custom duty at concessional rate of 5.15% is only payable by IITK under notification no.51/96 customs dated 23.07.1996 and 43/2017 customs dated 30.06.2017 and High sea Sale also acceptable by the IIT Kanpur. No other tax is payable.

16. In the event of any dispute, difference, interpretation or application relating to this agreement arises, the same shall be settled amicably by the parties. In case the dispute or differences could not be settled amicably, the same shall be referred for adjudication through Arbitration by an Arbitrator to be appointed by the Director, IITK. The Arbitration shall be concluded in accordance with the provisions of Arbitration & Conciliation Act, 1996 or any statutory modifications or re-enactment thereof and the rules made their under and for the time being in force shall apply to the arbitration proceedings. Venue of such arbitration shall be at Lucknow. The language of arbitration proceedings shall be English. The Arbitrator shall make a reasoned award (the “award”), which shall be final and binding on the parties. The cost of the arbitration shall be shared equally by the parties to the contract. However, expenses incurred by each party in connection with the preparation, presentation etc., shall be borne by each party.

17. The bidder shall furnish, as a part of his bid, documents establishing the bidder’s eligibility to bid and his qualification to perform the contract if his bid is accepted. The bidder must possess PAN No. and any other registration to claim the statutory levies.

18. The bidder is qualified only when he is the original manufacturer or established dealer with original manufacturer’s authorization letter to quote, sell and service the products offered as per the prescribed format in our web site along with agency agreement.

19. In a tender, either the Indian agent on behalf of the Principal / OEM or Principal / OEM itself can bid but both cannot bid simultaneously for the same item / product in the same tender. If an agent submits bid

on behalf of Principal / OEM, the same agent shall not submit a bid on behalf of another Principal / OEM in the same item / product. In case a bidder not doing business within India, he shall furnish the certificate to the effect that the bidder is or will be represented by an agent in India equipped and able to carry out the supply, maintenance, repair obligations etc. during the warranty and post warranty period or ensure a mechanism at place for carrying out the supply, maintenance, repair obligations etc. during the warranty and post warranty period. OEM also shall provide agency agreement and indicate agency commission payable to make remitting in INR.

20. Institute has full rights to check the credentials of the OEM and the bidder by its own sources. The OEM will be responsible for the successful implementation and maintenance of the deployment, and has to validate and certify the solution.

21. **Training**

a. Bidder shall impart one week training for all the items of CCTV deployment (Hardware & Software) to at least ten (12) Department's personnel at IIT Kanpur's premise absolutely free of cost.

b. Contractor shall upon completion of the installation provide complete training with documentations on the configuration, operation and maintenance of the systems to the required Department's personnel assigned by the Department.

c. Training should include documentation required for understanding the system, its working concepts and basic trouble shooting guidelines and maintenance procedure.

d. Training shall be arranged for security personnel (IIT Kanpur) on basic operation, administration, updating & personalization including all other aspects of CCTV operation.

e. It should cover all the aspects related to analysis of video footage during online/offline mode, exigency operation, etc. All above training shall be part of integration and acceptance of the system.

22. **Documentation**

a. Bidder shall submit documents for operation and maintenance of the entire system.

b. Systems block diagram along with wiring layout of all the items of CCTV deployment shall be submitted. VMS software working principle, capabilities, and detail operational parameters for all the application.

c. Software description manual which shall include customization as per requirements, flow charts, operating procedures for all applications.

d. OS for Servers and PCs shall be supplied with license (OEM/full) along with original media with key no. on the name of PRL.

All the documents shall be provided in Suitable Memory Device in two copies absolutely free of cost.

Annexure -1

Eligibility Criteria of OEM and Bidder:

S. No.	Description	Complied (Y/N)	Remarks
1	OEM should be ISO 9001:2015 certified.		
2	The OEM should support next business day delivery against defective spares in major locations in India. OEM should have 24x7x365 support for India with a direct TAC support in the country.		
3	The bidder must be a reputed manufacturer (OEM) or his authorized System Integrator of the type of products offered. In case of System Integrator, a **Letter of Authorization from OEM and End to End Agreement** specific to the tender should be enclosed. **The bids received without authority are liable to be rejected.**		
4	The bidder should have at Least 5 Year experience in the field CCTV surveillance, Server and Storage in Single Order in IIT's/ Central University, Central Government & PSU's. **Documentary proof in this regard should be submitted.**		
5.	The bidder **should not be blacklisted nor got any unsatisfactory performance letter from** IIT's/ Central University, Central Government & PSU's.		
6	The bidder must enclose a copy of complication certificate / Purchase Order having successfully executed work of CCTV surveillance, Server and Storage in Single Order. Bidder have at least certificate of (One work) of 150 Camera or (Two work) of 100 Camera or (Three work) of 50 Camera each in IIT's/ Central University , Central Government , Government & PSU's for last 5 Years.		
7	For after sales services the agency shall be available at all times and communication by Tele/E-Mail/Fax to agency shall be acknowledged immediately on the same day.		
8	Bidder should be ISO 9001:2015, 27001:2013 and 20000-1:2011 certified. For providing Solutions and Services for Server , Storage , CCTV , Cameras etc.		
9	The Bidder shall provide the Registration number GST/Sales Tax / Service Tax /PAN /TIN - Registration number.		
10	Bidder should have minimum 5 years presence in India. **(Attach Company Registration Certificate)**		
11	Bidder should have minimum 1.5 Cr. net worth in last financial year 2018- 19 **(Attach CA certificate)**.		
12	Bidder should have Solvency Certificate of Rs. 1 Cr. **(Attach Bank Certificate)**		
13	Bidder should have minimum Rs. 5 Cr. Average Turnover for last 3 years 2016-17, 2017-18, and 2018-19. **(Attach CA certificate and Balance sheet & P&L Account).**		
14.	**Bidder has to quote the products from the "List of Approved Makes only"**; else his bid will not be considered for evaluation.		

Note:

1. Please don't upload unnecessary documents or bulk documents as a single document.

2. Name each document with the same name which is asked, so that it can be easily trackable.
(For example – "CA Certificate" will be named as "CA Certificate.pdf")

(Signature of the Tenderer)
Name:
Seal of the Company

List of Approved Makes

S.NO.	DETAILS OF EQUIPMENT AND MATERIALS	MANUFACTURER'S NAME
1.	CCTV/ Video-Surveillance Cameras – IR-Bullet/180 Degree Camera	PANASONIC/ PELCO/ SONY/ HONEYWELL/ AXIS/ BOSCH/CP PLUS
2.	VMS Software Application/Analytics for CCTV/Video-Surveillance	GENETEC SECURITY CENTER/ HONEYWELL/ MILESTONE/ BOSCH
3.	Storage for CCTV, Server Hardware for CCTV (VMS), IBMS and Access Control System:	DELL/ HP/ IBM

Annexure – 2

Compliance Sheet:

Management and Failover Servers (2 Nos.)		
Item	**Description of Requirement**	**Compliance**
Chassis	Rack mount server with 2U form factor.	
CPU	2 x Intel 4114 Xeon Silver (10 core, 2.20 GHz, 13.75 MB L3 Cache, 85 Watt TDP) processor, C621 Series Chipset	
Memory	2x32 GB Advanced ECC DDR4 2666 MT/s RAM with 24 RDIMM slots Support upto 512 GB.	
Memory Protection	Advanced ECC with multi-bit error protection, Online spare, mirrored memory and fast fault tolerance	
HDD Bays	Minimum 8 number of drive bay	
Hard disk drive	SFF Hot-swap 2x 600 GB, 10 K hot plug SAS Disks.	
Controller	RAID controller with 2GB NV flash Cache, minimum 12Gb/s SAS per lane transfer rate, RAID 0, 1, 5, 6, 10, 50, 60 support.	
Networking features	Shall have minimum of 4 x 1Gb, 4 x 10Gbps ISCSI and 4 x 10Gbps IP (Ports for file operations) host ports for connectivity to servers Minimum two number of gigabit NIC on separate controller with TCP/IP offload engine, WoL, PXE support.	
Interfaces	Integrated VGA, minimum 4 USB ports supporting USB 3.1. Fully functional dedicated management Ethernet port (latest IPMI v2.x) with remote console access over LAN, email alerts, hardware monitoring (pre-failure alert) etc.	
Power Supply	Efficient (minimum 93%) hot plug dual redundant power supply with N+1 configuration.	
Fans	Redundant hot-plug system fans	
Operating Systems and Virtualization Software Support	All hardware must fully support latest CentOS, RHEL, Ubuntu, Open Suse and windows server operating system.	
Industry Standard Compliance	ACPI 6.1 Compliant PCIe 3.0 Compliant PXE Support Energy Star ASHRAE A3/A4 UEFI 2.6 SMBIOS Redfish API SNMP v3 TLS 1.2 DMTF Systems Management Architecture	
Warranty	Five years on-site comprehensive warranty from OEM.	

Video Analytics Servers (2 Nos.)		
Item	**Description of Requirement**	**Compliance**
Chassis	Rack mount server with 2U form factor.	
CPU	2 x Intel 4114 Xeon Silver (10 core, 2.20 GHz, 13.75 MB L3 Cache, 85 Watt TDP) processor, C621 Series Chipset	
Memory	2x32 GB Advanced ECC DDR4 2666 MT/s RAM with 24 RDIMM slots Support upto 512 GB.	
Memory Protection	Advanced ECC with multi-bit error protection, Online spare, mirrored memory and fast fault tolerance	
HDD Bays	Minimum 8 number of drive bay	
Hard disk drive	SFF Hot-swap 2x 600 GB, 10 K hot plug SAS Disks.	
Controller	RAID controller with 2GB NV flash Cache, minimum 12Gb/s SAS per lane transfer rate, RAID 0, 1, 5, 6, 10, 50, 60 support.	
Networking features	Shall have minimum of 4 x 1Gb, 4 x 10Gbps ISCSI and 4 x 10Gbps IP (Ports for file operations) host ports for connectivity to servers Minimum two number of gigabit NIC on separate controller with TCP/IP offload engine, WoL, PXE support.	
Interfaces	Integrated VGA, minimum 4 USB ports supporting USB 3.1. Fully functional dedicated management Ethernet port (latest IPMI v2.x) with remote console access over LAN, email alerts, hardware monitoring (pre-failure alert) etc.	
Power Supply	Efficient (minimum 93%) hot plug dual redundant power supply with N+1 configuration.	
Fans	Redundant hot-plug system fans	
Operating Systems and Virtualization Software Support	All hardware must fully support latest CentOS, RHEL, Ubuntu, Open Suse and windows server operating system.	
GPU support	2 x NVIDIA Quadro P4000 Graphics Accelerator	
Industry Standard Compliance	ACPI 6.1 Compliant PCIe 3.0 Compliant PXE Support Energy Star ASHRAE A3/A4 UEFI 2.6 SMBIOS Redfish API SNMP v3 TLS 1.2 DMTF Systems Management Architecture	
Warranty	Five years on-site comprehensive warranty from OEM.	

Unified Storage (1 No.)				
S. No.	**Parameter**	**Description of requirement**	**Compliance**	**Remarks if Any**
1.	Converge / Unified Storage	Offered Storage array shall be a true converge / unified storage with a single Microcode / operating system instead of running different Microcode / Operating system / Controllers for File, block and object services respectively.		
2.	Operating System	The storage array should support industry-leading Operating System platforms including: Windows, Linux.		
3.	Capacity & Scalability	1. The Storage Array shall be offered with **40 x 8TB NL-SAS drives**.		
		2. Offered storage array should be future extendable up-to 1000 TB.		
4.	Disk Drive Type	NL-SAS drives, 7000 RPM or higher		
5.	Cache	1. Offered Storage Array shall be given with Minimum of 64GB cache in a single unit and shall be scalable to 128GB without any controller change.		
		2. Cache shall be completely dynamic for read and write operations and vendor shall not offer any additional card / module for write cache operations.		
		3. Cache shall be used only for Data and Control information. OS overhead shall not be done inside cache.		
		4. Offered Storage array shall also have additional support for Flash Cache using SSD / Flash drives. Both File services as well as Block operations shall be able to utilize flash cache. Minimum of 1TB Flash cache shall be supported.		
		5. If Flash cache is not supported inside the storage array then vendor shall ensure that offered storage array shall be scalable to minimum of 256GB DRAM cache without any replacement or upgrade of controllers.		
6.	Processing Power	Offered Storage architecture shall be such that there shall be no load on the storage CPU during Raid Parity calculations.		
7.	Architecture	Controllers shall be **true active-active** so that a single logical unit can be shared across all offered controllers in symmetrical fashion, while supporting all the major functionalities like Thin Provisioning, Data Tiering etc.		
8.	No Single point of Failure	Offered Storage Array shall be configured in a No Single Point of configuration including Array Controller card, Cache memory, FAN, Power supply etc.		
		Controller should be scalable to four controllers within same Storage Array.		
9.	Raid Support, Virtualization	1. Offered Storage Subsystem shall support Raid 1, 5 and Raid 6.		

		2. Offered storage array shall have native virtualization support so that Raid 1. Raid 5, Raid 6 can be carved out from a logical space instead of dedicating separate physical disks for each application.		
		3. Every supplied disk shall be able to participate into multiple and different raid sets simultaneously.		
		4. In case vendor doesn't have above functionality, then 20% additional raw capacity shall be provided for each type of disk to balance out the capacity utilization.		
10.	Monitoring and Analytics	1. Offered storage shall have cloud enabled monitoring and analytics engine for proactive Storage management. All required licenses for same shall be included in the offer.		
		2. Cloud Enabled Monitoring and analytics engine shall have capability to provide following: e. Providing Firmware upgrade and patch upgrade recommendations proactively. f. Providing historical capacity and performance trend analysis. g. Shall provide history of support cases logged with Support team under different column like Critical, Normal and low severity along with closed cases. Cloud monitoring tool shall be able to provide the complete month-wise breakup. h. A Complete connectivity map starting from controller to back-end disks. i. Shall be able to provide a dashboard covering various critical and aspects of Total Capacity, overall health score of array. De-duplication and compression ratio, over-all front-end performance etc.		
11.	Data Protection	In-case of Power failure, Storage array shall have de-staged feature to avoid any data loss.		
12.	Protocols	Offered Storage array shall support all well-known protocols like FC, ISCSI, FCOE, Ethernet, SMB 3.0, NFS V4, FTP/FTPS etc.		
13.	Host and Back-end Ports	1. Offered Storage shall have minimum of 4 x 10Gbps ISCSI and 4 x 10Gbps IP (Ports for file operations) host ports for connectivity to servers. All types of ports shall be 100% scalable.		
		2. Offered storage shall have two additional IP ports for the storage based replication.		
		3. Offered storage shall support 32Gbps FC front-end ports also, if required in future.		
14.	Global Hot Spare	1. Offered Storage Array shall support distributed Global hot Spare for offered Disk drives.		
		2. Global hot spare configuring as per industry practice.		

		3. It shall provide at-least two hot spare disk per appliance		
15.	Performance and Quality of Service	1. Shall have capability to use more than 30 drives per array group or raid group for better performance.		
		2. Offered storage array shall support quality of service for critical applications so that appropriate and required response time can be defined for application logical units at storage. It shall be possible to define different service / response time for different application logical units.		
		3. Quality of service engine shall allow to define minimum and maximum cap for required IOPS / bandwidth for a given logical units of application running at storage array.		
		4. It shall be possible to change the quality of service Response time (In both milliseconds as well as Sub-milliseconds), IOPS, bandwidth specification on basis of real time.		
16.	Maintenance	Offered storage shall support online non-disruptive firmware upgrade for both Controller and disk drives.		
17.	Snapshot / Point in time copy / Clone	1. Offered Storage shall have support to make the snapshot and full copy (Clone) on the thin volumes if original volume is created on thick or vice-versa.		
		2. The storage array should have support for both controller-based as well as file system based snapshots functionality (At-least 1024 copies for a given volume or a file store).		
18.	Quota Management and Antivirus Scanning	1. For file services operations, offered storage shall support both user level as well as file level hard and soft quota.		
		2. For file services operations, offered storage shall support integration with industry leading antivirus vendors like Symantec, Trend Micro and MacAfee.		
19.	Storage Array Configuration & Management Software	1. Vendor shall provide Storage Array configuration and Management software.		
		2. Software shall be able to manage more than one array of same family.		
20.	Storage Tiering	1. Offered storage shall support dynamic migration of Volume from one Raid set to another set while keeping the application online.		
		2. For effective data tiering, Storage subsystem shall support automatically Policy based Sub-Lun Data Migration from one Set of drive Tier to another set of drive tier.		
21.	Remote Replication	1. The storage array should support hardware based data replication at the array controller level across all models of the offered family.		

		2. Replication shall support incremental replication after resumption from Link Failure or failback situations.		
22.	File Level retention and immutability	1. For file services operation, offered storage shall support file protection against accidental, premature, malicious deletion and modification of data using file locking mechanism of WORM and Legal hold.		
		2. Apply of legal hold shall ensure that File cannot be moved, modified, or deleted regardless of the retention period		
23.	Licenses	Storage subsystem shall be supplied with Thin provisioning, Snapshot, Clone, Performance Monitoring, Online Raid Migration, Online Volume conversion (thin to thin compressed, thin to thin de-dup etc.), Quality of services, Sub-LUN data tiering, Flash cache, and File services on day 1 for the maximum supported capacity of array.		
24.	Investment Protection	Offered storage array shall support data in place upgrade for higher models within the same offered series.		
		Data in place shall also allow addition of more controllers in the given array without any federation technology.		
		The proposed Storage should be none disruptively upgraded to 10G Ethernet, FC and FCoE protocols in future and managed by the same Unified Storage Management Software.		
		Storage System quoted by the OEM should be in the Leaders Quadrant in the latest Gartner Magic Quadrant for Midrange and High End Modular Storage Arrays Report.		
25.	Regulatory Model	The device should have the following certifications - FCC Class A or CE Mark for immunity against electromagnetic emissions		
26.	Safety and Quality Standards	The device should have the following quality and safety standard certifications - CAN/ CSAC22.2-60950/UL60950.		

Video Management Application (100 cameras)			
S. No	**Technical Specification**	**Compliance (Y/ N)**	**Remarks If any**
1.0	**VMS General Requirements**		
1.1	The VMS shall be based on a true open and Cloud ready architecture that shall allow the use of non-proprietary workstation and server hardware, non-proprietary network infrastructure and non-proprietary storage. The VMS application provider must support at least 50 + brands of Cameras and the list of integrations must be listed on the global web site of the application provider.		
1.2	The VMS shall integrate cameras using dedicated driver or using the industry standards ONVIF Profile S and Profile G. The same must be listed on the ONVIF website.		
1.3	The Security application shall offer a complete and scalable video surveillance solution which allows cameras to be added on a unit-by-unit basis. The database shall support more than 50000 cameras / IP end points in a single Hardware machine.		
1.4	The Proposed VMS Solution Shall support native Fail over with in application with no dependency on any external application for both hardware and application redundancy. Solutions with external clustering like Windows, NEC etc should not be proposed. The native fail over architecture must be for both management and recording servers.		
1.5	Should record H.265, MPEG4 or MJPEG in at minimum 25 fps		
1.6	Should be capable of doing the recordings in NAS, SAN, iSCSI, network drive – defining different drives for each individual camera.		
1.7	Option to record at low frame rate on no motion and high frame rate on Motion		
1.8	Option to define multiple recording paths		
1.9	Export recordings in mp4, avi, asf formats etc. Must be playable in any operating system- Windows, any flavour of Linux, Unix or Apple MAC		
1.10	Option for Windows-Pop Up, Email, Sound Alarm, SMS etc on recording or video loss		
1.11	Image Enhancement on recorded videos. The image enhancement should be able to enhance videos of fog, rain, low light conditions etc.		
1.12	The user should be informed via email and video popup on low disk space event.		
1.13	Automatic Archiving after set number of days and automatic recording deletion after disk full, along-with triggering email to the user.		
1.14	Should have adaptive streaming – Option to switch stream from lower stream to higher stream and vice-versa on full screen.		
1.15	Both live and zoomed picture should be visible simultaneously while zooming.		
1.16	The Application shall offer a plug and play type hardware discovery service with the following functionalities:		

14.	Automatically discover Video surveillance units as they are attached to the network.		
15.	Discover Surveillance units on different network segments, including the Internet, and across routers with or without network address translation (NAT) capabilities.		
16.	The Application shall have the capacity to configure the key frame interval (I-frame) in seconds or number of frames.		
17.	The Application shall allow for multiple recording schedules to be assigned to a single camera.		
18.	The Application shall support Direct Multicast from Camera. For network topologies that restrict the Application from sending multicast UDP streams, the application shall redirect audio/video streams to active viewing clients on the network using multicast UDP directly from cameras and the architecture should not use Multicast streaming via recording servers or any other servers and increase the overall compute capacity of Recording servers.		
19.	The Application shall allow important video sequences to be protected against normal disk clean-up routines.		
20.	The application shall have the following options when protecting a video sequence: Until a specified date, for a specified number of days, indefinitely (until the protection is explicitly removed for evidence).		
21.	The application shall support edge recording capabilities with ability to playback the video recorded at different speeds and ability to offload the video recorded on the application server on schedule, on event, or manually to store it on the recording server.		
22.	The proposed software shall be scalable to support live viewing and automatic transfer of video recorded to the cloud on demand basis from the same VMs user interface, based on the age of the video for future scalability and the hosted Cloud Platform must be among the approved vendors as per the MeiTY approved GI Cloud initiative from Govt of India. The proposed application must provide a single interface to monitor, collaborate and action for both on premises and cloud devices like cameras, ANPR devices etc.		
23.	The Application shall be capable to handle both IP v4 and IP v6 Unicast and Multicast traffic with both PIM - SM and PIM - DM support.		
24.	The application management server should not have any limitation on the no of recording servers added on one single management / fail over server. Any limitations must be clearly specified by the bidder.		
25.	There should not be any dependency on the end point MAC address for licensing for ease of operations.		
26.	The application vendor must be a Gold partner of the proposed OS vendor for seamless integration and higher level of support commitment.		
2.0	**Fail-over Server**		
2.1	The Fail over and Fall back management and recording Server shall be on hot standby, ready to take over during the primary management server fails.		
2.2	No manual action from the user shall be required.		
2.3	The fail over time should not be beyond 30 seconds and there should		

	not be any loss in the Live video and recorded video.		
2.4	The Standby VMS server shall support disaster recovery scenarios where a server can be in another geographic area (or building) and only take over if Primary server becomes offline.		
2.5	The Standby Server shall support real-time synchronization of the configuration databases for high reliability.		
3.0	**Client Interface**		
3.1	The Monitoring UI shall support the role of a Unified Security Interface that can monitor various Video, ALPR, and other system events and alarms, as well as view live and recorded video.		
3.2	**User workspace customization:**		
15.	The user shall have full control over the user workspace through a variety of user-selectable customization options. Administrators shall also be able to limit what users and operators can modify in their workspace through privileges.		
16.	Once customized, the user shall be able to save his or her workspace.		
17.	The user workspace shall be accessible by a specific user from any client application on the network.		
18.	Display tile patterns shall be customizable.		
19.	Event or alarm lists shall span anywhere from a portion of the screen up to the entire screen and shall be resizable by the user. The length of event or alarm lists shall be user-defined. Scroll bars shall enable the user to navigate through lengthy lists of events and alarms.		
20.	The Monitoring UI shall support multiple display tile patterns (e.g. 1 display tile (1x1 matrix), 16 tiles (8x8 matrix), and multiple additional variations).		
21.	Additional customization options include: show/hide window panes, show/hide menus/toolbars, show/hide overlaid information on video, resize different window panes, and choice of tile display pattern on a per task basis.		
22.	The Monitoring UI shall provide an interface to support the following tasks and activities common to Various systems		
23.	Monitoring the events from a live security system		
24.	Generating reports, including custom reports.		
25.	Monitoring and acknowledging alarms.		
26.	Creating and editing incidents and generating incident reports.		
27.	Displaying dynamic graphical maps and floor plans as well as executing actions from dynamic graphical maps and floor plans Unified with UC&C.		
28.	The live video viewing capabilities of the Monitoring UI shall include:		
Q.	The ability to display all cameras attached to the system both Public, Collaborative monitoring and Cloud based entities.		
R.	The ability to drag and drop a camera into a display tile for live viewing.		
S.	The ability to drag and drop a camera from a map into a display tile for live viewing.		
T.	Support for digital zoom on live camera video streams.		
U.	The ability for audio communication with video units with audio input and output.		

V.	The ability to control pan-tilt-zoom, iris, focus, and presets.		
W.	The ability to bookmark important events for later retrieval on any archiving camera and to uniquely name each bookmark in order to facilitate future searches.		
X.	The ability to start/stop recording on any camera in the system that is configured to allow manual recording by clicking on a single button.		
Y.	The ability to activate or de-activate viewing of all system events as they occur.		
Z.	The ability to switch to instant replay of the video for any archiving camera with the simple click of button.		
AA.	The ability to take snapshots of live video and be able to save or print the snapshots.		
BB.	The ability to browse through a list of all bookmarks created on the system and selects any bookmarked event for viewing.		
CC.	Tools for exporting video and a self-contained video player on various media such as USB keys, CD/DVD-ROM and Proposed Evidence management and Collaboration system. This video player shall be easy to use without training and shall still support reviewing video metadata.		
DD.	Tools for exporting video sequences in standard video formats, such as AVI, ASF, MP4 etc		
EE.	The ability to encrypt exported video files with industry standard encryption.		
FF.	A tool building and exporting a set of videos into a single container. This tool shall allow the operator to build sequences of video to create a storyboard and allow the export of synchronous cameras.		
4.0	**Cyber Security Requirements:**		
4.1	The VMS shall support only secured media stream requests, unless explicitly configured otherwise. Secured media stream requests shall be secured with strong certificate-based authentication leveraging RTSPS (aka RTSP over TLS). Client authentication for media stream requests is claims-based and may use a limited lifetime security token.		
4.2	The VMS shall offer the ability to encrypt the media stream, including video, audio, and metadata with authenticated encryption. Media stream encryption shall be done at rest and in transit and be a certificate-based AES 128-bit encryption.		
4.3	The VMS shall allow encryption to be set on a per camera basis for all or some of the cameras.		
4.4	Provide up to 20 different certificates for different groups of users who have been granted access to decrypted streams.		
4.5	Use Secure RTP (SRTP) to encrypt the payload of a media stream in transit and allow multicast and unicast of the encrypted stream.		
4.6	Use a random encryption key and change periodically.		
4.7	Allow encrypted streams to be exported.		
4.8	The VMS shall support end to end encrypted streams with cameras supporting Secure RTP (SRTP) both in unicast and multicast from the camera.		
4.9	The Application shall support digitally sign recorded video using 248-bit RSA public/private key cryptography.		

4.10	The Application shall protect archived audio/video files and the system database against network access and non-administrative user access.		
4.11	Media encryption shall support with latest industry standards - AES-128.		
4.12	The application must support encryptions at the rest and not only on the exported videos footage		
4.13	The proposed VMS platform must be UL 2900-2-3 Level 3 Cybersecurity certification		
5.0	**Mobile App interface**		
5.1	The VMS shall support mobile apps for various off-the-shelf devices. The mobile apps shall communicate with the Mobile Server of the VMS over any Wi-Fi or cellular network connection.		
5.2	All communication between the mobile apps and central server shall be based on standard TCP/IP protocol and shall use the TLS encryption with digital certificates to secure the communication channel.		
5.3	Ability to view live video on Windows, iOS and Android Phones or devices with and without installing proprietary Apps.		
5.4	Ability to receive alerts/notifications on Mobile phones with and without SMS using Push Technology		
5.5	Functionalities: Core j. The mobile app should a COTS based app from the VMS provider being made available from the day 1 and must be easily be downloadable from IOS and Android stores online. k. Ability to display a geographic map with VMS entities geo-located on the map. l. Ability to view any camera configured on the map. m. Ability to search cameras or location on the map. n. Ability to view live and recorded video from the cameras of the central recording server. o. Ability to display live and recorded video side-by-side for a specific camera. p. Ability to perform digital zoom on cameras. q. Ability to perform actions on cameras such as add a bookmark, control a PTZ, control the iris/focus function, save a snapshot, start/stop recording. r. Ability to use the camera of the smartphone and stream a live video feed to a video recorder in the system. s. Ability to locate the mobile app user on map and provisioning to message and collaborate in real time with the central command center or field staff.		
5.6	It shall be possible to extend to the widgets of a dashboard using the SDK. This will provide the ability to develop custom widgets to the system.		
5.7	The VMS shall support the following actions on a dashboard: print dashboard, export dashboard to PNG file, and automatically email a report based on a schedule and a list of one or more recipients.		
5.8	Camera Integrity Monitor: The VMS shall have native module for monitoring the camera integrity. It should raise alarm if there is change in view, Blurr, Tampering in the camera.		

Video Analytics and Licenses (25 Nos.)			
6.1	All below mentioned analytics will comprise as a single Video Analytic License: **1.** Perimeter Trip Wire, Crossing Virtual Line **2.** Object Counting or people/vehicle counting Analytics **3.** Stopped Vehicle Detection for longer span of time – parked at no parking zone. **4.** Crowd Counting & Detection **5.** Intrusion detection on scheduled time intervals **6.** Abandoned Baggage Detection **7.** Missing Object Detection and Selection **8.** Camera Tempering Detection for Camera Blurred video or blocking **9.** Speed Violation		
6.2	Analytics have to be applied on the above VMS at every possible configuration and at every video formats, without any deviation.		
6.3	Real time and Offline analytics option should be available.		
6.4	Offline analytics can be run in batch mode in the folder and sub folders –considering every file.		
6.5	Define minimum 20 shapes, lines or zone in single camera for video analytics		
6.6	Video Analytics can be configured on day/night, daily, weekly or according to users specified date and time		
6.7	Reporting feature of analytics should be available for all possible events.		
6.8	All the video analytics if come with the camera directly- should be supported directly by the VMS and **no separate video analytic license required for such cases.**		

180 Degree Camera (10 Nos.)				
Sr. No	**Camera Characteristics**	**Minimum Specifications**	**Compliance (Yes/No)**	**Remarks If Any**
1.	Imaging Device	1/3.2 inch		
2.	Imager Type	CMOS		
3.	Imager Readout	Progressive Scan		
4.	Sensor	Minimum 4 no's or better		
5.	Resolution	12 MP		
6.	Image Processing	Minimum 4 no's or better		
7.	Signal to Noise Ratio	>50 dB		
8.	Sensitivity	Color@0.2 Lux, B/W@.14 Lux		
9.	Day Night Capabilities	Yes		
10.	Mechanical IR Cut Filter	Yes		
11.	Wide Dynamic Range	120 db or better		
12.	Lens	4.8 mm		
13.	Video Streams	Set of streams to deliver full resolution views		
14.	Frame Per Second	up to 30 fps		
15.	Video Encoding	H.264 and H.265		
16.	Field of View	180º horizontal, 41º vertical		
17.	Video Analytics	➢ **Abandoned Object:** Detects objects placed within a defined zone and triggers an alarm if the object remains in the zone longer than the user-defined time allows. An airport terminal is a typical installation for this behaviour. This behaviour can also detect objects left behind at an ATM, signalling possible card skimming. ➢ **Adaptive Motion Detection:** Detects and tracks objects that enter scene and then triggers an alarm when the objects enter a user-defined zone. This behaviour is primarily used in outdoor environments with light traffic to reduce the number of false alarms caused by environmental changes. ➢ **Camera Sabotage:** Detects contrast changes in the field of view. An alarm is triggered if the lens is obstructed by spray paint, a cloth, or a lens cap. Any unauthorized repositioning of the camera also triggers an alarm. ➢ **Directional Motion:** Generates an alarm in a high traffic area when a person or object moves in a specified direction. Typical installations for this behaviour include an airport gate or tunnel where cameras can detect objects moving in the opposite direction of the normal flow of traffic or an individual entering through an exit door. ➢ **Loitering Detection:** Identifies when people or vehicles remain in a defined zone longer than the user-defined time allows. This behaviour is effective in real-time notification of suspicious behaviour around ATMs, stairwells, and school grounds. ➢ **Object Counting:** Counts the number of objects that		

		enter a defined zone. This behaviour can be used to count the number of people at a store entrance/exit or inside a store where the traffic is light. This behaviour is based on tracking and does not count people in a crowded setting. ➢ **Object Removal:** Triggers an alarm if an object is removed from a user-defined zone. This behaviour is ideal for customers who want to detect the removal of high value objects, such as painting from a wall or a statue from a pedestal. ➢ **Stopped Vehicle:** Detects vehicles stopped near a sensitive area longer than the user-defined time allows. This behaviour is idea for drop-offs, parking enforcement, suspicious parking, traffic lane breakdowns, and vehicles waiting at gates.		
18.	Supported Protocols	TCP/IP, UDP/IP (Unicast, Multicast IGMP), UPnP, DNS, DHCP, RTP, RTSP, NTP, SNMP v2c/v3, QoS, HTTP, HTTPS, LDAP (client), SSH, SSL, SMTP, FTP, ARP, ICMP, and 802.1x (EAP)		
19.	Users	➢ **Unicast:** Up to 20 simultaneous depending on the resolution settings, and frame rate ➢ **Multicast:** Unlimited H.264 and H.265		
20.	Streaming	Bi-directional: Full or half duplex		
21.	Window Blanking	32		
22.	Temperature	–40º to 50ºC		
23.	Humidity	10 to 95%, RH condensing		
24.	Impact resistance	IK10		
25.	Ingress Protection	IP66 & Type 4X		
26.	Certification	➢ CE, Class A ➢ FCC Part 15 Class A ➢ ICES-003, Class A ➢ UL/cUL Listed ➢ C-Tick ➢ NEMA Type 4X, and IP66 rating (Environmental Vandal) ➢ RoHS, Lead Free, REACH ➢ NTCIP 1205 ➢ IEC 62676 image quality measurement		
27.	ONVIF	S,G & Q		

Bullet Camera (15 Nos)				
Sr. No	**Specification**	**Description**	**Compliance**	**Remarks If Any**
1.	Image sensor	1/2.8" Progressive scan CMOS sensor with WDR.		
2.	Resolution	3 Mega Pixel ; 2048 X 1536 @ 30FPS		
3.	Lens	5-50 mm Autofocus motorized remote zoom lens		
4.	Angle of View	H:90°~ 31°; V: 66° ~ 24°; D: 120°~ 38°		
5.	Minimum Illumination	Colour- 0.104 Lux @ 30IRE, B/W -0.05lux; 0Lux with IR ON		
6.	IR Illumination	Inbuilt Adaptive IR up to 80 mtr range		
7.	Signal to Noise Ratio	>=50dB, Back light compensation ON/OFF selectable.		
8.	Compression	H.265, H.264 High & Main profiles; and MJPEG		
9.	Wide Dynamic Range	up to 120db as per IEC 62676		
10.	3D Digital Noise Reduction	Yes (ON/OFF selectable)		
11.	Day/Night Camera	Auto day/night configuration.		
12.	Window Blanking	8 configurable windows		
13.	Video Stream	Up to three simultaneous streams, the second and the third stream are variable based on the setup of the primary stream		
14.	Smart Compression	Yes, to lower bandwidth and storage requirements by up to 70%.		
15.	Shutter speed	1/10,000 sec ~ 1 sec		
16.	Edge based analytics	Object Counting, Motion detection, Intrusion Detection , camera sabotage, Audio Detection, Adaptive Motion, Object Removal, Directional Motion		
17.	Audio	Bi-directional , G.711 A-law/G.711 U-law		
18.	Streaming	Camera should support uncast and multicast streams.		
19.	Web interface	Camera should have web interface to configure and control.		
20.	Text superimposing	Super imposing the title and date & time on the video.		
21.	Alarm input	One alarm input & One alarm output.		
22.	Edge Storage	Provision for 128GB SD Card.		
23.	Ethernet, Network protocols	TCP/IP, UDP/IP (Unicast, Multicast IGMP), UPnP, DNS, DHCP, RTP, RTSP, NTP, IPv4, IPv6, SNMP v2c/v3, QoS, HTTP, HTTPS, SSH, SSL, SMTP, FTP, 802.1x (EAP), and NTCIP 1205,ARP, DDNS, ICMP, IGMP, RTCP, SFTP, SIP, TLS/TTLS, WS-discovery		
24.	Discovery interface	OEM interface to detect the cameras automatically and configure network settings.		
25.	Housing	Vandal resistant Aluminium enclosure with polycarbonate window		
26.	Power requirement	PoE , 24VAC & 2VDC		
27.	Power Consumption	Up to 25W		
28.	Environmental Protection	Type 4X and IP66/67 rated enclosure		

29.	Vandal Proof Certification	IK10		
30.	Operating Temperature	-40 to 60 C Degrees.		
31.	Operating Humidity	5 to 95% RH non-condensing.		
32.	ONVIF Compliance	ONVIF Profile S , Profile G conformant, Profile Q conformant & Profile T conformant		
33.	Regulatory Approvals	➢ CE - EN 55032 (Class A), EN 50130-4, EN 60950-1 ➢ FCC (Class A) - 47 CFR Part 15 ➢ UL and cUL Listed - UL 60950-1, CAN/CSA-C22.2 No. 60950-1-07 ➢ UL/IEC 60950-22 ➢ ICES-003 (Class A)		
34.	Shock and vibration resistance	IEC 60068:2-6 and 2-27		

Sr. No	Mandatory Conditions	Compliance	Remarks If Any
1.	All the Items will have to be supplied by the same bidder.		
2.	The Servers and Storage should be of the same make.		
3.	All the camera brands mentioned are mandatory to be compatible with the mentioned VMS Software Application/Analytics for CCTV/Video-Surveillance.		
4.	The prices of cameras, License for VMS and Video Analytics - should be valid for 02 years from the issue of Purchase Order.		
5.	One week training/knowledge transfer for all the items (software & hardware) of entire system supplied.		
6.	All the documents to be submitted for operation, troubleshooting and maintenance of the entire system supplied		

Annexure – 3

Organization Letter Head
DECLARATION SHEET

We, _____ hereby certify that all the information and data furnished by our organization with regard to this tender specification are true and complete to the best of our knowledge. I have gone through the specification, conditions and stipulations in details and agree to comply with the requirements and intent of specification.

This is certified that our organization has been authorized (Copy attached) by the OEM to participate in Tender. We further certified that our organization meets all the conditions of eligibility criteria laid down in this tender document. Moreover, OEM has agreed to support on regular basis with technology / product updates and extend support for the warranty.

The prices quoted in the financial bids are subsidized due to academic discount given to IIT Kanpur.

We, further specifically certify that our organization has not been Black Listed/De Listed or put to any Holiday by any Institutional Agency/ Govt. Department/ Public Sector Undertaking in the last three years.

NAME & ADDRESS OF the authorized Dealers/ distributors	
1 Phone	
2 Fax	
3 E-mail	
4 Contact Person Name	
5 Mobile Number	

Signature of Tenderer
Name:

Seal of the Company

Appendix

TENDER ACCEPTANCE LETTER
(To be given on Company Letter Head)

Date:

To,
_____
_____
_____
_____
_____

Sub: Acceptance of Terms & Conditions of Tender.

Tender Reference No: _____

Name of Tender / Work: -
_____
_____
_____

Dear Sir,

1. I/ We have downloaded / obtained the tender document(s) for the above mentioned 'Tender/Work' from the web site(s) namely:
_____
_____

as per your advertisement, given in the above mentioned website(s).

2. I / We hereby certify that I / we have read the entire terms and conditions of the tender documents from Page No. _____ to _____ (including all documents like annexure(s), schedule(s), etc .,), which form part of the contract agreement and I / we shall abide hereby by the terms / conditions / clauses contained therein.

3. The corrigendum(s) issued from time to time by your department/ organisation too have also been taken into consideration, while submitting this acceptance letter.

4. I / We hereby unconditionally accept the tender conditions of above mentioned tender document(s) / corrigendum(s) in its totality / entirety.

5. I / We do hereby declare that our Firm has not been blacklisted/ debarred/ terminated/ banned by any Govt. Department/Public sector undertaking.

6. I / We certify that all information furnished by our Firm is true & correct and in the event that the information is found to be incorrect/untrue or found violated, then your department/ organisation shall without giving any notice or reason therefore or summarily reject the bid or terminate the contract, without prejudice to any other rights or remedy including the forfeiture of the full said earnest money deposit absolutely.

Yours Faithfully,
(Signature of the Bidder, with Official Seal)