GUWAHATI SMART CITY LTD.

(Formerly Guwahati Smart City Development Agency Ltd.)
(CIN U45309AS2016SGC017403)
04th Floor, Aditya Tower, Opp. Down Town Hospital, G.S. Road, Guwahati-781006
E-mail: mdsmartguwahati@gmail.com
Website: www.gscl.assam.gov.in

No. SPV/GSCL/DEV/214/2023/690 Dated Guwahati 21st November, 2023

Corrigendum 5: Changes in Clause of RFP

Tender Title:	"RFP for Selection of System Integrator for Intelligent City Surveillance"
Tender Number:	SPV/GSCL/DEV/214/2023/194
Tender_ ID:	2023_GSCT_32416_1
Tender Published Date:	11th September, 2023

This Corrigendum is being issued in reference to the changes in clause of RFP. The intending bidders are to take note of the following changes and accordingly shall have to submit the tender. Statement showing the amendments to the existing clause in tender volumes is published online.

21/11/23

Managing Director
Guwahati Smart City Limited

Corrigendum no. 5

Volume-1

Mobilization Advance (MA) -MA considered for this project.

MA of 10% of total Project cost may be released at the sole discretion of the customer (GSCL) against submission of Advance Bank Guarantee (ABG) (As per shared format by GSCL) and on approval of detailed survey report, design-built report and detailed project deployment plan as per RFP guideline.

MA if availed by MSI, is to be adjusted against supply, installation and commissioning within project duration (as defined in RFP and corrigendum) or completion of supply whichever is earlier.

Volume-2

5.1 CAMERA SPECIFICATION:

All Cameras to be of Same Make and need to share this specification (Power Consumption, Warranty Period, Field Of View, Firmware update (Auto or manual) spec, Form factor/dimension/weight) along with table mentioned spec.

CCTV		**Technical Compliance (Yes/No)**	**Remarks**
S.No	**OEM Criteria**		
1	CCTV OEM should be active company and should have direct presence in India from last ten years (not as joint venture, partnership firms or through any other association) & manufacturing in India since last Five years (not as joint venture, partnership firms or through any other association) (3rd Party Manufacturing not allowed) and Foreign CCTV OEM should have manufacturing unit globally from last 10 Years at the time of bidding. Documentary evidence should be submitted.		

2	Bidder shall ensure compliance to the Office Memorandum for insertion of Rule 144 (xi) in the General Finance Rules (GFR)-2017 bearing reference number F.No. 6/18/2019-PPD dated 23 July 2020 or latest, by the Public Procurement Division, Department of Expenditure, Ministry of Finance. Non- compliant bid(s) will be summarily rejected. The OEM should not have any common directors who are also on the board of companies having beneficiaries from land border countries at the time of bidding. The camera OEM must submit declaration regarding their own manufacturing setups and shall not have 3rd party manufacturing from any company blacklisted in India or any company sharing land border with India. The IPR/copyright of source code of firmware/software etc. should not reside in countries sharing land borders with India. OEM should submit supporting document to establish proof of this eligibility criteria.			
3	Bid should be compliant to the Policy and Make in India makes shall be given preference as per Order 2017-Revision vide the Department of Industrial Policy and Promotion (DIPP) Order No. P-45021/2/2017-PP(BE-II) dated 16th September,2020 or latest. OEMs under make in India must submit Undertaking and supporting documents.			
5 MP IP Bullet Camera with in-built 100 Mtr. IR			**Technical Compliance (Yes/No)**	**Remarks**
S.No	**Features**	**Required Parameter**		
1	Sensor	1/2.7", 5MP Progressive Scan CMOS Sensor		
2	Max resolution	5 MP		
3	Min. illumination	Color: 0.01 Lux @F1.2, B/W: 0.001 Lux@F1.2, 0 Lux at IR ON		
4	Electronic Shutter	Auto, Slow Shutter, (1/1s-1/100,000s Adjustable)		
5	Lens	5-50mm Motorized Lens		

6	IR Range	up to 100Mtr		
7	Camera Feature	WDR (120dB), 3D-DNR, AGC, AWB, Day & Night,		
8	S/N ratio	≥60db		
9	Video Analytics	Line Crossing, Motion Detection, Intrusion Detection, Scene Change, Human Detection		
10	Video & Audio Compression	Video: H.265 & H.264 (H.265/ HEVC and H.264 /AVC Certificate to be submitted at the time of submitting bid) Audio: G.711A		
11	Video & Audio Bit Rate	Video: Constant bit rate, variable bit rate (250kbps-8Mbps)		
12	Video Streams	Mainstream: 5MP (2880X1620) /2MP (1920×1080) @25/30fps Sub Stream: D1 (704x576)/ CIF (352×288) @15FPS Third Stream: VGA (640X480)/CIF (352×288) @15FPS		
13	Security Feature	New Password Policy, ActiveX Remove, Shifting to HTML5, HTTPS, Video Encryption, HTTPS X 509 certificate, syslog, 801.X, Trusted Boot		
14	Protocol	TCP/IP, IPv4,Ipv6, RTCP, NTP, UPnP, SMTP, ICMP, HTTP, HTTPS, HTTP-Base64, DHCP, DNS, RTP, RTSP, IGMP, IP Filter, SNMP V1 & V2		
15	Alarm In/out	1 Alarm In/1 Alarm Out		
16	Audio In/out	1 Audio In/1 Audio Out		
17	System Compatibility	ONVIF Profile S, G & T . CCTV OEM Should be ONVIF Full Member.		
18	Privacy Mask	Support 4 area privacy mask		

19	Network Port	RJ45 10M,100M adaptive Ethernet interface		
20	SD Card	Support up to 512GB		
21	Operating Conditions	-30°C ~ 60 °C Humidity 95% or less (non-condensing)		
22	Ingress protection	IP66/67 Complaint		
23	Vandalism	IK10 Vandal Proof Complaint		
24	Product Certification	CE, FCC, IS-13252 (Part 1):2010, BIS Registered		
25	OEM should have ISO 9001, 14001, 27001, 45001, ISO/IEC 27032:2012 and CMMI Level 5 (preferred)Certificate.			
5MP IP PTZ Camera 30x Optical Zoom				
Sl. No.	**Parameters**	**Specifications**	**Technical Compliance Yes/No**	**Remark**
1	Image Sensor	1/1.9” Progressive Scan CMOS		
2	Min. Illumination	Color: 0.005Lux@F1.2 B/W: 0Lux with IR on		
3	Zoom	Optical Zoom 30X & Digital Zoom 16X		
4	Focal Length	4.7~141mm @F1.5~F4.0 or equivalent to 30x Optical zoom		
5	Video Compression	H.265 & H.264 (H.265/ HEVC and H.264 /AVC Certificate to be submitted at the time of submitting bid)		
6	Field of View	H58°~H3°/D71°~D3°/V44°~V2°		
7	WDR	140dB Super WDR		
8	Shutter Time	1/100000s~1s		
9	Other Feature	Day & Night, 3D positioning, Backlight Compensation, White Balance, Gain		

		Control, Ultra DNR (2D/3D), Electronic Image Stabilization (EIS)		
10	S/N	>65dB		
11	Pan Range/Pan Speed	360° endless/ Pan Manual Speed: 0.1°~400°/s, Pan Preset Speed: 400°/s		
12	Tilt Range/Tilt Speed	0°~90°(Auto Flip)/ Tilt Manual Speed: 0.1°~320°/s, Tilt Preset Speed: 320°/s		
13	Preset	256		
14	Patrol	8 Patrols, up to 48 presets each patrol		
15	Pattern	4 Patterns		
16	IR Distance	Up to 200m		
17	Video Streaming	Main Stream: 30fps@(2592x1944), 60fps@ (1920x1080, 1280x960) Sub Stream: 60fps@(704x576, 640x480, 640x360) Third Stream: 30fps@(1920x1080, 1280x720, 704x576)		
18	**Network**			
19	Ethernet	1*RJ45 10M/100M Ethernet Port		
20	Streaming Method	Unicast / Multicast		
21	Protocol	IPv4/IPv6, SMTP, SNMP, UPnP, PPPoE, 802.1x, QoS, IGMP, ICMP, SSL, TCP, UDP, RTP, RTSP, RTCP, HTTP, HTTPS, DNS, DHCP, NTP		
22	Audio Compression	G.711/AAC/G.722/G.726		
23	Audio I/O	1 IN/1 out		
24	Alarm I/O	4 IN/2 Out		
25	RS485	Support		

26	Edge Storage	Support for micro-SD/SDHC/SDXC (Max 256 GB supported)		
27	Advanced Function	Auto Tracking, IP Address Filtering, AGC		
28	Privacy Masking	Up to 8 areas		
29	Region of Interest	Support		
30	Smart Defogger	Built-In Fan & Heater combined with Software algorithm Provide Fog Free Picture		
31	PTZ Auto Tracking	Support		
32	**Events**			
33	Event Trigger	Motion Detection, Network Disconnection, External Input, IP address conflict, Illegal Access, Storage anomaly etc.		
34	Event Action	FTP Upload, SMTP Upload, SD Card Record		
35	Video Analysis	Region Entrance, Region Exiting, Advanced Motion Detection, Tamper Detection, Line Crossing, Loitering, Object Left, Object Removed		
36	System Compatibility	ONVIF Profile S, G & T . CCTV OEM Should be ONVIF Full Member.		
37	**General**			
38	Working Condition	Temperature: -50℃~70℃ / Humidity: 0~95%(Non-condensing)		
39	Power Supply	PoE (802.3at) / AC 24V/3A±10%		
40	Power Consumption	16.5W MAX / 35.5W MAX		
41	Surge Protection	IP67 Compliant, IK10 Certified, Level 2 lightning protection 6000V surge protection		

42	Certification	CE, FCC, IS-13252 (Part 1):2010, BIS Registered		
43	OEM should have ISO 9001, 14001, 27001, 45001, ISO/IEC 27032:2012 and CMMI Level 5 (preferred)Certificate.			
5 MP IP BOX Camera				
Sl. No.	**Parameters**	**Specifications**		
1	Sensor	1/2.7", 5MP Progressive Scan CMOS Sensor		
3	Max resolution	5 MP		
4	Min. illumination	Color: 0.01 Lux @F1.2, B/W: 0.001 Lux@F1.2, 0 Lux at IR ON		
5	Electronic Shutter	Auto, Slow Shutter, (1/1s-1/100,000s Adjustable)		
6	Lens	5-50mm CSMount/M12 Mount Lens/Any Other mount		
7	IR Range	External IR		
8	Camera Feature	WDR (120dB), 3D-DNR, AGC, AWB, Day & Night,		
9	S/N ratio	≥60db		
11	Video & Audio Compression	Video: H.265 & H.264 (H.265/ HEVC and H.264 /AVC Certificate to be submitted at the time of submitting bid) Audio: G.711A		
12	Video & Audio Bit Rate	Video: Constant bit rate, variable bit rate (250kbps-8Mbps)		
13	Video Streams	Mainstream: 5MP (2880X1620)/2MP(1920×1080)@25/30fps Sub Stream: D1 (704x576)/ CIF (352×288) @15FPS		

		Third Stream: VGA (640X480)/CIF (352×288) @15FPS		
14	Security Feature	New Password Policy, ActiveX Remove, Shifting to HTML5, HTTPS, Video Encryption , HTTPS X 509 certificate, syslog, 801.X, Trusted Boot		
15	Protocol	TCP/IP, IPv4,Ipv6, RTCP, NTP, UPnP, SMTP, ICMP, HTTP, HTTPS, HTTP-Base64, DHCP, DNS, RTP, RTSP, IGMP, IP Filter, SNMP V1 & V2		
16	Alarm In/out	1 Alarm In/1 Alarm Out		
17	Audio In/out	1 Audio In/1 Audio Out		
18	System Compatibility	ONVIF Profile S, G & T . CCTV OEM Should be ONVIF Full Member.		
19	Privacy Mask	Support 4 area privacy mask		
20	Network Port	RJ45 10M,100M adaptive Ethernet interface		
21	SD Card	Support up to 512GB		
22	Operating Conditions	-30°C ~ 60 °C Humidity 95% or less (non-condensing)		
23	Ingress protection	IP66/67 Complaint		
24	Vandalism	IK10 Vandal Proof Complaint		
25	Product Certification	CE, FCC, IS-13252 (Part 1):2010, BIS Registered		
26	OEM should have ISO 9001, 14001, 27001, 45001, ISO/IEC 27032:2012 and CMMI Level 5(preferred) Certificate.			

5.5 Technical Specifications of AI Based Video Intelligence Platform

AI based Integrated Security Management			Technical Compliance (Yes/No)	Remark
Policing Platform				
Sr. No	**Key**	**Description**		
1	**Unified Platform for Deployment, Training, Scaling and Management of all the video AI related application and Hardware provisioning**	**Singular Unified Video AI Platform -** The Platform shall be a singular and unified AI based Video Intelligence platform capable to run all the Surveillance, Women Safety, Citizen safety, encroachment detection and any other Video Analytics use cases on a single platform, namely -		
		Surveillance Related –		
		Facial Detection		
		Advance Intrusion Detection		
		Women Safety		
		Vandalism		
		Crowd Estimation and Management		
		Abandon Object Detection		
		Person Collapsing		
		Encroachment Detection		
		Stray animal Detection		
		People Fighting/Violence		
		Perimeter Detection		
		Camera Health Monitoring		
		Each of the video analytics use case shall be able to run on a unified video intelligence platform. Where the platform shall have the capability to support several multi-vendor/OEM video		

		analytics applications that can be deployed on any camera or video-feed seamlessly.		
		Hardware Provisioning for Surveillance Application -		
		The inferencing hardware provisioned to run the video analytics application should be common to all the applications irrespective of the type of architecture of deployment. Any application including but not limited to surveillance apps like FRS, person attribute etc. should be capable of running on any device be it a central server or an edge based device or LPU .		
2	**Dynamic Deployment**	Each of the video analytics use-case shall be structured as an independent module that can be deployed on any camera using a simple user interface utility, providing a complete visibility of the use cases and which cameras they are running on.		
		The platform should have utility of scheduling each use case on individual camera by minimum of an hourly granularity.		
		The user should be able to easily select the camera by tag, groups or locations and schedule applications on any camera.		

3	**Advanced AI compatible**	The Video Analytics system shall be compatible with the latest technological advancements in the domain of computer vision and AI. Hence, it shall be able to quickly adapt to newer libraries and AI advancements. All the analytics and use-cases shall be based on advanced AI technology and shall not depend on traditional algorithms.		
4	**Libraries and frameworks**	The system shall be fully compatible with popular Computer Vision and Artificial Intelligence frameworks including but not limited to OpenCV, OpenVINO, Tensorflow, CAFFE, Pytorch, MXNet, TensorRT, Keras and Darknet from day one		
5	**Training new models**	The system shall allow seamless training by labelling any objects within the images and providing them suitable attributes of multiple types such as class, subclass, colour, type etc. The system shall allow training to happen continuously, on demand or on periodic intervals, which shall be configurable.		
6	**Annotation Capabilities of the Platform**	The system shall have an inbuilt annotation tool that allows a user to label the images with relevant information using both rectangle and polygon drawing facilities.		
		The annotation should allow labelling of images or drawn objects with different class names. In case of persons, it should also support labelling of various attributes		

		such as color of clothing, type of clothing, age, gender etc as well.		
		The annotation tool should have a comprehensive project management feature, including assigning annotation jobs on a set of images to individual users. The system should also have support for higher privileged users who can approve/disapprove the annotations done by the annotators.		
		The user should be able to train new deep-learning models from the annotated data using the Annotation UI itself. The user-interface should allow to plug-in the trained model in any of the relevant Video Analytics use-cases dynamically at each camera.		
		The system should allow the testing & implementing agency to plug newly trained AI models at runtime by simply selecting the models in the per-camera configuration page.		
		SI to consider sufficient hardware and sizing as required for optimal running of proposed software during design phase.		

7	**Model Comparison**	The System shall have a library (This library has to be regularly updated over the time) of standardized AI models developed by the OEM of the Video Analytics System, and members of the developer community. These models shall be used for comparing and benchmarking the performance of newly developed models. The system shall allow for both qualitative and quantitative comparison of models, i.e. it shall allow the end user to compare individual parameters of the model (such as learning rate) as well as the overall performance of the model on any given dataset when compared to a standardized model.		
8	**Monitoring and analytics**	Autonomously objective metrics shall be available to be evaluated and Insights into the performance of each algorithm, model and their versions shall be made available to key stakeholders or users as defined. Visual map of composition, workflow, usage analytics, resource utilization, failure points etc. would be made available to provide complete control of A.I. workload.		
9	**Key UI View and operational**	**The System shall provide the following key results from the use case**		

	functionalities of the Video Intelligence Platform	**Event Notifications:** The result of each of the use case shall be in the form of events that contain the screenshot with other metadata describing the event, such as detected objects, timestamp, camera/video that generated the event and all other metadata representing the event from different use cases. The User Interface shall have a grid and list view with all the events from different use cases, cameras etc. These features should be also supported through a mobile application to may be utilized by various users in future.		
		There should be option to export data (video, insights, analysis, etc. files) to a suitable file format		
		The system should support customization of alerts, video feeds, and priority-based alerts for individual users from day one.		
		Resource Management View: The User interface shall provide a list of all the resources available in the system such as computing servers and cameras. The status of each of the devices, whether they are online/offline shall also be available at all times.		
		AI Training Tool: The system should support annotation and label images to train new AI models and update the existing ones as per user reported issues or to increase accuracy of the system.		

		Use case deployment matrix: The user interface shall have a matrix to assign, start, stop and schedule any use case on any camera. The status of active and non-active use cases shall be clearly visible with colour coded information.		
		There will be 2 video analytics use cases deployed per fixed camera on an average.		
		Video Synopsys UI- The Video Intelligence shall provide an intuitive UI for Vide Synopsys. Able to analyze all the recorded video files and provide the operator with synopsis video for quick review and investigation thereby reducing viewing time considerably. The video files from all the 3rd Party Video Management Software (VMS) shall be supported.		
		Data Analytics Dashboard: The user interface shall also have an analytics dashboard listing all the patterns of events from different cameras with a heat-map of number of events on an hourly basis.		
10	**Common UI for all the use-cases**	The user interface shall be a unified dashboard that shows events from all the Video Analytics use-cases and all the cameras in a common UI, and which gets populated in real time from event notifications.		

11	**Web based Interface**	The User based access and interface of the system shall be completely web interface that can be accessed from any system in the local area network (LAN) or wide area network (WAN) with login credentials. It shall allow multiple users to log in at the same time, and receive real-time alerts and notifications.		
		The alerts and notifications should be based upon the user profile.		
		The user can log in from any device and yet should be able to access the system according to his/ her profile .		
12	**Live Video Interface**	The User interface shall allow a user to view the live video stream from any camera with overlaid information of regions, objects, people and vehicles based on each of the use-case		
13	**Configuration per-use-case per-camera level**	The system shall allow each use-case to be uniquely configured for every individual camera stream, with parameters for camera calibration, image quality improvement, night/day settings etc. .		
		Each use-case shall be able to run on different cameras with different settings (e.g., different Zones for Intrusion, different lines for line crossing detection, etc.) at different hours of the day.		
		The configuration page shall allow a user to choose any of the available AI models to detect and classify objects within the image. The description of the models shall clearly specify performance and		

		hardware requirements of each of the model.		
14	**Camera Calibration Tool**	The Video Analytics system UI should have camera-calibration tool that can take user inputs such as reference-heights, reference depths and floor landmarks to calibrate the camera. The calibration tool should have an option to use the GPS coordinates of the camera location.		
		Once the camera is calibrated, each detected object should also be assigned real-world coordinates with respect to the Camera GPS coordinates.		
		This functionality should be available for each camera added in the VA system		
		The OEM should ensure that there should not be any geometric distortions on the deployed cameras.		
15	**Key configuration parameters**	The use case on each camera shall allow setting up configuration of multiple detections zones such as lines and regions that can be used to define perimeters, regions of interest.		
		The configuration user interface shall allow adjusting various sensitivity and confidence parameters to adjust each video-analytics use-case's performance with respect to the physical deployment of the camera.		
16	**Filtering and Retrieval**	The system shall allow a user to filter and retrieve all the events based on any combination of the following parameters:		
		- Time of the event		

		- Objects in the event		
		- Type of the use-case		
		- Camera Location etc.		
17	**Transparent and Open Architecture**	The architecture shall clearly demonstrate the technology stack with layers of the core platform, data governance and interface to different software application		
18	**Highly parallel and distributed**	The algorithms powering the video intelligence system shall possess capability to operate parallel and distributed manner across a cluster of machines. Both training of AI algorithms and inference shall be distributed.		
19	**User Management**	The system shall support user with a hierarchical access level, with different access level for different users demarcated with respect to cameras, locations and the data. The user access control system shall allow setting of SOP's like CRUD (Create, Read, Update and Delete) operations for each user.		
20	**Deployment of use-case across any camera**	The system shall allow deployment of any use case on any camera without any MAC level or IP level locking. Ideally any use case shall be deployable and redeploy able on any camera or video source as far as the camera view supports such use cases to be deployed.		

21	**Video Compatibility**	The System shall be a real-time video analytics engine that utilizes advanced image processing algorithms to turn video into actionable intelligence. The AI based Video Analytics system shall consist of video-processing & analytics engine that works seamlessly both on saved videos or camera streams in real-time and provide events to the user based on the use-case basis. The system shall be compatible with all ONVIF compliant IP cameras with H.264/H.265 video decoding.		
22	**Centralized Deployment Support**	All the video streams shall be processed centrally at the Data Center with one or more servers for video processing. The user shall be able to log in to the system through the central dashboard to access all the data from all the servers. The processing of videos as well as alert generation shall be done on premise. At no point in time shall the data from the site be shared over the internet or sent over to the cloud. The System UI shall only be accessible using workstations and terminals available on premises.		
23	**Support for third-party use-cases**	The AI system shall also support third-party developed algorithms and use-cases that can provide the user with a large base of use-cases to choose from.		
		If a new use-case needs to be developed based on Video Intelligence, the system shall provide a developer Software Development Kit (SDK) for this purpose. The RESTful APIs/SOAP APIs or Web SDK/ AI and Machine Learning SDK as required shall be provided along with detailed		

		documentation for building end-to-end use-cases on the system.		
		The system shall also allow the user to plug different AI models in the individual running of the video analytics use-case.		
24	**Flexible Technology Stack**	The technology stack shall be modular and scalable based on containerized micro services. Each use-case shall be orchestrated as a stand-alone micro service, which communicates with a central server for exchanging of the data.		
		A.I. micro services components shall be agnostic to language used in technology stack. It shall work with any language, framework, and library of choice without any impact on the rest of the architecture. This type of flexibility will ensure lower friction for collaboration and deployment of AI.		
		Algorithms being containerized shall ensure both interoperability and portability, allowing for code to be written in any programming language or any version of library and framework but then seamlessly exposes a single API to be integrated and ported with multiple modules/AI components of diverse stack. It shall seamlessly integrate with other components and shall be portable/ replicable easily across the machines automatically.		
		High Availability and Virtualization Support - The Video Intelligence platform		

		should support HA and Virtualization from Day 1.		
25	**General VA specifications**	The Video Analytics shall be based upon Machine Learning and Deep Learning framework.		
		To save the duplication of the video storage, the analytics should flag the video for the configurable duration of time pre and post event in the Video Management System. It should be possible for the operator to jump to the alert flag in the archived video for detailed investigation of the event.		
		It shall be possible to run the analytic as per hourly/daily/weekly schedule. There should be a provision to define multiple such schedules. It should be possible to set the schedule to any analytic use case. It should be possible to assign multiple analytics on the same camera.		
		It is possible to generate email or a text message to the designated recipients in case critical alerts are generated. The application shall escalate the alert to the designated users through email or a text message in case the alert is not acknowledged by the operator in a specified period of time.		
		It shall enable common configuration settings in a batch mode on multiple cameras.		
		The application shall allow searching the analytics events based on priority, date and time (from and to) and camera. It should be possible to generate statistical		

		analysis of various use cases across the time of the day.		
		The analytics shall enable the operator to define an unlimited number of detection regions per camera. The system shall allow setting each region independently to be 'Active for Analytics' for any given period of time of the day.		
		The analytics events shall be stored in the database. In case the events are purged, the purged events stored to external files for later reference.		
		For Vehicular Analytics, it is possible to deploy the analytics in centralized architecture where all the feeds from the cameras are available in the Data Center and analyzed centrally.		
		The system shall have a single client application for setting analytics, live viewing, archived viewing, and the administrator functions.		

26	***Video Summarization System Functional Requirements & KPIs:***	The proposed solution should help in making Video Searchable, Quantifiable and Actionable, reviewing long duration of video in short time; quantitatively analyze video to derive actionable insights for data driven safety, security and operational decision making. The proposed system should be state of the art image processing technology essentially creating condensed summaries of original, full length video recordings, while preserving all objects and events of interest. These should be presented either simultaneously or in rapid succession, regardless of the time point and sequence in which they occurred, effectively providing operators with a clear view of activities and enabling them to rapidly review and home in on events of interest.		
		The system should provide operators, what they need to quickly scan through video data to find suspicious, out of the ordinary or potentially criminal aspects. After detecting an object of interest, the user shall be able to select to see the object in its original form in the original video which can then be exported.		
		Video Summarization tool based on attributes and meta data field will facilitate to reach to relevant and meaningful content for the defined search meeting the requirements for effective post investigation analyses within shorter time span.		

		System shall be able to analyze all the recorded video files and provide the operator with Summarization video for quick review and investigation thereby reducing viewing time considerably.		
		a. The video files from all the 3rd Party Video Management Software (VMS) shall be supported.		
		System shall support: -		
		· Shall support Video File exports from all kind of 3rd Party VMS and even the video files recorded from a Mobile Or any other kind of Analog Camera.		
		· System shall be able to enhance safety and security with quick rapid human response to critical events recorded on video		
		· Shall support Video File exports from all kind of 3rd Party VMS and even the video files recorded from a Mobile Or any other kind of other video sources.		
		· Shall automatically extracts objects from the original video and efficiently reconstructs and superimposes them back in the original scene, simultaneously displaying events that have occurred at different times.		
		· System shall rapidly pinpoint people and vehicles of interest, using an extensive range of appearance and movement filters, across multiple video sources from different cameras installed in the premises.		

		· Shall Instantly locate people, vehicles, and items of interest by searching for similar looking objects.		
		· System shall display time-stamps for various objects in the video continuously, while the summarization is played.		
		· Shall provide a web interface to upload the video files, generate the Summarization & for the management of multiple investigation cases		
		· System shall provide density control while replaying the Summarization video. Density refers to the number of events shown concurrently when playing a Summarization.		
		· The density control shall increase or decrease the number of events shown at once also changing the event density shall alter the run time duration of the video Summarization thereby enabling quick review time.		
		· Time Range - Limit the search criteria to specific time ranges		
		· Source - Limit objects to specific cameras or files		
		· Class – Video Summarization shall be shown based on People, Two-Wheeled Vehicles, Other Vehicles and Animals		
		- People Class: Man, Woman and child.		
		- Two-Wheeled Vehicle Class: Bicycle and Motorcycle		
		- Other Vehicles Class: Car, Pickup, Van, Truck, Bus		

		- Bags: Backpacks, Hand-held Bags		
		- Hats: Hats, No Hats		
		- Upper Wear: Short/No Sleeves, Long Sleeves		
		- Lower Wear: Long, Short		
		· Colour - Identify objects according to any combination of Brown, Red, Orange, Yellow, Green, Lime, Cyan, Purple, Pink, White, Grey and Black		
		· Size - Select objects based on their actual (real-life) size from a histogram of sizes relevant to a specific case		
		· Speed - Select objects based on their actual speed from a histogram of speeds relevant to a specific case		
		· Dwell - Select objects dwelling for longer than a certain period in a scene		
		· Area - Identify objects included or excluded within one or more user-defined 3- or 4-sided polygon areas. The user shall be able to set the minimum duration the object spends inside the area.		
		· Path - Identify objects traveling along one or more user-defined paths. The user shall be able to set the minimum duration the object spends inside the area.		
		· **Appearance similarity – System shall be able to do filter and display only the objects matching similar-looking people (People Similarity) or Vehicles (Vehicle Similarity).**		

App Specification – Abandon Object detection				
S. No.	**Key**	**Description**		
1	**App detection**	The app should be able to detect Left and Unattended baggage in a camera view.		
2	**App Reporting**	The app should report the incident with an image marked with the region / area where unattended baggage is detected.		
App Specification – Person Collapsing				
S. No.	**Key**	**Description**		
1	**App detection**	The app should detect if a person walking upright has collapsed or fallen on the ground.		
2	**Configurable parameters**	The user should be able to configure the amount of time beyond which if the person is on the ground, the system should raise an alert.		
3	**App Reporting**	This app should raise an alert if any pedestrian is Jay walking.		
		The app should provide zone wise data of both the pedestrian movements at zebra crossings and jay walking with a minimum of hourly granularity.		
App Specification – AI Based Advance Intrusion Detection				
S. No.	**Key**	**Description**		
1	**App detection**	The app should be able to detect an act of intrusion. Intrusion herein refers to the instance of an individual crossing a pre-defined virtual fence defined by the user.		

2	**Configurable parameters**	The user should be able to configure the length and orientation of the virtual fence. She should also be able to define the direction in which crossing the line would be considered as intrusion. App shall have intelligence of identifying intrusion done by Human , vehicle or Animal		
AI based Crowd Estimation and Management				
S. No.	**Key**	**Description**		
1	**Introduction**	Crowd Estimation and Management (CEM) Video Intelligence system shall allow estimation of crowd density within the camera view. This is an important tool for understanding the crowd movement and management for the security and facilities management agencies. System shall raise an alert if the crowd density within a camera view is above a certain threshold.		
2	**Deployment**	The CEM System shall be a purely computer vision and artificial intelligence-based system that be deployed on all the existing and new CCTV cameras, including box cameras and PTZ cameras.		
3	**Camera compatibility**	The system shall be completely independent of the make/model of the cameras and be compatible with ONVIF compliant cameras. The CEM system shall support H264, H264+, H265 and MJPEG video streaming from cameras.		
4	**Accuracy on datasets**	The CEM system shall have 85% average accuracy in estimation of crowd on public databases and/or real time situation to be		

		given during proof of concept time/need to submit the test report. The accuracy should be estimated in a test dataset following standard train/validation/test split methods-during detailed engineering and design phase.		
5	**Ability to define regions**	The CEM system shall have an ability to annotate multiple regions within the camera view and the user shall be able to specify crowd thresholds for each of the regions separately. If within any region the crowd density estimation if above the user defined threshold, the system shall raise an alert.		
6	**Alerts**	The system shall raise alerts in case of the following:		
		- The CEM system shall raise an alert if the density of crowd is above a user-defined threshold.		
		- The system shall raise an alert in case of erratic movement detected within the crowd		
		- The system shall raise an alert if there is any chance of stampede or overcrowding due to increase in flow rate and erratic movement		
		- The system shall trigger alarm if more than desired density is observed near specified regions of interest.		
7	**Crowd flow estimation data**	The CEM system shall also provide a data of crowd flow from one user-defined region to the other, in case of two regions selected by the user.		

8	**Data representation**	The CEM system shall have an MIS system with a detailed report and dashboard on crowding events and data at a minimum of hourly granularity.		
		- The system shall report Crowd Density and direction to load-balance various gates.		
		- The system shall provide detailed counts of total visitors in hourly/daily/weekly/monthly and overall.		
		- The system shall also provide IN and OUT counters for all the visitors		
9	**Heat Maps**	The CEM system shall have an option of generating real time heat maps of crowd density.		
AI Based Camera Health Monitoring				
S. No.	**Key**	**Description**		
1	**Camera Status**	The Camera Health Monitoring app should be able to monitor the status of the camera and report an alert in case the camera is not functional or tampered with intentionally or unintentionally.		
2	**View Obstruction**	It should detect and raise an alert if the camera view is obstructed by any foreign object. The user should be able to adjust the threshold parameters of extent of obstruction in terms of percentage of camera view		
3	**Bright Light Shown**	The app should be able to detect and raise an alert if the camera view is tampered with bright lights. The system should specifically identify it as a camera tampering event with light shining.		

4	**Camera View Changed**	It should raise an alert if the camera view is changed/moved suddenly.		
5	**Illumination Too Low**	It should raise an alert if the camera scenes gets too dark below a threshold.		
6	**Camera Connectivity**	It should raise an alert if the camera is turned off or connectivity is lost.		
7	**Notification with Health Type**	The health monitoring app should notify the user with the type of camera health issue, namely: View Obstruction, Bright Light Shown, Camera View Changed, Low Illumination and loss of connectivity		
8	**Sensitivity Management**	It should have provision to adjust the sensitivity of detection on each camera		
Facial Detection System				
S. No.	**Key**	**Description**		
1.	**Detection**	Face Recognition System shall work on real time and offline mode for identifying or verifying a person from various kinds of inputs from digital **image file** and **live video source** from any IP video streaming sensor like IP Camera, Body Worn Cameras, Mobile handset cameras, UAV/Drones etc.		
2.	**Live and Offline Mode**	FDS shall be able to capture face images from live & pre-recorded CCTV feeds received		

3.	**Detections in crowd**	The system shall be able work to detect more **than 20 faces** in crowd on moderate face rotation either horizontal or vertical. It should support a yaw angle of **-40 to +40 degrees**, a pitch angle of -30 to +30 degrees and a roll angle of -30 to +30 degrees.		
4.	**Detection of partial faces**	The FDS shall recognize partial faces with varying angles from multiple videos simultaneously from Video clips, Group Photographs and VMS Playback directly from FRS Client Interface. FRS shall be able to process uploaded pre-recorded video feeds with a speed of up to X20, depending on the proposed hosting hardware and the video quality		
5.	**Ability to add reference Images**	The system shall be able to add photographs obtained from law enforcement agencies to the criminals' repositories tagged for sex, age, scars, tattoos etc. for future searches.		
6.	**Support for cameras/video formats**	The system shall support diverse graphic & video formats as well as live cameras. FRS shall support day/night operation with ability to detect faces both in colour and in black/white mode by using any H.264, H.265 Fixed IP and PTZ Cameras with IR Illuminators without any special configurations required		
7.	**User-management**	FRS must support a user management module that enables different user level groups to support various permission levels.		
		FRS client shall have ability to share recognition data like images & videos with		

		multiple users and operators for better reference, alarm & incident management.		
8.	**Image Enhancement Capabilities**	FRS system must have capability to enroll whatever images fed in the system with image enhancement and ability to verify the quality of the enrolled images with different colour indicator for low quality images enrolled in watch list/database.		
9.	**Image Format support**	The system shall be able to utilize any of the file formats like JPEG, PNG, BMP, TIFF etc. format for enrolment.		
10.	**De-duplication**	FRS shall be able to check if new enrolled face is already enrolled in the database before registering the new enrolled face in the system. Also, the system shall be able to find a previous detection of a POI (person of interest) upon enrolment to watch list (retrospective search) in less than 2 sec.		
11.	**Enrolment of faces**	The system shall have option to automatically enroll face images from CCTV cameras/video source. This functionality should also be provided through the Video Intelligence platform in addition to the FRS application.		
		The system should also have an option for Bulk Enrollment either from file system or a 3rd party databases such as UID, SAARTHI, IT, NCRB, EPIC etc.		
12.	**Categories of database faces**	The system shall have capacity to create different categories of people with option to customize the matching threshold for different categories.		

13.	**Full HD Support**	The system shall be able to work on full HD Camera video with maximum performance.		
14.	**Implementation**	The system shall be able to be implemented on IT hardware like Server or Workstation.		
15.	**OS Support**	The FRS algorithm should be able to use proven open source tools and technologies like Linux to bring down the total cost of ownership of the solution. FRS running on any other OS should be supplied with Pre-Licensed Server based latest version OS like Microsoft Server 2016 and Microsoft SQL as needed by the application		
16.	**Database Support**	The system shall employ database system like MS SQL/ MYQL/ Leading Open Source Database/Sybase/ Mongo DB/ Postgres/Oracle etc. The FRS system should natively integrate with Video Intelligence platform and use a common database of the platform, so that common queries can be made on the common database for faces detection and other events.		
17.	**Algorithm Benchmarking**	The Vendor should have any performance benchmarking certificate. NIST certificate will be preferred.		
18.	**Performance**	The system must perform a full 1: N search of the probe image in under 5 seconds against a database of up to 50 mn face records.		

19.	**Mobile Application Support**	FRS Software vendor shall have mobile application of the same FRS software to support iOS and android based smart field devices. Mobile application shall be capturing the face of suspect in field and sending back to the FRS server for matching. Matching result shall be shown on the mobile application screen with matching score. There shall be provision in mobile application to stream mobile device camera as video streamer.		
20.	**Detection robustness**	System shall be able to detect the faces across the multiple CCTV video sources for online (real-time) and offline modes regardless of following conditions:		
		a. Changes in Facial expression		
		b. Changes in facial hair or hairstyle		
		c. Changes by moderate aging (up to 15 years)		
		d. Partially hidden faces or occluded faces like wearing dark glasses mask etc.		
		e. Changes in lighting conditions		
21.	**Search Capabilities**	Simple Search UI that facilitates quick and easy access to the collection of events recorded by the system without the constant monitoring by operators and must perform a full 1: N search of the probe image in under 2 seconds against a database of up to 5-8 Million POIs. It shall support following		
		a. Search previous events by images from previous detections		

		b. Search previous events by images uploaded by operator		
		c. Search previous events by enrolled names		
		d. Search previous events by date and time		
		e. Search previous events by watch list group		
		f. Search in Watch list by image		
22.	**Retrospective Search**	FRS shall have capability of Search backwards for previous detections and/or recognitions (events) of the detected person without enrolment from live CCTV & other forensic videos / offline videos		
23.	**Up to 5 nearest matches support**	FRS shall have ranking features to show next 5 closest & similar subjects in the Watch list with nearest score to the detection. This option enables you to review POIs that are potential matches for this detection for efficient system performance.		
24.	**OEM owned algorithm**	The FRS OEM should have ownership of Face Recognition Engine /Algorithm for any custom specific development as required by client		
25.	**Map feature**	FRS must allow tracking of person on maps to be uploaded in the system for cameras connected to FRS and shall highlight the camera location on the map for each detection/alert.		

26.	**SDK/API for integration**	FRS shall provide an SDK/API for integration with any third-party software like C4I (Command, Control Communication & Compute Center). API must be available with a full set of documentation of each method with accompanying sample code. All FRS function shall be fully accessible via API.		
27.	**Video Alert**	FRS shall be able to play a short video clip of the moment of face detection without dependency on VMS which can be downloaded/exported/saved for evidence proof		
28.	**Timeline of detections**	FRS shall provide timeline sequence of all detections of subject with date, time & location.		
29.	**Email Integration**	FRS shall support email Alerts via Gmail, Outlook or via an Exchange SMTP service. Different recipients can be defined for different Camera Groups. User shall be able to define how frequently recognition/detection emails are sent, the email subject and the email sender (among other things). The email itself includes the timestamp of the detection, the score, the description, the reference image (defined in the Watch list) and the detected image.		
30.	**Minimum hardware support**	FRS Application Engine must be able to run a minimum of 20 FRS Camera Channels per Server. (Server with 128 GB RAM, 3 NVIDIA Tesla T4 card with 40 cores.) Other optimized and better sizing shall be accepted.		

31.	**Use of AI accelerator hardware**	FRS shall use extensive AI Technology and perform video processing on GPUs like NVIDIA; INTEL or similar as per design & sizing vetted by AI FRS Algorithm OEM. The number of servers to be supplied, shall be based on the number of camera channels on which the FRS needs to be performed.		

Volume-3

43.6 Measurements & Targets

43.6.1 Implementation Phase Related Performance Levels

S. No.	Measurement	Definition	Target	Penalty
1	Team mobilization and commencemen tof work	SI is expected to mobilize project team for commencement of work. Commencement of work would mean reporting and availability of SI's resources (90% Key Personnel as per the RFP requirement) at the Authority's office for the project within defined period of 15 days and remaining 10% in next 15 days)	Within 15 days of Issuance of LOI or Contract Agreement , whichever is earliest	Delay beyond 7 calendar days = 0.2% of the contract value Delay beyond 8-15 calendar days = 0.5% of the contract value Delay beyond 15 days may lead to penalize up to 5% contract value at the discretion of the authority.