

This document is released by Directorate of Information Technology (DIT), Government of Maharashtra, Mumbai under Creative Commons License (Attribution 4.0 International).
See <http://creativecommons.org/licenses/by/4.0/>

**<CITY> CCTV based
City Surveillance
&
Smart City Framework**

Detailed Project Report

Table of Contents

Executive Summary of the Project Report.....	3
1. Introduction	4
1.1 About <CITY>	4
1.2 Project Vision	4
1.3 Project Coverage	4
2. Scope of the Project.....	6
2.1 Key Highlights.....	6
2.2 Components of the CCTV Surveillance System	7
2.3 Scope of Work for the System Integrator.....	9
3. Proposed Tender Conditions	20
3.1 Proposed Eligibility Criteria.....	20
3.2 Proposed Payment Terms	21
3.3 Selection criteria of OEMs for Camera, VMS, Analytics and Switches.....	22
4. Service Level Agreements	23
4.1 Definitions.....	23
4.2 Measurement of SLA.....	24
4.3 Planned Downtime.....	24
4.4 Pre Implementation SLA	25
5. Responsibility Matrix.....	32
6. Project Implementation Timelines	34
7. Estimated Project Cost.....	35
8. Annexures	36
8.1 List of the proposed Camera Locations & Camera distribution	36
8.2 Proposed Benchmark Specifications for IT Components	38
8.3 Functional Requirements for the roposed Surveillance System.....	62
8.4 Proposed Benchmark Specifications for Non-IT Components.....	69
8.5 Functional Layout for Command & Control Center	80
8.6 Proposed Bill of Material (BoQ).....	81

Executive Summary of the Project Report

1.	Name of the Project/Initiative	<CITY> Area CCTV based City Surveillance & Smart City Framework
2.	Location	<CITY> Area in <State>
3.	Objective of the project	<ul style="list-style-type: none"> ▪ Assist Police to respond faster in case of any incidence detection ▪ Assist Police in detecting crime & Act as an aid to investigation ▪ Act as a deterrent to crime & traffic violations ▪ Improve Traffic Management ▪ Integrate with the CCTV Surveillance System of large Private / Public institutions to connect to their feeds during the crisis situation. ▪ At select locations, make connectivity available for 'Smart City Project' Components
4.	Scope of the Project	Please Refer Section No. X, Page X
5.	Estimated Cost of the Project	<p>Total Estimated Project Cost of Rs. XX.XX Cr.</p> <ul style="list-style-type: none"> ▪ CAPEX of Rs. XX.XX Cr ▪ OPEX of Rs. XX.XX Cr (for YY yrs) ▪ Provisioning for Adaptive Sourcing of Rs. XX Cr <p>For further details, Please Refer Section No. X, on Page XX.</p>
6.	Expected time for completion activity	<ul style="list-style-type: none"> ▪ Selection of the System Integrator within 3 Months ▪ Go Live of the <Area 1>, <Area 2> and <Area 3> Area in 7 Months of selection of SI ▪ Go Live of the entire project in 10 Months of selection of SI <p>Please refer Section X on page XX for the detail timelines</p>

1. Introduction

1.1 About <CITY>

<Write City description here>.

1.2 Project Vision

Vision of the project is to implement holistic and integrated video surveillance system for the above mentioned nodes of <CITY>. This system shall also integrate with surveillance systems of different stakeholders with the objective of enhancing safety and security in the city. The system shall help-

- Support police to maintain Law and Order
- Act as an aid to investigation
- Improve Traffic Management
- Help in deterring, detecting and thus dealing with criminal activities
- Address threats from Terrorist attacks
- Attain faster turnaround time for crime resolution and proper investigation
- Monitoring of suspicious people, vehicles, objects etc. with respect to protecting life and property and maintaining law and order in the city
- Continuous monitoring of some vital installations/ public places in <CITY> area for keeping eye on regular activities & for disaster management support

The Proposed video surveillance system will enable the above by following:

- Providing alerts/ feedback to the Police Department about abnormal movements/ suspicious objects etc.
- Better Management of Security breaches based on alerts received from system
- Improved turnaround time in responding to any investigation case, faster access to evidence in case of security breach, law violation in the prescribed areas.

1.3 Project Coverage

<CITY> intends to implement security and surveillance system in the areas within jurisdiction for following nodes, in consultation with Police Department <City>:

- <Area 1>
- <Area 2>
- <Area 3>
- ...

Typical types of Locations to be kept under surveillance are:

- Entry and Exit points of the City / Toll Nakas
- Important Chowks
- Traffic Junctions
- Important Road Stretches (accident prone areas)
- Railway Station Entry/Exit
- Entry/Exit of Schools, Key Residential Places, Market Places, Jetties
- Vital installations in the city

The Joint survey has been carried out with the Police Department, <City>, in the areas under jurisdiction of respective police stations covering above mentioned nodes for identifying the locations

to be covered for CCTV cameras. Location those has been identified/ proposed for CCTV cameras covers entry and exit points, toll nakas, important chowks, junctions, roads, railway station premises, schools, residential place, market place, jetties and vital institutions in the city. List of police station visited and details of locations visited under respective police station are given as part of annexure.

Main Project Stakeholders

- <CITY administration>
- <City> Police Department

Other Project Stakeholders

- Project Management Consultant (if applicable)
- System Integrator (SI) – To be selected
- Airports, Railways
- Shopping malls, multiplexes, theatres, schools, hotels, hospitals and other public places
- Financial Institutions, Corporate Houses
- Citizens in General

2. Scope of the Project

2.1 Key Highlights

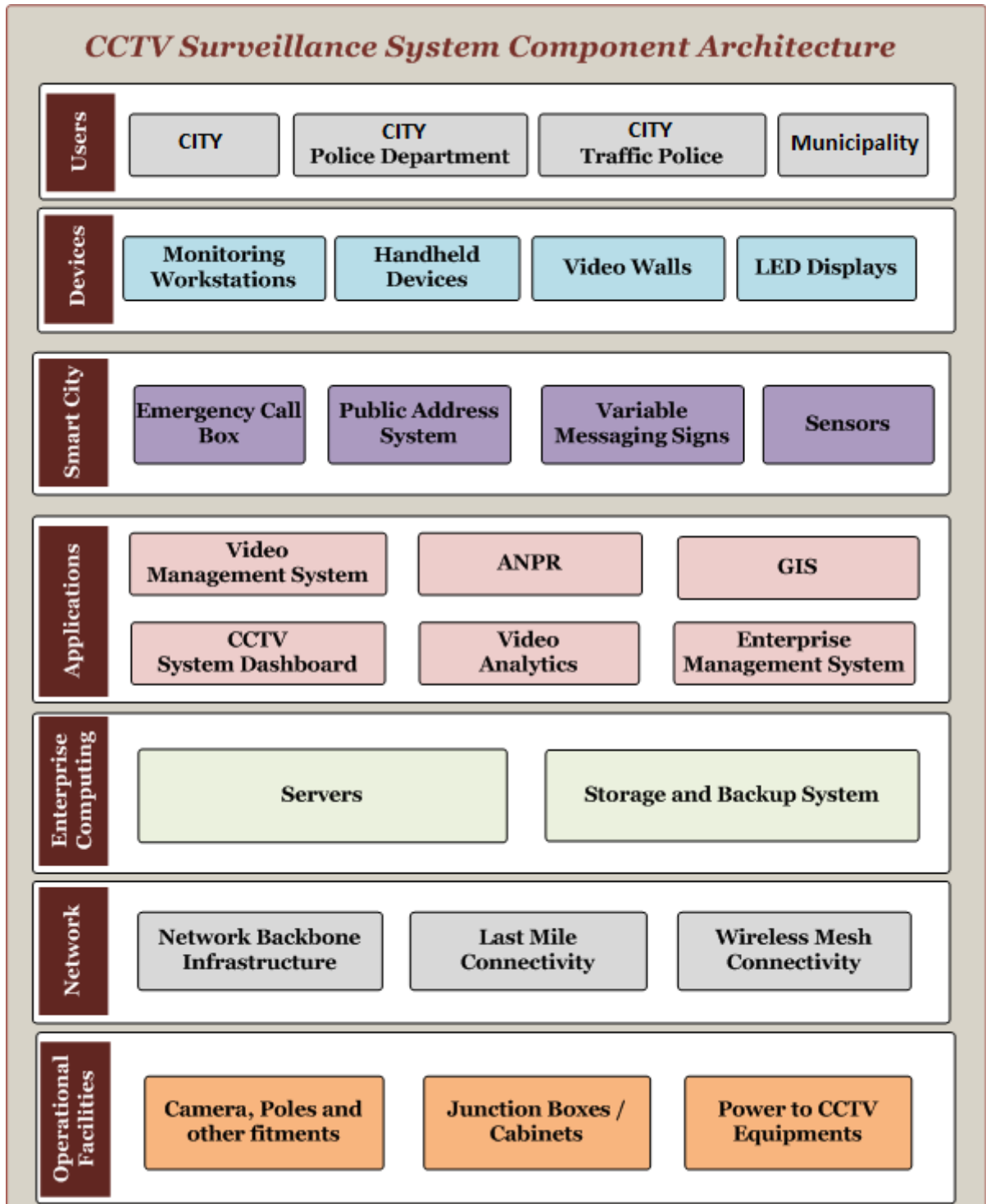
The proposed video surveillance system will involve setting up of IP based outdoor security cameras across various locations in the <CITY> Area. The video surveillance data from various cameras deployed will be stored and monitored at Command control centers and Viewing center at <CITY Location>

Key highlights of the scope of work of the successful System Integrator are as follows:

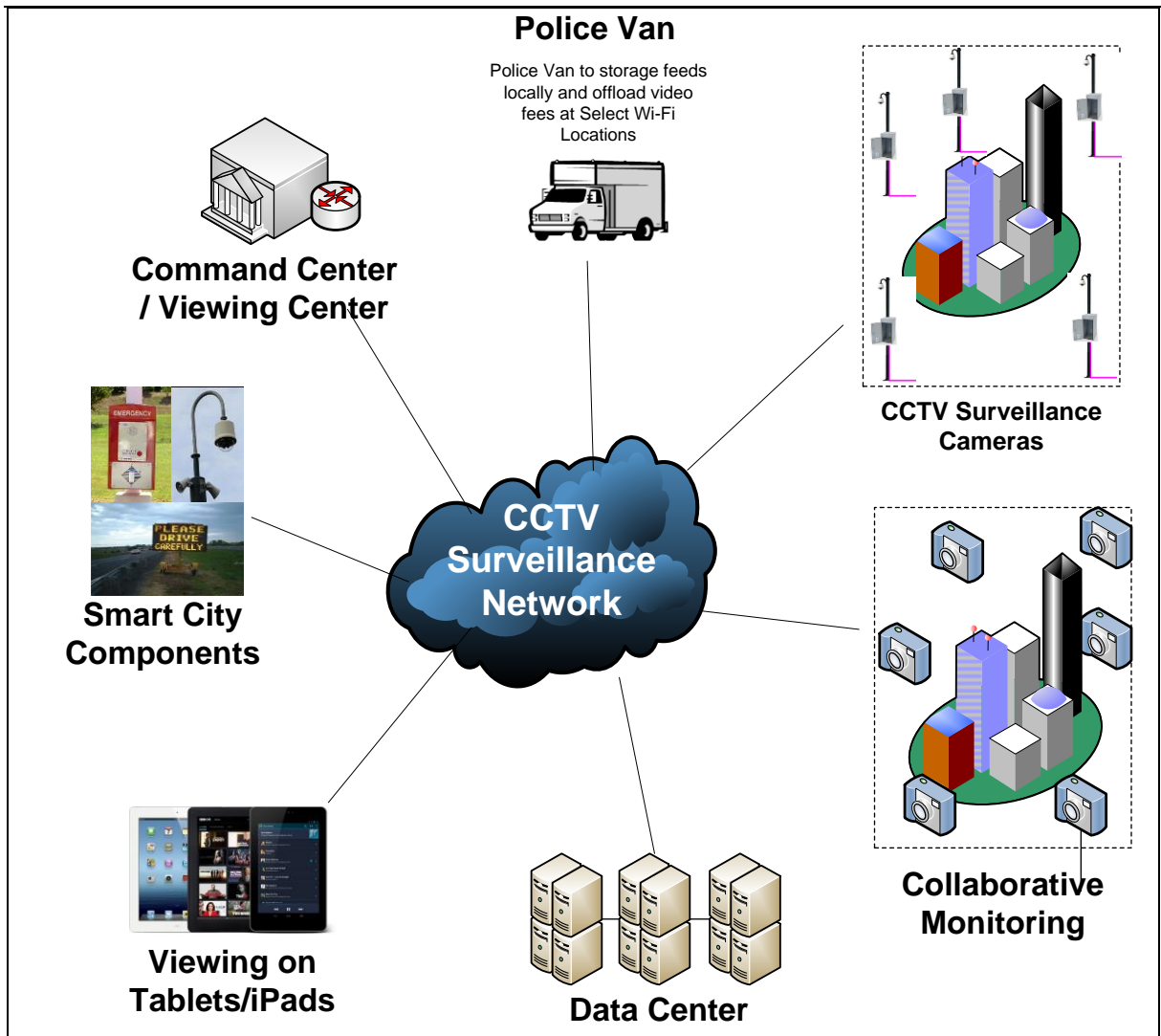
- Locations : Approx. **XXX**
- Cameras : Approx. **XXX** (Full HD : 1920 X 1080)
Plus **X** cameras on **X** Police Vehicles
- Smart City Components : Emergency Calling Boxes – **XX** locations
Public Address System – **XX** locations
Variable Messaging Signs – **XX** locations
Connectivity for Smart City Sensors – All locations
- Command Control Centers : **X** (CP Office)
- Viewing Center : <XX> & Tablets/iPads for select officials
- Data Center : In
Commercial Data Center
- Storage of feeds : **30**
days storage of video feeds
- Viewing & Storage Frames : **15 FPS**
during movement period & **8 FPS** during no
movement period
- Collaborative Monitoring :
Integration with about **XX** CCTV systems in
other Establishments
- Project Go Live Period (all regions) : **X Months** from the date of Work Order
- Maintenance & Operations Support : For **5 years** from the Go Live date

2.2 Components of the CCTV Surveillance System

Various components of the project, including the users expected to use the system are shown in the diagram below.



A High level system overview of the proposed CCTV Surveillance System for <CITY> area is given in the diagram below:



2.3 Scope of Work for the System Integrator

From the overall scoping perspective, project requirements have been classified into the following main components.

2.3.1 Surveillance Equipment

The project includes surveillance of about **220 locations** across <CITY> Area. These locations would get covered through different types of surveillance cameras including Fixed Box Camera and PTZ Cameras.

- **Total Approx. 500 Cameras**
 - About **XX** PTZ HD Cameras
 - About **XXX** Fixed Box Cameras
 - About **XX** Cameras to support ANPR System
 - About **XX** ANPR Cameras to capture License plate at **60 FPS**
 - About **XX** Cameras on Public transportation
 - All Cameras to support Analytics

The project also envisages transportable video surveillance by putting surveillance cameras upon 3 vehicles of <City> Police to further strengthen the coverage of some incidences / events. Video feed from all these locations shall be stored locally (**16 hour local feed storage** will be provided) and offloaded wirelessly over select Wi-Fi spots such as Parking lots, Command Center / Viewing Center, etc. The Cost of Van Drivers, Fuel, Vehicle Maintenance and Insurance cost, etc. would be borne by **concerned Government Department**.

The Audio facility of all CCTV cameras (to capture audio from the field) may need to be kept disabled and police should take appropriate decision in this regard from the perspective of privacy.

The System Integrator (SI) shall assess the feasibility to use any existing electricity, phone or advertisement poles that are under <CITY>'s jurisdiction during initial site surveys. SI shall also assess the feasibility of leveraging other structures such as areas under a bridge or billboards. For the locations identified for re-purposing the existing poles or structures, an agreement shall be signed between the **SI, <CITY>, MSEB, MTNL** and other relevant stakeholders for use of the facility for the **<CITY> CCTV Surveillance Project**. No advertisement rights shall be given to the SI on poles / at last mile.

UPS requirement on last mile is not mandatory, however, SI should ensure that proper protection is taken against power surges and ensure power stabilization to the surveillance equipment. The System Integrator would need to follow required earthing standards (e.g. IS-3043) and ensure that pole and the edge level components are protected against lightning. In addition, Junction box design should be modular and each component should be well organized and clamped inside to ensure components do not heat up or fall out on opening. The Electricity/Power costs for the **<CITY> CCTV Project** will be borne by **<CITY>**.

Select locations would be identified for placing Radar based Speeding Vehicle Detectors, integrated with CCTV Cameras to capture vehicle number plate & photographs. These would be ANPR cameras that would be expected to work at **60 FPS**. Multilane, double sided ANPR cameras with speed calculation features to be preferred. If ANPR recognition fails, these cameras should at least be able to capture a clear image of license plate for investigation purposes.

The video feeds will be recorded, stored and viewed **at Full HD Video quality i.e. 1080p (1920 X 1080 resolution)**. In some cases, video streaming into the system from a few handheld tablets/cameras or cameras attached to Motorcycles etc. can be done through 3G or 4G at low, compressed frame rate, while recording can be done at higher or better frames/resolution which can be offloaded later into the system.

Unmanned aerial vehicles (UAV) and Drones are going to be critical components in future to any security surveillance system where these machines can be deployed into sensitive / inhospitable environments for surveillance and transmitting video feeds to the Command center. Integration with Third party drones as an option could also be explored.

The project also envisages transportable video surveillance through 3 Police vans to further strengthen the coverage of some incidences / events. The Police vans will be provided by the Police Department; however the mounting of the cameras and connectivity to the cameras and other system is the responsibility of the SI. Video feed from all the Police vans shall be wirelessly offloaded to storage system as soon as it enters the Command center / Viewing Center or the Parking lot vicinity. The Video feeds should be made available to the Command Centers and Viewing Centers based on their jurisdiction / role. Offloading of video feeds from the mobile vans shall be made automatic and it should be ensured that there is no duplication in the same.

Indicative list of the Bill of Material for each Police Vans is as follows:

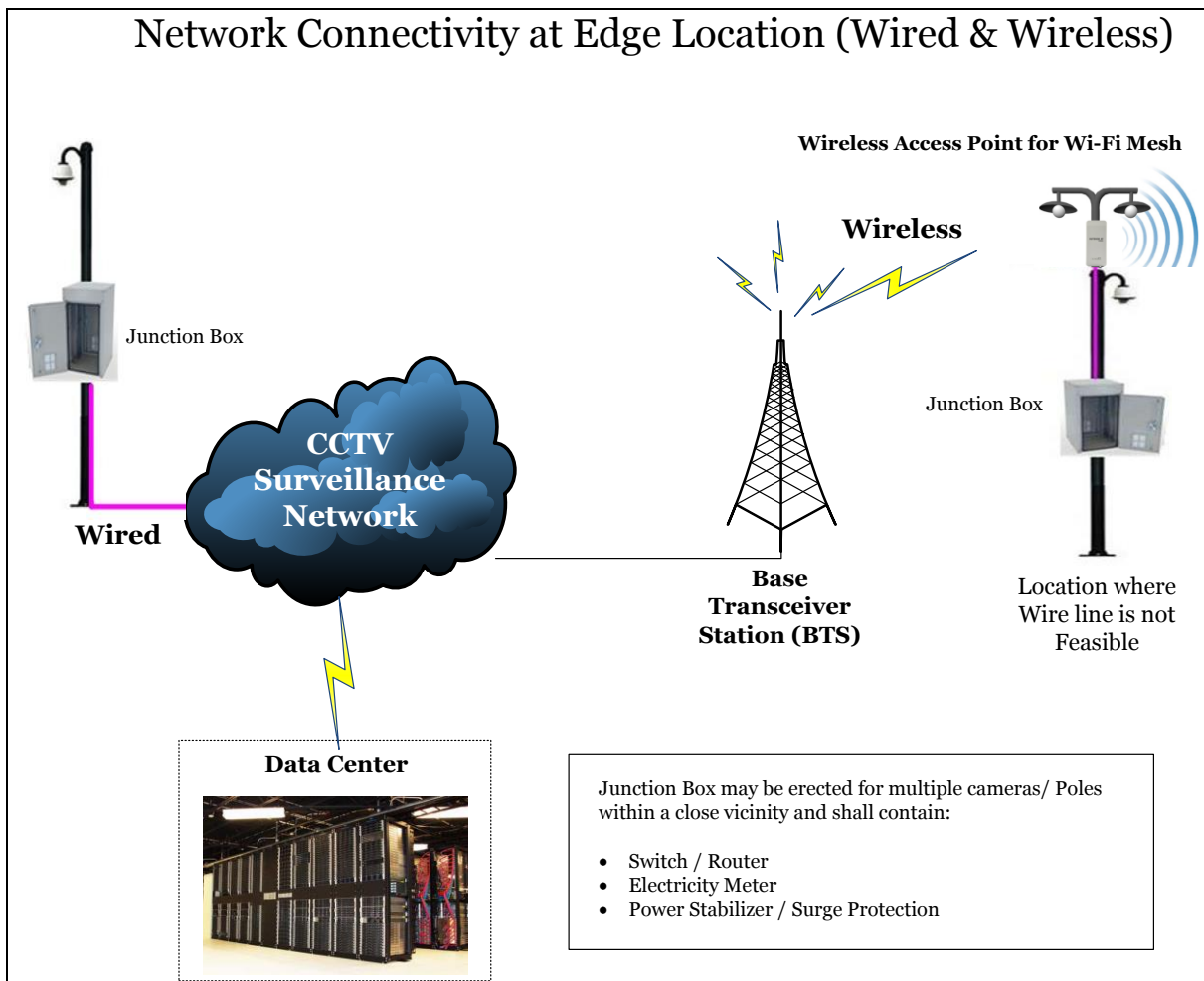
- 1 Laptop with 18.5” Screen (for local viewing)
- 2 Outdoor Fixed Box Cameras
- Local Storage for 16 hours
- Mounting Accessories
- 1 Video Full HD Handheld Camera with capability to stream videos through WiFi / WiMax.
(Vendor to propose a handheld camera meeting the common benchmark specifications specified for Fix Box cameras.)
- Cabling
- Installation, Testing and Training

Approximately XX buses could be used to monitor the freeways and critical routes by having external cameras mounted securely on them, with 16 hours storage facility. The video feeds can be stored locally and offloaded wirelessly in a batch mode manner while the bus is stationed at the depot.

2.3.2 Network

Robust, reliable and scalable network shall be deployed to enable converged communication. The points of connection include Cameras, Data Centre, CP Office Command Center, and <X> Viewing Center. All the required equipments (active and passive both) for establishing such connectivity and meet the service levels specified in the RFP will need to be deployed as a part of the overall networking solution. Networking requirements also include the LAN creation at Data center and Command center. A high level connectivity diagram, considering MPLS as the backbone to be used for the bandwidth is shown below:

- Establish connectivity between following -**
- Between Cameras & Aggregation Point at edge level
 - Between Aggregation Point & Data Center
 - Between Data Center & Command / Viewing Center



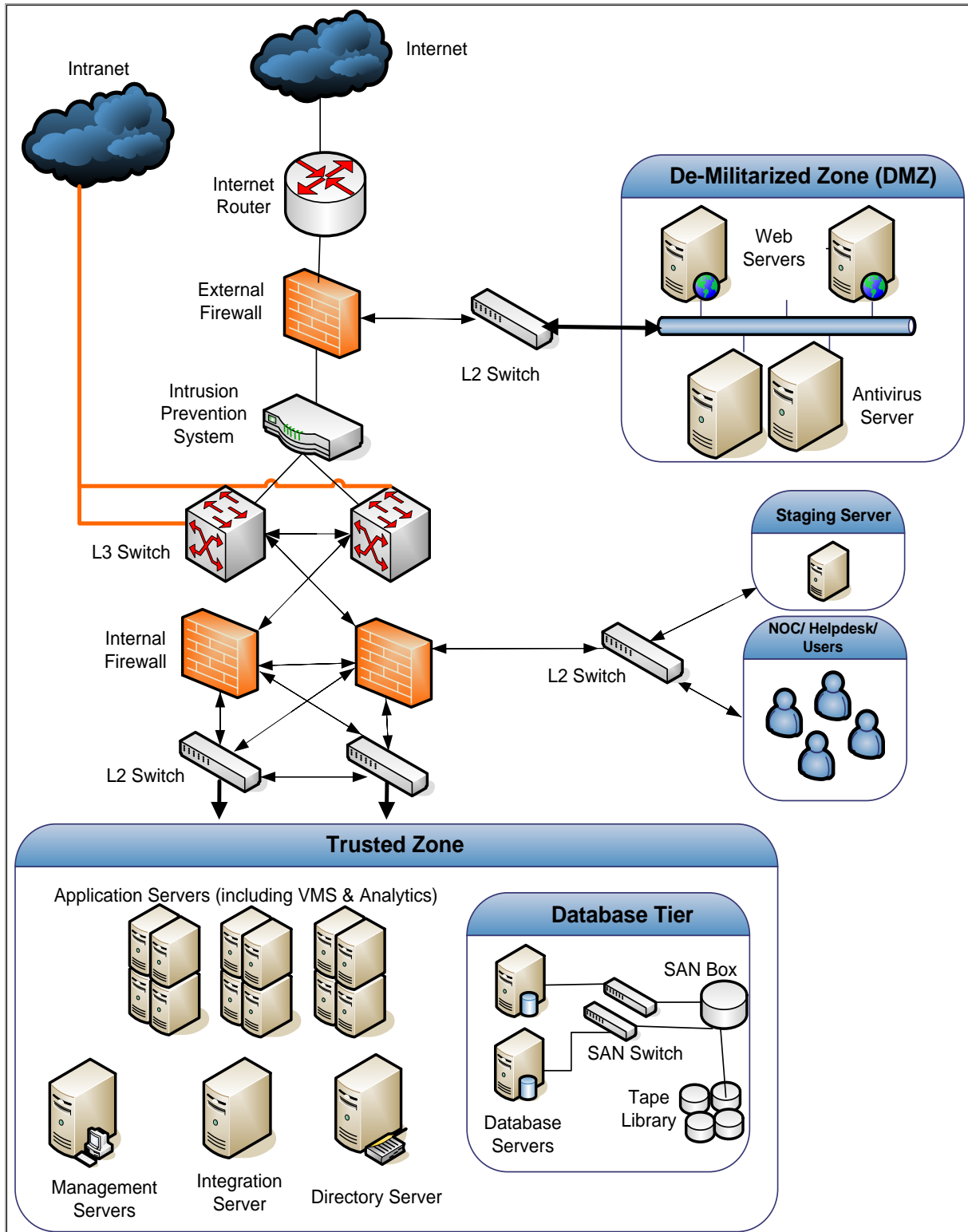
The System Integrator shall be allowed to propose network connectivity solution involving multiple service providers and using different technologies like OFC, Wireless, 4G, etc. Wherever System Integrator opts for wired connectivity, he shall be asked to use existing ducts and only then opt for Horizontal Directional Drilling (HDD) as an option for Fiber Optics laying. If, for certain location, the two options are not viable, then the SI should opt to dig to lay Fiber.

SI shall create WiFi mesh at the last mile (for all locations identified) to connect multiple smart city components (section 2.3.7). At the junction, Two ports on the switch/router to be kept open for Smart city components. At a later stage, other agencies and third party vendors can use this wireless mesh infrastructure to add additional smart city elements. On one port, a rugged WiFi point with min.

2.3.3 Data Center, Application Portfolio

It is proposed to host the Server Side Infrastructure in the Commercial Data Center within <City>. The Data center should be **at least Tier III data centers** and the DR site (for data back-up) should be preferably within the CP Office / <CITY> Office.

An indicative Network Architecture diagram at the Data Center is show below. System Integrator shall submit the suitable design to meet the project requirements to <CITY> for approval at design stage of the project.



Applications deployed in the Data Center would act as the brain of the system. Keeping in view the needs of interoperability and integration, especially the possibility that the solution would become the focal point for maintaining law and order in the city by the Police in future, the solution should be built on Open Standards. The datacenter shall also host application required for SLA monitoring and Help desk management. The SI should bear in mind that the System should have capability to access important cameras (identified by Police during implementation period) at CP Office Command Center even if the Data Center is unavailable.

The key components of the Application Portfolio are Video Management System, Recording System, Analytics System, GIS and the customized Dashboard for various categories of personnel. Police Department has estimated requirement of about 40 cameras, covering Octroi Nakas & Key Junctions, for implementation of Automatic Number Plate Recognition (ANPR) System. Apart from ANPR requirement, Analytics support is required on all cameras. System should support following Analytics:

- Unidentified object detection #
- Motion / intrusion detection #
- Noise level detection (gunshot, explosion, shattering of glass, etc.) #
- Camera Vandalism and tamper detection #
- Virtual Fence / Tress Passing / Tripwire #
- People / Mass movement #
- Vehicle tracking based upon the color, shape of the car (*optional*)
- Traffic violation detection (through integration with Signaling System)
- Matching of suspect / criminal photograph with different databases available with Police
- Vehicle speed detection radar system (video feeds for this should be captured at 60 FPS)

SI should provide option to run these analytics at edge level so that bandwidth can be saved.

Video Analytics system shall provide mechanism to allow alerts to be raised in a customized manner (i.e. certain types of alerts shall be raised in Command Control, certain types of alerts shall be raised to pre-designated officials & certain types of alerts may be asked to be made part of Decision Support System). Inputs would be also taken to avoid generation of false alarms.

The VMS shall allow access of the video feeds on Tablets/iPads/select devices on request. Such an access shall be based on MAC Address authentication over SSL (Secure Socket Layer) and/or by creating a VPN (Virtual Private Network) at minimum. In addition, the VMS should be able to stream feeds from authorized Tablets/iPads/select devices on the Video Wall.

The proposed new CCTV System shall be integrated with the existing CCTV System implemented at CP Office by <City> Corporation to allow viewing / storage of the existing cameras on the new system. The SI could explore the possibility to even integrate the proposed CCTV system to the existing Video Management System of the <MUNICIPALITY> CCTV Surveillance system. It shall also be integrated with CCTNS, VAHAN System of Transport Department and Stolen Vehicle databases. Stolen Vehicle Database integration shall be used to generate alerts in case stolen vehicle is captured onto the ANPR camera. Integration of CCTV System with criminal database will be used to primarily assist Police Department in matching images with a database of criminals / suspects or match still images with video feeds.

The Proposed CCTV system shall also be integrated with Dial 100 application and the call dispatch process at the police control room. The solution of automatically pulling up the location of the caller on a map and displaying the camera feeds from that location on the video wall (on command) should be explored. There would be several types of reports (Incident types, number of incidents by area, frequency of a certain incident, resolution time, etc.) that would need to be generated post the integration with the Dial 100 application.

2.3.4 Command Center / Viewing Center

All camera feeds shall be available for viewing by Police Personnel at any point of time. CP Office Command Center is proposed to have simultaneous viewing capability for about 10% of all cameras. <CITY> Viewing Center shall have viewing capacity of about 24 cameras at a given point. The <City > police will provide viewing manpower at the Command Control Center

The existing CCTV Command Centre at CP Office to be expanded so that it can handle feeds from both, <CITY> and <MUNICIPALITY> cameras. There already exists a separate Control room at CP office that manages <CITY> and <MUNICIPALITY> Areas. The Command Control center will also have a room identified for IT Analytics and Forensic Experts where they will analyze the incriminating video clips and certify its integrity & chain of custody. These experts shall oversee the integration of ANPR with the other relevant databases and also undertake R&D to evaluate and analyze various analytics related technologies and their implementation over the years. In addition, there will be a small control room in <CITY> to handle smart city components.

Broad level Bill of Material for Client Side IT Infrastructure at different command / viewing centers is given below:

Central Control Centers (at CP Office)

Broad level Bill of Material required at the Central Control Center at CP office is as follows:

IT Components

- Video Wall – Min. 46” LED Displays (Full HD) mounted in a 5 X 4 arrangement – XX no.s
- Touch Monitors – X nos.
- Monitoring Workstations (Computers) – X nos.
- Additional min. 46” LED Displays (Full HD viewing capacity) – X nos.
- Network Color Laser Printers – X no.
- Indoor Fixed Dome Cameras for Internal Surveillance (3 fixed box cameras)
- Active Networking Components (Switches, Routers)
- Passive Networking Components

Non-IT Components

- Electrical Cabling and Necessary Illumination Devices
- Fire Safety System with Alarm
- Access Control System (RFID/ Proximity based, for all staff)
- Full Biometric System to control entry / exit
- Office Workstations (Furniture and Fixtures)
- Comfort AC
- UPS (1 hour backup)
- Automatic DG Set to provide power backup for 12 hours to the command center

Note : The Civil work towards the Command Center (Construction of new structure / Expansion of existing structure, painting, etc.) and the furniture work (partitioning, false ceiling, flooring, chairs, tables, etc.) has not been considered in the cost estimation, since it was discussed that this would be taken up as a separate activity. A functional layout for the Command & Control Center is given in **Section 8.5.**

Viewing Center at <CITY>

Broad level Client side Bill of Material required at <CITY> is as follows:

IT Components

- **Min. 46" LED Displays (2 nos.)** (Full HD viewing capacity)
- Monitoring Workstation (4 no.) (Computers)
- Switches / Routers

Non-IT Components

- Office Workstations (Furniture and Fixtures)
- UPS (30 minutes backup)

2.3.5 Collaborative Monitoring

Already certain surveillance systems have been deployed by many public & private establishments. Therefore it becomes imperative for <City> Police to have a system which will have a collaborative framework for receiving video feeds from these systems and sub-systems. It is recommended to prepare the list of such institutions for which collaborative monitoring shall be implemented. For cost estimation purpose, it is assumed that the <CITY> CCTV Project shall be equipped to access the camera feeds of about 20 odd large institutions from <CITY> area, which have 50+ cameras. (This number needs a finalization in discussion with Police Department). As a part of the project implementation plan, the integration with the establishments identified for Collaborative monitoring would be tested for at least 1 week.

As a part of the Collaborative Monitoring effort, the system shall also facilitate citizens to upload video feeds to the CCTV System. However, this will be subject to administrative and technical checks so that frivolous or defamatory videos are not uploaded for e.g. a one-time password (OTP) would be generated for each citizen user to first authorize and then authenticate them to use the App

VMS shall have provision to ensure that such video feeds are continuously streamed on one of the cubes of the Video Wall. As a part of the <CITY> CCTV project implementation, the SI would test the integration with the establishments identified for Collaborative monitoring over a period of minimum 2 weeks before Go-Live of the collaborative monitoring component.

<CITY> shall form a committee for making of SOPs for video / photo sharing by other Public / Private institutions and privacy issues related to the CCTV project. The Committee will take decisions on what kind of masking may be allowed while sharing the evidence related information.

2.3.6 Help Desk and Facility Management Services

As part of Facilities Management System (FMS) the Command center to have dedicated man power, to be provided by the System Integrator to troubleshoot & solve issues / problems. The FMS shall be supported by a centralized helpdesk, to be located near the Command Center. This Helpdesk shall be the single point of contact for complaint management & resolution for all the users of the surveillance system. This helpdesk shall be integrated with the Enterprise Management System. The helpdesk shall be designed to meet the SLA response & resolution timelines.

2.3.7 Components of the Smart City System

Along with the components of the CCTV Surveillance system, the SI would be responsible to integrate the following services with the CCTV Surveillance system to build an infrastructure for a Smart city system in the <CITY> Area. The scope elements of the Smart city system are (images are only indicative of the requirement):

2.3.7.1 Emergency Call Box System

- A high quality digital transceiver, to be placed at certain locations determined by the <City> Police Department (mostly at junction boxes / camera poles to avoid a additional investments)
- Key is to make it easily accessible by public
- The unit shall preferably have a single button which when pressed, shall connect to the Police Department over the existing network infrastructure setup for CCTV Surveillance system.
- At some of the locations, this can be also used for Public Address
- These are to be placed only a select locations (about 10) such as Police/Traffic islands or pedestals or within the vicinity of constant Police supervision to avoid misuse and vandalism of the call box.
-



2.3.7.2 Public Address System

- Use of Public Address System at select public locations / junctions (about 20 locations)
- Integration with VMS to allow its use during crisis situation.
- Access control mechanism would be also required to establish so that the usage is regulated.
- This is to be IP based and the control room should have the capability to control individual PAS i.e. to make an announcement at select location (1:1) and all locations (1 : many) simultaneously. The PAS should also support both, Live and Recorded inputs.



2.3.7.3 Variable Messaging Signs

- The Dynamic Messaging Signs on roads can be used to provide dynamic information to commuters at strategic locations / main entrance roads to display traffic related information, traffic notifications, awareness, event messages.
- Dissemination of information can be intended help to commuters in making effective travelling decisions and reduce travel time and congestion.
- These messaging signs can be used to increase commuters awareness by regular display of traffic advisory, thereby improving the traffic discipline



- Such an infrastructure can also be used to gather statistical data on traffic & weather from sensors for further use.
- This would need to be installed in about 10 locations (identified by Police) and the text on the sign must be readable even in broad daylight.
- The messaging sign would be a digital display over a single pole.
- It would measure min. 32 sq. ft. and would be dual sided display.

2.3.7.4 Parking Lot Availability Automation

- Parking lot availability automation shall be implemented at following **Railway Stations** to be implemented on priority: **S1, S2, S3 etc.**
- Scope of SI shall include creation of a mobile app to be made available to the Parking Managers for updating the parking availability. Scope shall also include hand-held devices to be made available to the Parking Managers for online updating such data.
- Information about the Parking Availability shall be made available to public through mobile apps and on Variable Messaging Sign Boards.

2.3.7.5 Connectivity for Sensors & other Smart City Initiatives

- System Integrator shall provision additional bandwidth of 128 KBPS at select locations, for Smart City Initiatives like temperature sensors, air quality sensors, flood water sensors, fire / smoke sensors, capture GPS data from select vehicles, etc. and other Green city initiatives.
- To be provided at about all the camera locations
- The Viewing Center at <CITY> Municipal Control Room shall have provision for spacing and seating for about 4-5 people to control the smart city elements, gather data, etc. and Police to have about 2 people (can be part of proposed IT forensic room) for controlling smart city components

2.3.7.6 Integration with e-challan Smart Traffic Enforcement

- Police Department shall be implementing a Smart Traffic Enforcement System in the <City> area by using mobile devices for issue of challans to traffic rule violators. Police shall be able to issue and print the challans on the spot using smart phones and/or handheld thermal printers.
- A total of about **60-100** field level traffic officers are intended to be provided with smart devices to undertake traffic management
- The proposed system should integrate with CCTV ANPR cameras such that the Police would have the capability to issue challans based on reading of the License plate. The updated address of the owner can be received from integration with Insurance companies and RTO. In addition to the Integration with the CCTV Network, if a license plate of a 'wanted vehicle' is captured on the system, a SMS should be sent to a registered/authorized number (typically of a high rank Police official) with timestamp and latitude/longitude of the location.

2.3.8 Information security policy, including policies on backup

System Integrator shall be asked to prepare the Information Security Policy for the overall project, which would be reviewed & finalized by the <CITY>, <City> Police Department & its Consultant. It is proposed that Security policy would be submitted by the Systems Integrator within 1st quarter of the successful Final Acceptance Tests.

The Systems Integrator shall obtain ISO 27001 certification for the CP Office Control Center within 2 quarters of final acceptance test. Payment from 3rd Quarter to be with held till this certification is obtained by the successful bidder.

2.3.9 Adaptive Sourcing

<CITY> intends to implement a state-of-art system. It is also important that the project continues to adapt to the new technologies which can enhance the outcome and assist <CITY> / Police to meet the objectives of the project in improved manner.

<CITY> would like to provision INR 1 Crore per year (post go live of the original system) or upto 10% total CAPEX cost (whichever is minimum) towards Adaptive sourcing, during the 5 year project duration. A committee should be authorized to negotiate with SI, based on market cost plus fair profits, for any new additions to the project. For bigger components, it could be new tender, but SI could be compensated for its integration efforts from this Adaptive sourcing funds. However, any technological changes which actually can reduce costs to the SI, while enhancing quality of project, would obviously not be compensated further from <CITY> funds.

Following process shall be following for the same:

- Proposal for adaptive sourcing shall be submitted by either <CITY> or by SI to the “Project Steering Committee” during the post-implementation, contractual period
- Proposal shall clearly identify the proposed solution, innovativeness of the solution and it’s cost-benefit analysis
- Steering Committee shall evaluate the proposal worthiness and satisfy itself on the commercial proposition
 - take demonstration of the product / solution
 - take an undertaking from the SI that the net profit margin for the adaptive sourcing is not over 15%
 - check for price referencing in other projects (if available)

3. Proposed Tender Conditions

3.1 Proposed Eligibility Criteria

To encourage participation, the Eligibility Criteria for the <CITY> CCTV Surveillance project is suggested as below:

1. The bidder (or all consortium partners) must be a registered company in India, registered under the Companies Act 1956. The bidder should be operating in India for the last five years as on 31/03/2014.
2. The bidder (prime bidder in case of consortium) should have overall revenue (gross income) of minimum **Rs. 250 Cr from IT/ITES/Telecom or Public Infrastructure Projects** in each of the last **3 financial years** as on 31/03/2014.
 - In case of consortium, each consortium partner should have over revenue (gross income) of minimum **Rs. 100 Cr from IT/ITES/Telecom or Public Infrastructure Projects** in each of the last **3 financial years** as on 31/03/2014.
 - In case of consortium, **maximum number of consortium partners allowed shall be three**. Consortium partners shall sign a consortium agreement format given in the RFP.
3. The bidder (or all consortium partners) should have a **positive net-worth** as on 31/03/2014.
4. The bidder (prime bidder in case of consortium) should have made cumulative net profit of minimum **Rs. 100 Crores** in the last **5 Financial Years** as on 31/03/2014.
5. The bidder (prime bidder in case of consortium) should have a valid ISO 9001:2008 or should an SEI CMM Level 3 (or above) certification.
6. The bidder (or all consortium partners) should submit valid documentary proof of Sales Tax/VAT registration number and the details of income tax registration (PAN).

Notes:

- a) In case of Central Govt./PSU in IT/ITES/Telecom business or Public Infrastructure Projects, criteria **2)** will be applicable and criteria **3)** and **4)** can be relaxed
- b) In case of consortium, a consortium partner shall only participate in one consortium bid unless the partner is an OEM or Network Service Provider and has been part of consortium only as OEM or Network Service Provider.

3.2 Proposed Payment Terms

- a) **10% of CAPEX** to be paid as mobilization advance against equivalent Bank Guarantee. (This BG, which will be **valid for 1 year**, would be apart from the Performance Bank Guarantee payable by the successful bidder). The Performance Bank Guarantee submitted by the SI should be valid for **6.5 years** from the date of issue.
- b) **35% of CAPEX** against Go Live of Phase I. It is required that at least 90% of the cameras from this phase should be live.
- c) **15% of CAPEX** against UAT for the Infrastructure for Command Center at CP Office & Viewing Center at <CITY> Municipal Council.
- d) **30% of the CAPEX** against the entire Project Go Live. It is required that at least 95% of the total cameras should be live. The BG (valid for 1 year) will be returned after successful Project Go-Live
- e) Remaining **20% of CAPEX and OPEX** payment in **20 equal installments for five years** after successful Go Live (Rs. ----- /- per quarter)

Note :

- The mobilization advance shall be recovered through payment of **b), c) and d)** in three installments at 30%, 40% and 30% of the total mobilization advance.
- CAPEX should not be over 50% of total project cost (i.e. CAPEX + OPEX for 5 years).
- If any Bidder quotes CAPEX as over 50% of total project cost, <CITY> shall cap CAPEX as 50% & shall pay 60% of total project cost in 20 equal installments for five years post Go Live.

TIMELY payments to be ensured: Interest of 12% per annum (calculated monthly) to be given by the <CITY> for payments delayed beyond 15 days of submission of the invoice (as per the due payment milestone).

3.3 Selection criteria of OEMs for Camera, VMS, Analytics and Switches

Following experience criteria are proposed to be followed to select OEMs for cameras, VMS, ANPR and other analytics

Component	Selection Criteria
Surveillance Cameras	<ul style="list-style-type: none"> • Minimum installation base of 50,000 IP based cameras across globe as on 31/03/2014 • Should have been operational in last 5 years for atleast 2 City Surveillance projects (globally) of minimum 1000 IP based cameras each <p style="text-align: center;">OR</p> <p>IMS World Report for Network Security Cameras or Report for Intelligent Cameras</p>
Video Management Software	<ul style="list-style-type: none"> • Minimum installation base of 50 projects across globe as on 31/03/2014 • Should have been operational in last 5 years for atleast 2 City Surveillance projects (globally) of minimum 1000 cameras each <p style="text-align: center;">OR</p> <p>IMS World Report for Video Management Software</p>
ANPR Cameras	<ul style="list-style-type: none"> • Minimum installation base of 5,000 cameras across globe as on 31/03/2014 • Should have been operational for atleast 2 City Surveillance projects (globally) in last 5 years for supporting minimum 100 ANPR cameras each <p style="text-align: center;">OR</p> <p>IMS World Report for ANPR Camera</p>
Thermal Cameras	<ul style="list-style-type: none"> • Minimum installation base of 1,000 cameras across globe as on 31/03/2014 • Should have been operational in last 5 years for atleast 2 City Surveillance projects (globally) for supporting minimum 10 Thermal cameras each <p style="text-align: center;">OR</p> <p>IMS World Report for Thermal Cameras</p>
Other Analytics	<ul style="list-style-type: none"> • Minimum installation base of 5,000 cameras across globe • Should have been operational in last 5 years for atleast 2 City Surveillance projects (globally) of minimum 500 cameras each <p style="text-align: center;">OR</p> <ul style="list-style-type: none"> • IMS World Report for Video Analytics
Edge Level Switch	<ul style="list-style-type: none"> • Minimum installation base of 5,000 switches across globe as on 31/03/2014 • Should have been operational in last 5 years for atleast 2 City Surveillance projects (globally) for supporting minimum 1000 cameras each

OEMs will certify the installation base and the project experience. This certificate shall be issued through the global Headquarters and attested by the Indian office. Tendering authority shall verify the claim of OEMs by using publicly available reports like IMS, in case there is any doubt of gross negligence. Decision of <CITY> shall be final and binding upon the Bidder and OEM

4. Service Level Agreements

Service Level Agreement (SLA) shall become the part of contract between <CITY> and the Successful Bidder. SLA defines the terms of the successful Bidder's responsibility in ensuring the timely delivery of the deliverables and the correctness of the same based on the agreed Performance Indicators as detailed in this section. The successful Bidder has to comply with Service Levels requirements to ensure adherence to project timelines, quality and availability of services.

The successful bidder has to supply software / automated tools to monitor all the SLAs mentioned below.

Note: Penalties shall not be levied on the successful Bidder in the following cases:

- There is a force majeure event effecting the SLA which is beyond the control of the successful Bidder
- The non-compliance to the SLA has been due to reasons beyond the control of the bidder. Theft cases by default would not be considered as "beyond the control of bidder". However, certain cases, based on circumstances & certain locations, police may agree to qualify as "beyond the control of bidder". Damages due to Road Accident / Mishap shall be considered as "beyond the control of bidder". However, Power shut down or deliberate damage to camera / Pole would not be considered as "beyond the control of bidder".

The purpose of this Service Level Agreement (hereinafter referred to as SLA) is to clearly define the levels of service which shall be provided by the System Integrator to <CITY> for the duration of this contract.

4.1 Definitions

For the purposes of this service level agreement, the definitions and terms are specified in the contract along with the following terms shall have the meanings set forth below :

- **"Uptime"** shall mean the time period for the specified services / components with the specified technical service standards are available to the user department. Uptime, in percentage, of any component (Non IT & IT) can be calculated as:
$$\text{Uptime} = \{1 - [(\text{Downtime}) / (\text{Total Time} - \text{Maintenance Time})]\} * 100$$
- **"Downtime"** shall mean the time period for which the specified services / components with specified technical and service standards are not available to the user department and excludes downtime owing to Force Majeure & Reasons beyond control of SI.
- **"Incident"** refers to any event / abnormalities in the functioning of the Services specified as part of the Scope of Work of the Systems Integrator that may lead to disruption in normal operations of the Surveillance System.
- **"Helpdesk Support"** shall mean the 24 x 7 x 365 centre which shall handle Fault reporting, Trouble Ticketing and related enquiries during this contract.

- **“Resolution Time”** shall mean the time taken (after the incident has been reported at the helpdesk), in resolving (diagnosing, troubleshooting and fixing) or escalating (to the second level or to respective Vendors, getting the confirmatory details about the same from the Vendor and conveying the same to the end user), the services related troubles during the first level escalation.

4.2 Measurement of SLA:

The SLA metrics provided specifies performance parameters as baseline performance, lower performance and breach. All SLA calculations will be done on quarterly basis. The SLA also specifies the penalties for lower performance and breach conditions.

Payment to the successful bidder is linked to the compliance with the SLA metrics. The matrix specifies three levels of performance, namely,

- The Agency will get 100% of the contracted value if the all baseline performance metrics are complied and the cumulative credit points are 100
- The Agency will get lesser payment in case of the lower performance. (For eg. If SLA point score is 80 then the vendor will get 20% penalized on the quarterly payment)
- If the performance of the Agency in respect of any parameter falls below the prescribed lower performance limit, debit points are imposed for the breach.

The credit (+) points earned during the quarter will be considered for computing penalty. The quarterly payment shall be made after deducting the penalty as mentioned above.

The aforementioned SLA parameters shall be measured per the individual SLA parameter requirements and measurement methods, through appropriate SLA Measurement tools to be provided by the SI and audited by <CITY> or its appointed Consultant for accuracy and reliability. The System Integrator would need to configure the SLA Measurement Tools such that all the parameters as defined under SLA matrix given at section 4.4 can be measured and appropriate reports be generated for monitoring the compliance.

<CITY> shall also have the right to conduct, either itself or through any other agency as it may deem fit, an audit / revision of the SLA parameters. The SLAs defined, shall be reviewed by <CITY> on an annual basis after consulting the SI, Project Management Consultants and other experts. All the changes would be made by <CITY> after consultation with the SI and might include some corrections to reduce undue relaxation in Service levels or some corrections to avoid unrealistic imposition of penalty, which are noticed after project has gone live.

Total penalty to be levied on the SI shall be capped at **15% of the total contract value**. However, <CITY> would have right to invoke termination of the contract in case the overall penalty equals 15% of total contract value. <CITY> would also have right to invoke termination of contract in case cumulative debit point (breach points) are above 30 in 2 consecutive quarters.

4.3 Planned Downtime

Any planned application / server downtime would not be included in the calculation of application / server availability. However, the Successful Bidder should take at least 10 days prior approval from <CITY> in writing for the planned outage, which should not be for more than 30 minutes, would be in lean period (non-movement period, like post mid-night) and limited to max. 4 outages in a year. In

case of planned outages at Data Centre level, services of other Data Centre services to be used to service the clients, while there would be no planned outages for Cameras.

4.4 Pre Implementation SLA

4.4.1 Timely delivery of the Scope of Work

Definition	Timely delivery of deliverables would comprise entire bill of material and the application systems, and as per successful UAT of the same.
Service Level Requirement	All the deliverables defined in the contract has to be submitted On-time on the date as mentioned in the contract with no delay.
Measurement of Service Level Parameter	To be measured in Number of weeks of delay from the timelines mentioned in the section “Project Timelines”
Penalty for non-achievement of SLA Requirement	Any delay in the delivery of the project deliverables would attract a penalty per week of 0.5% of the CAPEX of contract value per week for first 10 weeks and 0.75% per week for every subsequent week.

4.5 SLA Matrix for Post Implementation SLAs

Sr. No.	Performance Area	Baseline		Lower Performance		Breach	
		Metric	Points	Metric	Points	Metric	Points
1. Camera, Video Feed Uptime and Quality							
1	Uptime per camera (live feed available irrespective of bandwidth or last mile issues, which are in control of SI)	97%	15	>= 92% to <97%	10	< 92%	-15
2	At CP Office Command Centre : Live camera feed available from selected cameras for viewing) at any given time	97%	10	>= 92 % to <97%	4	< 92%	-12
3	At <CITY> Viewing Centre: Live camera feed available from various other viewing centers at any given time	96%	4	>= 92 % to <96%	2	< 92%	-3
4	Quality of Video feeds (Bad feeds due to Video Jitter, dim, blurred, unfocused, obstructed, non-aligned feeds*)	97%	10	>=94% to 97%	5	< 94%	-10
5	Average Frame rate maintained for viewing	88%	8	80.01 to 88 %	3	Less than 80%	-8
6	Average Frame rate maintained for recording	95%	5	90 to 95 %	3	Less than 90%	-7
7	Video stream Latency Latency refers to the average time required for transmission of video feed from one point to another	=< 40 ms	5	> 40 – 50 ms	3	> 50 ms	-7
2. Application Performance							
1	Overall application(s) availability at CP Office Command & Control Center	99%	4	>= 96.5 % to <99%	1.5	< 96 %	-4
2	Maximum time for User Login at Command Center	< 2 sec	1	2.01 – 4.0 secs	0.5	> 4 sec	-1
3	Maximum time for Surveillance Application(s) opening, this includes any application deployed	<5 secs	1	5.01 – 10.0 secs	0.75	> 10 secs	-1.5

Sr. No.	Performance Area	Baseline		Lower Performance		Breach	
		Metric	Points	Metric	Points	Metric	Points
	for the project at Command Center						
4	Menu Navigation, Window/Screen Opening, Screen Navigation (Average) at Command Center	<2 sec	1	2.01 – 5.0 secs	0.5	>5 secs	-1
6	Retrieval of video feeds at Command Center	<2 sec	2	2.01 – 6.0 secs	0.5	>6 secs	-1
6	Reports Generation Response Time (Alerts/MIS/Logs etc)	Simple query - < 5secs Medium complexity query - <30 secs High Complexity query - < 1min	1	Simple complexity Query = 5.01 – 10 secs Medium complexity query = 10.01 – 15 secs High Complexity query = < 15.1 sec – 1 min	0.5	Simple complexity Query = > 10 secs Medium complexity query = > 15 secs High Complexity query = > 1 min	-1
7	PTZ Lag time (movement at keyboard/joystick and actual moving indication through video feed viewed)	< 3 sec	1	3.01 – 5.0 secs	0.5	>5 secs	-1
8	Maximum time for successful camera settings modification (in online mode)	< 5 secs	0.5	5.01 – 10.0 secs	0.25	>10 secs	-0.5
3. Video Analytics Performance							
1	ANPR for Standard Roman Number plates (3 wheelers & above)	80%	1	79.99% to 70%	0.5	< 70 %	-1
2	ANPR for Non-Standard Roman Number plates (3 wheelers & above)	50%	0.5	49.99% to 40%	0.25	< 40 %	-0.5
3	ANPR for Standard Roman Number plates (2 wheelers)	70%	0.3	69.99% to 60%	0.15	< 60 %	-0.3

Sr. No.	Performance Area	Baseline		Lower Performance		Breach	
		Metric	Points	Metric	Points	Metric	Points
4	ANPR for Non-Standard Roman Number plates (2 wheelers)	50%	0.2	49.99% to 40%	0.1	< 40%	-0.2
5	Any other analytics (SLA to be defined in discussion with successful bidder)	80%	1	79.99% to 70%	0.5	< 70%	-1
4. End-User Equipment Uptime							
1	Monitoring workstations at Command Center & Viewing Centers	99 %	2	>= 97 % to <99%	1	< 97 %	-2
2	Video wall	99 %	2	>= 97 % to <99%	1	< 97 %	-2
3	IP Phones	97 %	1	>= 92 % to <97%	0.5	< 92 %	-1
4	LED Display screens	97 %	1	>= 90 % to <95 %	0.5	< 90 %	-1
5. Underlying IT Infrastructure Uptime/Availability at Data Center							
1	Production Servers Uptime	99.9%	4	>= 99.5 % to <99.9%	2	< 99.5%	-10
2	Storage System Uptime	99.9%	3	>= 99.5 % to <99.9%	1.5	< 99.5%	-10
4	Physical Security	Fully compliant	1	Lacunae shown in compliance procedures	0.5	For every Non-compliance instance	-2
5	CCTV surveillance of data centre area	99%	1	97%-99%	0.5	< 97%	-1
6. Security /Patch Services for IT Infrastructure							
1	Firewall and any other security appliance Uptime	100%	1	97 % to 99.99%	0.5	< 97%	-4
2	Security rules update within 2 hours of approved change management request	0 violations of service parameters	0.5	1 – 4 violations	0.25	> 4 violations	-0.5
3	Anti-virus, Anti-spyware, Anti-spam updates	0 violations of	0.5	1 – 4 violations	0.25	> 4 violations	-0.5

Sr. No.	Performance Area	Baseline		Lower Performance		Breach	
		Metric	Points	Metric	Points	Metric	Points
	within 24 hrs of request	service parameters					
4	Critical Patches – within 48 hours of patch release.	0 violations of service parameters	0.5	1 – 4 violations	0.25	> 4 violations	-0.5
5	Non Critical Patches – within 15 days of patch release.	Upto 1 violations of service parameters	0.5	2 – 5 violations	0.25	> 5 violations	-0.5
7. Technical Helpdesk, Trouble Ticketing, Issue Resolution							
1	Average Speed of Answer	<= 10 secs	1	10 to 14 secs	0.25	> 14 sec	-1
2	Average Call Lost Rate	0 – 0.5	1	0.5 – 2 %	0.5	> 2 %	-1
3	Resolution of Critical Issue (that impacts more than one production services & higher mgmt call)	60 minutes	2	60.01 to 120 min	1	> 120 min	-2
4	Resolution of Medium Level Issue (that does not impact production services)	120 minutes	1.5	120.01 to 240 min	0.75	> 240 min	-1
5	Resolution of low level Issue (upgrade, shifting and preventive maintenance (of non-production items))	2 days	1	>2 to 3 days	0.5	> 3 days	-1
8.Smart City Components (Uptime)							
1	Emergency Call Box System	97%	0.5	>= 92% to <97%	0.25	< 92%	-0.5
2	Public Address System	97%	0.5	>= 92% to <97%	0.25	< 92%	-0.5
3	Variable Messaging	97%	1	>= 92% to <97%	0.5	< 92%	-1
4	Connectivity to Sensors	97%	1	>= 92% to <97%	0.5	< 92%	-1
	Total Score		100		50		-120

4.5.1 Security Breach SLA

Note – This SLA for Security Breach is applicable over and above the SLAs mentioned in above table.

Definition	Security of the video feeds and the overall system is quite important and successful bidder shall be required to ensure no compromise is done on the same. Security Breach types considered for this SLA are– <ul style="list-style-type: none"> • Availability of Video feeds to any other user than those authorized by the Police Dept, and provided passwords • Availability of any report / data to any other user than those authorized by the Police Dept, and provided passwords • Successful hacking of any active component on the network by any standardized user • Or any other privacy rule is broken as per Govt of India guidelines
Service Level Requirement	Security compliance of the system should be 100%
Measurement of Service Level Parameter	Any reported security breach shall be logged into the SLA Management solution as a security breach
Penalty for non-achievement of SLA Requirement	For every security breach reported and proved, there shall be a penalty of INR 200,000/-.

4.5.2 Breach in supply of Technical Manpower

Note – This SLA for supply of Technical Manpower is applicable over and above the SLAs mentioned in the table 6.5.

Definition	Bidder is required to propose the CVs of the required technical manpower. It is vital that such manpower is available to Police Department as mentioned in the RFP and performs to the expected levels. The current SLA breach shall specify penalty amount for non-availability of these man-power.
Service Level Requirement	Availability of the required man-power should be 100%
Measurement of Service Level Parameter	Following instances would be considered as SLA non-compliances : <ul style="list-style-type: none"> • Replacement of a profile by the bidder (only one replacement per profile would be permitted per year) • Non-deployment of the profile for more than 1 month. <CITY> reserves the right to ask SI to replace the profile if the performance / commitment is not upto the mark <p>Note: Replacement due to reasons not in control of SI (like resignation of the resource, accident, etc.) would not be counted in the permissible 1 replacement.</p>
Penalty for non-achievement of SLA Requirement	For every SLA non-compliance reported and proved, there shall be a penalty of INR 100,000/-.

4.5.3 Explanation Notes for SLA Matrix

A) Camera Availability

Definition	“Camera Availability” means availability of the camera feed to the Command Centers / Police Stations.
Measurement of Service Level Parameter	$[(\text{Total average Uptime of all the Cameras in a quarter}) / (\text{Total Time in a quarter})] * 100$

10 Application Availability

Definition	Application availability refers to the total time when the Application is available to the users for performing all activities and tasks.
Measurement of Service Level Parameter	$[(\text{Total Uptime of the Application in a quarter}) / (\text{Total Time in a quarter})] * 100$

10 Quality of Feed

Definition	“Poor quality video feed” means blurred, jiggered, dim or unclear video. Camera Feed Error Resolution time is the time taken to improve the feed to satisfactory levels after it has been detected & logged by the Surveillance System / administrative officials. Logging of such calls would be through helpdesk system.
Service Level Requirement	The average availability of the quality of feed should be at 99.94%. This period is excluding the period of unavailability of camera. (i.e. the camera video quality would be judged for the period it’s available).
Measurement of Service Level Parameter	$[(\text{Total average Uptime of all the Cameras in a quarter} - \text{Total time logged for poor quality video feed}) / (\text{Total average Uptime of all the Cameras in a quarter})] * 100$

D) Issue Resolution SLA

Explanation	Issue Resolution SLA shall monitor the time taken to resolve a complaint / query after it has been reported by <CITY> to the successful bidder.
Service Level Requirement	<p>Different Issues / Queries shall be classified as in following three categories as defined above.</p> <p>Critical: Issue that impacts more than one production services / is raised by higher management / is impacting high importance areas</p> <p>Medium: Issue that doesn’t impact more than one production services but has a potential to impact or may get escalated to top management if not resolved quickly</p> <p>Low: Upgrades, shifting, preventive maintenance. Issues which don’t have impact on services.</p>

5. Responsibility Matrix

The roles of the stakeholders shall change over a period of time as the project will evolve from design to implementation and enter the operations phase. Stakeholders' responsibilities, illustrative organizational structure for the design & implementation phase, operational phase is given below:

Various Stakeholders identified for City Surveillance Project are as below:

<CITY> <CITY Full Name>.

PD <City> Police Department (Under the leadership of CP)

CON Project Management Consultant (<Name>)

SI Systems Integrator (Vendor to be selected for the Project's Implementation)

Responsibilities are shown using RACI Matrix which splits project tasks down to four participatory responsibility types that are then assigned to different Stakeholders in the project.

- R** (Responsible) - Those who do work to achieve the task
A (Approve) - The Stakeholder that ultimately approves the task
C (Consulted) - Those whose opinions are sought (2 way communication)
I (Informed) - Those who are kept up-to-date on progress (1 way communication)

Sr. No	Activity	<CITY>	PD	Con	SI
1.	Preparation of the Draft DPR	C	C	R	-
2.	Review of the Draft DPR	R	R	I	-
3.	Preparation of the Final DPR	C	C	R	-
4.	Approval to the DPR	R	C	I	-
5.	Preparation of the Draft RFP	C	C	R	-
6.	Review of the Draft RFP	R	C	I	-
7.	Preparation of the Final RFP	C	C	R	-
8.	Publishing of Tender & Bid Management	R	I	C	I
9.	Bid Evaluation	C	I	R	I
10.	Signing of the Contract	R	I	C	R
11.	Preparation of the Inception Report	A	A	C	R
12.	Finalise the List of Locations for Edge Devises in consultation with Police Department & Prepare the detailed plan for Camera Connectivity with Command Centers	A	R	C	R
13.	Prepare SRS documentation for the Video Surveillance Solution & the Video Analytics Solution, Finalize Reporting Formats / Base Rules	A	C	C	R
14.	Validate the Technical Design and Review SRS documentation	A	C	R	I
15.	Submission of the Partial Acceptance Testing & Final Acceptance Testing	C	C	C	R

Sr. No	Activity	<CITY>	PD	Con	SI
	Formats				
16.	Supply, Installation, Configuration and Commissioning of various equipments, components, systems	I	A	C	R
17.	Supply, Installation of other facilities such as Interiors, Electrical, UPS, DG Sets, Access Control System, BMS Fire detection and suppression System, etc	I	A	C	R
18.	Provisioning of Connectivity between Cameras, Control Center, Viewing Centers	I	A	C	R
19.	Preparing and implementing the Surveillance system information security policy, including policies on backup	I	I	C	R
20.	Preparation of the Policy Documents for Use & Operations of Surveillance System for the <CITY> CCTV System	A	A	C	R
21.	Guideline document / manual to standardize file formats, compression types, interfaces, to be used by various agencies concerned with video / photograph recording & storage.	A	A	C	R
22.	Guidelines for video data handling for submission of the video data to judiciary as legal evidence	A	A	C	R
23.	Guideline document / manual for setting up of Video Surveillance System by Private and Public institutions within the city	A	A	C	R
24.	Preparation of the Guideline Documents for allowing CCTV Feed of Public / Private Organisations to Police CCTV System	A	C	C	R
25.	Training and Capacity Building for the <City> Police Department for operation of the system	I	A	I	R
26.	Partial Acceptance Testing & Final Acceptance Testing of IT & Non-IT Equipments	A	C	R	R
27.	System Documents, User Documents as per ITIL (Information Technology Infrastructure Library) standards	I	A	C	R
28.	Review and Validation of the Documentation submitted by System Integrator	A	I	R	I
29.	Providing technically qualified manpower for maintenance of the entire system	I	A	C	R
30.	On-Site Facilities Management service	I	A	C	R
31.	Comprehensive Warranty Maintenance of the supplied equipment	I	A	C	R
32.	Provision of on-site spares	I	A	C	R
33.	Hand-over of the system at the end of contractual period along with all documentation required to operate and maintain the system	A	C	C	R
34.	Weekly Progress Reports	I	I	C	R
35.	Monthly Progress Reports	I	I	R	I
36.	Penalty for breach of SLA	R	I	C	I

6. Project Implementation Timelines

T : Date of the approval of RFP by <CITY>

#	Activity	Timeline
1.	Bid Process Management	T + 2 Months
2.	Contract Signing with the winning bidder	T + 3 Months
3.	Prepare SRS, SDD for the Entire Video Surveillance System	T + 6 Months
4.	Supply, Installation, Configuration of various equipments, components, systems at Data Center	T + 8 Months
5.	Installation of Cameras at <Area 1> <Area 2> <Area 3> .. (Phase I) & Operationalisation of the System on Pilot basis	T + 9 Months
6.	Training and Capacity Building for the Police Personnel	T + 9 Months
7.	Installation of Cameras at other locations (If necessary)	T + 11 Months
8.	Final Acceptance Testing (FAT) for Video Surveillance System, Data Center Equipments & Phase I Cameras	T + 12 Months
9.	Go Live for rest of the Locations	T + 13 Months
10.	Preparation and Submission of the following Manuals <ul style="list-style-type: none"> a. Systems Administration Manuals b. User Manuals c. Installation Manuals d. Operational Manuals e. Maintenance Manuals 	T + 13 Months
11.	Operations and Maintenance post Go-Live	5 Years

7. Estimated Project Cost

Estimation of the Project Cost for the scope mentioned in earlier Sections is given in the table below:

#	Line Item	Estimated Cost (in INR Crore)
Capital Expenditure		
1.	Edge Devices (Cameras, Poles, Labour, etc.)	XX
2.	Data Center Infrastructure (Servers, Storage, Application Software, etc.)	XX
3.	Infrastructure for Command Center at CP Office	XX
4.	Infrastructure for <CITY> Viewing Center	XX
5.	Surveillance System on Police Vans (3 Nos.)	XX
6.	Miscellaneous Costs (Training, Project Management, etc.)	XX
7.	Total Capital Expenditure	XX
Operational Expenditure for 5 Years		
8.	Bandwidth Cost	XX
9.	Operations & Maintenance for IT / Non-IT Infrastructure	XX
10.	Managed Hosting Cost	XX
11.	Technical & Operational Manpower Cost	XX
12.	Cost to Connect other institutions (Collaborative Monitoring)	XX
13.	Total Operation Expenditure for 5 Years	XX
14.	Provision for Adaptive Sourcing (One Crore per annum for 5 yrs)	XX
Total Estimated Project Expenditure		XXX

Notes / Assumptions:

- * It is recommended to discover the unit prices of cameras, poles, networking components, computing requirements, etc. towards the additional purchases <CITY> may do subsequent to the implementation of the current project. Such price discovery tables may be put in the RFP document.
- * Detail Bill of Material (BoM) for the different cost elements considered in the table above is given in **Section XX**

8. Annexures

8.1 List of the proposed Camera Locations & Camera distribution

Proposed distribution of cameras to about 167 locations, identified through a joint survey between Police Dept and PwC is given below.

Sr. No	Location Name	No. of Locations	Camera Type			Night Vision (IR Illuminators)	Total No. Cameras
			Fixed Camera		PTZ		
			ANPR	N-ANPR			
1	<XX Police station 1>	X1	X1	X1	X1	X1	XX1
2	<XX Police station 2>	X2	X2	X2	X2	X2	XX2
3	<XX Police station 3>	X3	X3	X3	X3	X3	XX3
4						
Total		XX	XX	XX	XX	XX	XXX

* Total No. Cameras = ANPR + N-ANPR + PTZ

List of the above proposed camera locations for each of the above police stations are given in subsequent tables:

8.1.1 XX Police Station 1

Sr. No	Location Name	Type of Location	Camera Type				Total No. Cameras
			Fixed Camera		PTZ	Night Vision	
			ANPR	Non-ANPR			
1	<Area 1>	Chowk / Entry Exit / Junction (etc.)	Xi	Xi	Xi	Xi	Xxi
2	<Area 2>	Chowk / Entry Exit / Junction (etc.)	Xii	Xii	Xii	Xii	XXii
Total Number of Cameras Required			X1	X1	X1	X1	XX1

The same to be done for each Police station identified as a part of the Coverage Area,

8.2 Proposed Benchmark Specifications for IT Components

Given below is an indicative benchmark to be considered.

8.2.1 Fixed Box cameras (High Definition)

#	Parameter	Minimum Specifications or better
1.	Video Compression	H.264 or better
2.	Video Resolution	1920 X 1080
3.	Frame rate	Min. 25 fps
4.	Image Sensor	1/3" Progressive Scan CCD / CMOS
5.	Lens Type	Varifocal, C/CS Mount, IR Correction
6.	Lens#	Auto IRIS 8 – 40 mm, F1.4
7.	Minimum Illumination	Colour: 0.5 lux, B/W: 0.1 lux (at 30 IRE)
8.	IR Cut Filter	Automatically Removable IR-cut filter
9.	Day/Night Mode	Colour, Mono, Auto
10.	S/N Ratio	≥ 50 dB
11.	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control
12.	Wide Dynamic Range	On/Off
13.	Audio	Audio Capture Capability
14.	Local storage	Memory card slot availability
15.	Protocol	HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP,
16.	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption
17.	Operating conditions	0 to 50°C
18.	Casing	NEMA 4X / IP-66 rated
19.	Certification	UL / CE / FCC / EN

At few places 2.8mm – 11 mm lens would be required depending upon the location of the camera and area to be covered. 2.8mm – 11mm lens requirement can be assumed as 20%. However the

actual type of lens required would depend upon the field-specific user requirement & percentages may vary to some extent.

- * All of the camera feeds would be used for Video Analytics while about 30 would be used for ANPR (Automatic Number Plate Recognition). Please note that the exact numbers may change depending upon the survey carried out by the successful bidder along with Police Dept. Bidders would be expected to provide necessary provisions in these cameras to support Analytics.

8.2.2 Pan, Tilt and Zoom cameras (PTZ)

#	Parameters	Minimum Specifications or better
1.	Video Compression	H.264 or better
2.	Video Resolution	1920 X 1080
3.	Frame rate	Min. 25 fps
4.	Image Sensor	1/3" OR 1/4" Progressive Scan CCD / CMOS
5.	Lens	Auto-focus, 4.7 – 84.6 mm (corresponding to 18x)
6.	Minimum Illumination	Colour: 0.5 lux, B/W: 0.1 lux (at 30 IRE)
7.	Day/Night Mode	Colour, Mono, Auto
8.	S/N Ratio	≥ 50dB
9.	PTZ	Pan: 360° endless/continuous, 0.2 to 300°/s (auto), 0.2 to 100°/s (Manual) Tilt: 90°, 0.2 to 100°/s (Auto), 0.2 to 40°/s (Manual) 18x optical zoom and 10x digital zoom 16 preset positions Auto-Tracking Pre-set tour
10.	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, Wide Dynamic Range
11.	Protocol	HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP,
12.	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption
13.	Operating conditions	0 to 50°C
14.	Casing	NEMA 4X / IP-66 rated
15.	Certification	UL / CE / FCC / EN

8.2.3 Thermal Cameras

#	Parameter	Minimum Specifications
1.	Video Compression	MJPEG, MPEG-4 / H.264 or better
2.	Resolution	320 X 240
3.	Thermal Sensor	320 X 240 pixels Focal Plan Array (FPA), uncooled Vanadium Oxide (Vox) / Amorphous Silicon Microbolometer
4.	Thermal Sensitivity	50 mK or better
5.	Pan and Tilt	Pan: 360°; 0.2° to 60°/s Tilt: 120° range; 10° to 50°/s Optical Zoom: 26x
6.	Lens	Minimum 80 mm
7.	Detection Range	Should detect an object of size 2.5m X 2.5m upto 4 km
8.	Minimum Illumination	Suitable for pitch-dark conditions (Zero Lux)
9.	Casing	NEMA 4X / IP-66 rated
10.	Operating conditions	-5° to 50°C
11.	Certification	UL / CE / FCC / EN

8.2.4 Infrared Illuminators

The infrared illuminators are to be used in conjunction with the Fix Box / PTZ cameras specified above to enhance the night vision.

#	Parameter	Minimum Specifications or better
1.	Range	Min. 100 mtrs
2.	Minimum Illumination	High sensitivity at Zero Lux
3.	Power	Automatic on/off operation
4.	Casing	NEMA 4X / IP-66 rated
5.	Operating conditions	-5° to 50°C
6.	Certification	UL / CE / FCC / EN

8.2.5 Workstation with Joystick Controller

#	Parameter	Minimum Specifications
1.	Processor	Latest generation 64 bit x86 Dual core CPU with 3.33GHz or more
2.	Memory	Minimum 8 GB Memory
3.	Graphics card	Graphics card with 2 GB video memory (non shared)
4.	HDD	500 GB SATA Hard drive @7200 rpm
5.	Media Drive	NO CD / DVD Drive
6.	Network interface	1000BaseT, Gigabit Ethernet (10/100/1G auto sensing)
7.	Audio	Line/Mic IN, Line-out/Spr Out (3.5 mm)
8.	USB ports	Minimum 6 USB ports (out of that 2 in front). These would be disabled for data transfer.
9.	Keyboard	104 keys minimum OEM keyboard
10.	Mouse	2 button optical scroll mouse (USB)
11.	PTZ joystick controller	<ul style="list-style-type: none"> • PTZ speed dome control for IP cameras • Minimum 10 programmable buttons • Multi-camera operations • Compatible with all the camera models offered in the solution • Compatible with VMS /Monitoring software offered
12.	Monitor	22" TFT LCD monitor, Minimum 1920 x1080 resolution, 5 ms or better response time, TCO o3 (or higher) certified <ul style="list-style-type: none"> • For command Control Centers : 3 LCD Monitors • For Viewing Centers : 1 LCD Monitor
13.	Operating System	64 bit pre-loaded OS with recovery disc
14.	Anti-virus feature	Advanced antivirus, antispysware, desktop firewall, intrusion prevention (comprising of a single, deployable agent) which can be managed by a central server. (Support, updates, patches and errata for the entire contract/ project period)

Note: There would be DRM Software/application installed on the workstations at the Command & Viewing Centres and mobile tablets/smartphones that would prevent unauthorized copying of video feeds and other sensitive data.

8.2.6 Laptop

#	Parameter	Minimum Specifications
1.	Processor	Latest generation 64 bit x86 Dual core CPU with 2.5 GHz or more
2.	Display	15" TFT, XGA Backlight LED display
3.	Memory	8GB DDR3 SDRAM with 1DIMM Slot free
4.	HDD	250 GB SATA HDD @ 7200 rpm
5.	Ports	1- Integrated Gigabit LAN ; 1- HDMI/ Display port, 1- VGA, 1- RJ-45, 1- headphone/ Microphone out; 3 – USB 2.0, Wireless LAN – 802.11b/g/n Wi-Fi Certified, Bluetooth 3.0, Built in web cam
6.	Battery backup	Minimum 6 lithium ion battery with a back up of min 3 hrs in standby mode
7.	Keyboard & Mouse	84 Keys Windows Compatible keyboard, Integrated Touch Pad
8.	OS	64 bit pre-loaded OS with recovery disc
9.	Antivirus	Advanced antivirus, antispymware, desktop firewall, intrusion prevention (comprising of a single, deployable agent) which can be managed by a central server. (Support, updates, patches and errata for the entire contract/ project period)
10.	Accessories	Laptop carrying case, Kensington lock

8.2.7 Fixed Dome Camera for Indoor Surveillance

#	Parameter	Minimum Specifications
1.	Video Compression	H.264 or better
2.	Video Resolution	1920 X 1080
3.	Frame rate	25 fps in all resolutions
4.	Image Sensor	1/4" / 1/3" Progressive Scan CMOS
5.	Lens Type	Varifocal, C/CS Mount, IR Correction
6.	Lens	Fixed IRIS 2.8-10mm, F1.7, 10x digital zoom
7.	Minimum Illumination	0.9 lux
8.	Image settings	Compression, colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, rotation

#	Parameter	Minimum Specifications
9.	Protocol	HTTP, HTTPS, FTP, SMTP, RTSP, RTP, TCP, UDP, RTCP, DHCP,
10.	Security	Password Protection, IP Address filtering, User Access Log
11.	Operating conditions	0 to 50°C
12.	Casing	Tamper Resistant casing for Indoor Environment

8.2.8 Application / Database/ Recording / Viewing / Other Servers

#	Parameter	Minimum Specifications
1.	Processor	Latest series/ generation of 64 bit x86/RISC/EPIC/CISC processors with Four (or higher) Cores. (Minimum 2 processors per each blade/server)
2.	RAM	Minimum 64 GB Memory
3.	Internal Storage	300 GB SAS / SATA (15k rpm) disk
4.	Network interface	Dual Integrated 10 Gigabit Ethernet ports (Minimum 2 Integrated 10 Gigabit Ethernet ports) Optional : Fiber channel adapter (if required)
5.	Power supply	Dual Redundant Power Supply
6.	RAID support	As per requirement/solution
7.	Operating System	Licensed version of 64 bit latest version of Linux/ Unix/Microsoft® Windows based Operating system, matching with the processor(s)
8.	Form Factor	Rack mountable/ Blade
9.	Virtualisation	Shall support Industry standard virtualization hypervisor like Hyper-V, VMware and Citrix.

8.2.9 LED Display

#	Parameter	Minimum Specifications
1.	Technology	LED lights for back lighting
2.	Screen Size	Min. 46"
3.	Resolution	Full high definition (1080p)

#	Parameter	Minimum Specifications
4.	Control	- RS232 control (with loop-through) - On Screen Display (OSD) - IR remote control
5.	Operations	24 x 7

8.2.10 Network Laser Color Printer

#	Parameter	Minimum Specifications
1.	Print Speed	Black : 16 ppm or above on A3, 24 ppm or above on A4 Color : 8 ppm or above on A3, 12 ppm or above on A4
2.	Resolution	600 X 600 DPI
3.	Memory	8 MB or more
4.	Paper Size	A3, A4, Legal, Letter, Executive, custom sizes
5.	Paper Capacity	250 sheets or above on standard input tray, 100 Sheet or above on Output Tray
6.	Duty Cycle	25,000 sheets or better per month
7.	OS Support	Linux, Windows 2000, Vista, 7, 8, 8.1
8.	Interface	Ethernet Interface

8.2.11 Online UPS

#	Parameter	Minimum Specifications
1.	Capacity	Adequate capacity to cover all above IT Components at respective location
2.	Output Wave Form	Pure Sine wave
3.	Input Power Factor at Full Load	>0.90
4.	Input	Three Phase 3 Wire for over 5 KVA
5.	Input Voltage Range	305-475VAC at Full Load
6.	Input Frequency	50Hz +/- 3 Hz

#	Parameter	Minimum Specifications
7.	Output Voltage	400V AC, Three Phase for over 5 KVA UPS
8.	Output Frequency	50Hz+/- 0.5% (Free running); +/- 3% (Sync. Mode)
9.	Inverter efficiency	>90%
10.	Over All AC-AC Efficiency	>85%
11.	UPS shutdown	UPS should shutdown with an alarm and indication on following conditions 1)Output over voltage 2)Output under voltage 3)Battery low 4)Inverter overload 5)Over temperature 6)Output short
12.	Battery Backup	30 minutes in full load
13.	Battery	VRLA (Valve Regulated Lead Acid) SMF (Sealed Maintenance Free) Battery
14.	Indicators & Metering	Indicators for AC Mains, Load on Battery, Fault, Load Level, Battery Low Warning, Inverter On, UPS on Bypass, Overload, etc Metering for Input Voltage, Output Voltage and frequency, battery voltage, output current etc
15.	Audio Alarm	Battery low, Mains Failure, Over temperature, Inverter overload, Fault etc.
16.	Cabinet	Rack / Tower type
17.	Operating Temp	0 to 50 degrees centigrade

8.2.12 Storage Solution

#	Parameter	Minimum Specifications
1.	Solution/Type	<ul style="list-style-type: none"> Bidder is expected to provide NAS / Scale-out NAS / SAN / Unified or equivalent storage solution (via IP based and/or FC based networking) meeting benchmark performance parameters specified in SLA Solution proposed should yield low cost per TB, while meeting the performance parameters
2.	Storage	<ul style="list-style-type: none"> Disks should be preferably of 3 TB minimum per disk To store video stream and other data as required, to meet the archival requirement for different type of video feeds Storage to have 100% capacity for all cameras of the project plus for the storage for video feeds received from Internet and through Collaborative Monitoring requirements specified in the RFP. The storage design must be based on the expected data volume from the project, including the expansion requirement of 5 years (System capable of scaling vertically (Controller) & horizontally (disk capacity))
3.	Hardware Platform	<ul style="list-style-type: none"> Rack mounted form-factor Modular design to support controllers and disk drives expansion
4.	Software Platform	Must include backup/archive application portfolio required
5.	Connectivity	<ul style="list-style-type: none"> The Storage System shall be capable of providing 1 GbE, 10 GbE, iSCSI, Fiber Channel IP, and 10 GB Fiber Channel over Ethernet connectivity.
6.	Controllers	<ul style="list-style-type: none"> Atleast 2 numbers of Controllers in active/active mode The controllers / Storage nodes should be upgradable seamlessly, without any disruptions / downtime to production workflow for performance, capacity enhancement and software / firmware upgrades.
7.	RAID support	<ul style="list-style-type: none"> Hardware based RAID support, should support various RAID levels (RAID 5 minimum)
8.	Redundancy and High Availability	<ul style="list-style-type: none"> The Storage System should be able to protect the data against single point of failure with respect to hard disks, connectivity interfaces, fans and power supplies
9.	Management software	<ul style="list-style-type: none"> All the necessary software (GUI based) to configure and manage the storage space, RAID configuration, logical drives allocation, snapshots etc.

		<ul style="list-style-type: none"> • A Single command console for entire storage system • Should also include storage performance monitoring and management software • Should provide the functionality of proactive monitoring of Disk drive and Storage system for all possible disk failures • Should be able to take “snapshots” of the stored data to another logical drive for backup purposes
10.	Data Protection	The storage array must have complete cache protection mechanism either by de-staging data to disk or providing complete cache data protection with battery backup for up to 4 hours
11.	Retrival time	<ul style="list-style-type: none"> • Retrieval time for any data stored should be max. 4 hours for critical data & 8 hours for other data. This would be taken into account for SLA calculation. (Critical data means any data needing urgent attention by the Judicial System or by Police Dept for investigation / terrorist treat perception). • Every incidence of this SLA not being met would be charged a penalty of Rs. 10,000/-.

Note:

- The video feeds will be **recorded, stored and viewed** at Full HD Video quality i.e. 1080p (1920 X 1080 resolution)
- Estimated storage requirement at Data Center is **XX TB**. However, Bidder is expected to carry out the storage requirement estimation and supply as per the solution proposed.
- Bidder should also quote for additional Storage as specified in the commercial format.

8.2.13 Database Licenses

- Bidder needs to provide Licensed RDBMS, enterprise/full version as required for the proposed Surveillance System and following all standard industry norms for performance, data security, authentication and database shall be exportable in to XML.

8.2.14 Backup Software

- The software shall be primarily used to backup the necessary and relevant video feeds from storage that are marked or flagged by the Police. The other data that would require backing up would include the various databases that shall be created for the surveillance system. Details of data that would be created are available in the table at section ‘Data Requirements’
- Scheduled unattended backup using policy-based management for all Server and OS platforms
- The software should support on-line backup and restore of various applications and Databases
- The backup software should be capable of having multiple back-up sessions simultaneously

- The backup software should support different types of backup such as Full back up, Incremental back up, Differential back up, Selective back up, Point in Time back up and Progressive Incremental back up and snapshots
- The backup software should support different types of user interface such as GUI, Web-based interface

8.2.15 Anti-virus Software

- Shall be able to scan through several types of compression formats.
- Must update itself over internet for virus definitions, program updates etc (periodically as well as in push-updates in case of outbreaks)
- Able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)
- Shall be able to scan only those file types which are potential virus carriers (based on true file type)
- Shall be able to scan for HTML, VBScript Viruses, malicious applets and ActiveX controls
- Shall provide Real-time product Performance Monitor and Built-in Debug and Diagnostic tools, and context- sensitive help.
- The solution must support multiple remote installations
- Shall provide for virus notification options for Virus Outbreak Alert and other configurable Conditional Notification.
- Should be capable of providing multiple layers of defense
- Shall have facility to clean, delete and quarantine the virus affected files.
- Should support scanning for ZIP, RAR compressed files, and TAR archive files
- Should support online update, where by most product updates and patches can be performed without bringing messaging server off-line.
- Should use multiple scan engines during the scanning process
- Should support in-memory scanning so as to minimize Disk IO.
- Should support Multi-threaded scanning
- Should support scanning of nested compressed files
- Should support heuristic scanning to allow rule-based detection of unknown viruses
- Updates to the scan engines should be automated and should not require manual intervention
- All binaries from the vendor that are downloaded and distributed must be signed and the signature verified during runtime for enhanced security
- Updates should be capable of being rolled back in case required
- File filtering should be supported by the proposed solution; file filtering should be based on true file type.
- Should support various types of reporting formats such as CSV, HTML and text files
- Shall scan at least HTTP, FTP traffic (sending & receiving) in real time and protect against viruses, worms & Trojan horse attacks and other malicious code.

- Shall be able to automatically push any updates, patches, fixes to all client machines to ensure up-to-date antivirus protection for all IT devices and systems.

8.2.16 Enterprise Management System

The Enterprise Management System (EMS) is an important requirement of this Project. Various key components of the EMS are –

- SLA & Contract management System
- Network Monitoring System
- Server Monitoring System
- Helpdesk System

The solution should provide a unified web based console which consolidates all aspects of role based access under a single console

- **SLA & Contract management System**

The SLA & Contract Management solution should enable <CITY> / Police Department to capture all the System based SLAs defined in this RFP and then calculate quarterly (or for any duration) penalty automatically. Measuring service performance requires incorporation of a wide variety of data sources of the Surveillance project. The SLA solution should support the collection data from various sources in order to calculate Uptime / Performance / Security SLAs. Various features required in this component to EMS are –

- It must be a centralized monitoring solution for all IT assets (including servers, network equipments etc)
- The solution must have integrated dashboard providing view of non performing components / issues with related to service on any active components
- The solution must follow governance, compliance and content validations to improve standardization of service level contracts
- Application should be pre-configured so as to allow the users to generate timely reports on the SLAs on various parameters.
- The solution must support Service Level Agreements & Lifecycle Management including Version Control, Status Control, Effectively and audit Trail to ensure accountability for the project.
- The solution must have the ability to define and calculate key performance indicators from an End to End Business Service delivery perspective related to Surveillance Project under discussion.
- The solution should support requirements of the auditors requiring technical audit of the whole system.
- The solution must have an integrated dashboard, view of Contract Parties & current SLA delivery levels and view of Services & current SLA performance
- The solution should support SLA Alerts escalation and approval process.
- Solution should support effective root cause analysis, support capabilities for investigating the root causes of failed service levels and must make it possible to find the underlying events that cause the service level contract to fail.
- Accept Data from a variety of formats, provide pre-configured connectors and adapters, Ability to define Adapters to data source in a visual manner without coding.
- Support for Defining and Calculating service Credit and Penalty based on clauses in SLAs.

Reporting

- Ability to generate reports on penalty and credit due, to check on non-compliance of SLAs for the surveillance project
- Monetary penalties to be levied for non-compliance of SLA, thus the system must provide Service Level Performance Report over time, contract, service and more.
- The solution should provide historical and concurrent service level reports for the surveillance project in order to ensure accountability of the service provider's performance
- Automatic Report creation, execution and Scheduling, must support variety of export formats including Microsoft Word, Adobe PDF etc.
- The solution must support Templates for report generation, Report Filtering and Consolidation and Context sensitive Drill-down on specific report data to drive standardization and governance of the surveillance project
- The solution must support security for drill-down capabilities in dashboard reports ensuring visibility for only relevant personnel of the surveillance project
- Support real-time reports (like at-a-glance status) as well as historical analysis reports (like Trend, TopN, Capacity planning reports etc.)
 - Resource utilization exceeding or below customer-defined limits
 - Resource utilization exceeding or below predefined threshold limits

An indicative List of SLAs that needs to be measured centrally by SLA contract management system are given in the RFP document. These SLAs must be represented using appropriate customizable reports to ensure overall service delivery.

• Network Management System

Solution should provide fault & performance management of the entire datacenter infrastructure and should monitor IP\SNMP enabled devices like Routers, Switches, Cameras, etc. Proposed Network Management shall integrate with SLA & Contract Management system in order to supply KPI metrics like availability, utilization in order to measure central SLA's and calculate penalties. Following are key functionalities that are required which will help measuring SLA's as well as assist administrators to monitor network faults & performance degradations in order to reduce downtimes, increase availability and take proactive actions to remediate & restore network services.

- The proposed solution must automatically discover manageable elements connected to the infrastructure and map the connectivity between them. Solution should provide centralized monitoring console displaying network topology map from central location to Zonal / Police Station Level.
- Proposed solution should provide customizable reporting interface to create custom reports for collected data.
- The system must use advanced root-cause analysis techniques and policy-based condition correlation technology for comprehensive analysis of infrastructure faults.
- The system should be able to clearly identify configuration changes as root cause of network problems and administrators should receive an alert in case of any change made on routers spread across surveillance project.

- Network Performance management system should provide predictive performance monitoring and should be able to auto-calculate resource utilization baselines for the entire managed systems and networks and allow user to set corresponding upper and lower threshold limits based on baseline data instead of setting up manual thresholds for monitored devices.
- The system must support the ability to create reports that allow the surveillance administrators to search all IP traffic over a specified historical period, for a variety of conditions for critical router interfaces
- The proposed system must be capable of providing the following detailed analysis across surveillance domain:
 - Top utilized links (inbound and outbound) based on utilization of link
 - Top protocols by volume based on utilization of link
 - Top host by volume based on utilization of link
- **Server Performance Monitoring System**
 - The proposed tool should integrate with network performance management system and support operating system monitoring for various platforms supplied as part of the Surveillance Project.
 - The proposed tool must provide information about availability and performance for target server nodes.
 - The proposed tool should be able to monitor various operating system parameters such as processors, memory, files, processes, file systems, etc. where applicable.
 - The solution should provide a unified web based console which consolidates all aspects of privileged user management under a single console.
 - Proposed Network Management shall integrate with SLA & Contract Management system in order to supply KPI metrics like availability, utilization, performance in order to measure central SLA's and calculate penalties.
- **Centralized Helpdesk System**
 - The proposed helpdesk solution must provide flexibility of logging, viewing, updating and closing incident manually via web interface for issues related to surveillance project.
 - Helpdesk system should provide incident management, problem management templates along with helpdesk SLA system for tracking SLA's pertaining to incident resolution time for priority / non-priority incidents.
 - The proposed helpdesk solution must have a built-in workflow engine to define escalations or tasks to be carried out after issues or change order are logged pertaining to surveillance project.
 - Centralized HelpDesk System should have integration with Network / Server Monitoring Systems so that the HelpDesk Operators can to associate alarms with Service Desk tickets to help surveillance operators that for what particular alarms corresponding helpdesk tickets got logged.
 - Surveillance Network admin should be able to manually create tickets through Fault Management GUI.
 - System should also automatically create tickets based on alarm type

- System should provide a link to directly launch a Service Desk view of a particular ticket created by alarm from within the Network Operation console.

8.2.17 Directory services

- Should be compliant with LDAP v3
- Support for integrated LDAP compliant directory services to record information for users and system resources
- Should provide integrated authentication mechanism across operating system, messaging services
- Should provide directory services for ease of management and administration/replication
- Should provide support for Group policies and software restriction policies
- Should support security features, such as Kerberos, Smart Cards, Public Key Infrastructure (PKI), etc
- Should provide support for X.500 naming standards
- Should support Kerberos for logon and authentication
- Should support that password reset capabilities for a given group or groups of users can be delegated to any nominated user
- Should support that user account creation/deletion rights within a group or groups can be delegated to any nominated user
- Should support directory services integrated DNS zones for ease of management and administration/replication.

8.2.18 Edge Level Switch (at Camera locations)

#	Parameter	Minimum Specifications
1.	Type	Managed Outdoor Industrial grade switch
2.	Total Ports	<ul style="list-style-type: none"> • Minimum 4 10/100 TX PoE • May require higher port density at some locations, depending upon site conditions • May require fiber ports at some locations, depending upon site conditions/distances.
3.	PoE Standard	IEEE 802.3af or better
4.	Protocols	<ul style="list-style-type: none"> • Support 802.1Q VLAN • DHCP support • SNMP Management
5.	Access Control	<ul style="list-style-type: none"> • Support port security • Support 802.1x (Port based network access control). • Support for MAC filtering.
6.	PoE Power per port	Sufficient to operate the CCTV cameras connected

7.	Rating	IP 31 or equivalent Industrial Grade Rating
8.	Operating Temperature	0 – 50 degrees C or better

8.2.19 Data Center / Aggregation Switches (Manageable)

(To be used for Data centre LAN Switch and as base specification for Core switch for any command center / viewing center)

#	Parameter	Minimum Specifications
1.	Ports	<ul style="list-style-type: none"> • 24 or 48 (as per requirements) 10/100/1000 Base-TX Ethernet ports and extra 2 nos of Base-SX/LX ports • All ports can auto-negotiate between 10Mbps/ 100Mbps/ 1000Mbps, half-duplex or full duplex and flow control for half-duplex ports.
2.	Switch type	Layer 3
3.	MAC	Support 8K MAC address.
4.	Backplane	56 Gbps or more Switching fabric capacity (as per network configuration to meet performance requirements)
5.	Forwarding rate	Packet Forwarding Rate should be 70.0 Mpps or better
6.	Port Features	Must support Port Mirroring, Port Trunking and 802.3ad LACP Link Aggregation port trunks
7.	Flow Control	Support IEEE 802.3x flow control for full-duplex mode ports.
8.	Protocols	<ul style="list-style-type: none"> • Support 802.1D, 802.1S, 802.1w, Rate limiting • Support 802.1Q VLAN encapsulation, IGMP v1, v2 and v3 snooping • 802.1p Priority Queues, port mirroring, DiffServ • Support based on 802.1p priority bits with at least 8 queues • DHCP support & DHCP snooping/relay/optional 82/ server support • Shaped Round Robin (SRR) or WRR scheduling support. • Support for Strict priority queuing & Sflow • Support for IPV6 ready features with dual stack • Support upto 255 VLANs and upto 4K VLAN IDs
9.	Access Control	<ul style="list-style-type: none"> • Support port security • Support 802.1x (Port based network access control). • Support for MAC filtering. • Should support TACACS+ and RADIUS authentication
10.	VLAN	<ul style="list-style-type: none"> • Support 802.1Q Tagged VLAN and port based VLANs and Private VLAN

		<ul style="list-style-type: none"> • The switch must support dynamic VLAN Registration or equivalent • Dynamic Trunking protocol or equivalent
11.	Protocol and Traffic	<ul style="list-style-type: none"> • Network Time Protocol or equivalent Simple Network Time Protocol support • Switch should support traffic segmentation • Traffic classification should be based on user-definable application types: TOS, DSCP, Port based, TCP/UDP port number
12.	Management	<ul style="list-style-type: none"> • Switch needs to have RS-232 console port for management via a console terminal or PC • Must have support SNMP v1,v2 and v3 • Should support 4 groups of RMON • Should have accessibility using Telnet, SSH, Console access, easier software upgrade through network using TFTP etc. Configuration management through CLI, GUI based software utility and using web interface

8.2.20 KVM Module

#	Item	Minimum Specifications
1.	KVM Requirement	Keyboard, Video Display Unit and Mouse Unit (KVM) for the IT Infrastructure Management at Data Center
2.	Form Factor	19” rack mountable
3.	Ports	minimum 8 ports
4.	Server Connections	USB or KVM over IP.
5.	Auto-Scan	It should be capable to auto scan servers
6.	Rack Access	It should support local user port for rack access
7.	SNMP	The KVM switch should be SNMP enabled. It should be operable from remote locations
8.	OS Support	It should support multiple operating system
9.	Power Supply	It should have dual power with failover and built-in surge protection
10.	Multi-User support	It should support multi-user access and collaboration

8.2.21 First Level Router (Edge Level)

#	Item	Minimum Specifications
1.	Ports	The router should have 2 LAN & 2 WAN slots loaded with minimum one 2-port sync/async Serial Interface card and cable for connectivity to Internet / other offices. The sync / async port should support data

		rates of up-to 128Kbps in sync mode
2.	Speed	As per requirement
3.	Protocol Support	Must have support for TCP/IP, PPP, X.25, Frame relay and HDLC Must support VPN Must have support for integration of data and voice services Routing protocols of RIP, OSPF, and BGP.
4.	SNMP	Must be SNMP manageable

8.2.22 Second Level (Aggregation) Level Routers

#	Item	Minimum Specifications
1.	Ports	The router should have 2 LAN & 5 WAN slots loaded with minimum one 4- port sync/async Serial Interface card or 4- port channelized E1 card with cable for connectivity to Internet / other offices. The sync / async port should support data rates of up-to 128Kbps in sync mode
2.	Speed	As per requirement
3.	Protocol Support	Must have support for TCP/IP, PPP, X.25, Frame relay and HDLC Must support VPN Must have support for integration of data and voice services Routing protocols of RIP, OSPF, and BGP. Support IPV4 & IPV6
4.	Manageability	Must be SNMP manageable
5.	Multi-Services	Should deliver multiple IP services over a flexible combination of interfaces
6.	Scalable	The router should be scalable. For each slot multiple modules should be available
7.	Traffic control	Traffic Control and Filtering features for flexible user control policies
8.	Bandwidth	Bandwidth on demand for cost effective connection performance enhancement
9.	Remote Access	Remote access features
10.	Redundancy	Redundancy in terms of Power supply
11.	Security features	<ul style="list-style-type: none"> • MD5 encryption for routing protocol • NAT

		<ul style="list-style-type: none"> • URL based Filtering • RADIUS Authentication • Management Access policy • IPSec / Encryption
12.	QOS Features	<ul style="list-style-type: none"> • RSVP • Priority Queuing • Policy based routing • Traffic shaping • Time-based QoS Policy • Bandwidth Reservation / Committed Information Rate

8.2.23 Central (Core) Router

#	Item	Minimum Specifications
1.	Multi-Services	Should deliver multiple IP services over a flexible combination of interfaces
2.	Ports	As per overall network architecture proposed by the bidder, the router should be populated with required number of LAN/WAN ports/modules, with cable for connectivity to other network elements.
3.	Speed	As per requirement, to cater to entire bandwidth requirement of the project.
4.	Interface modules	Must support upto 10G interfaces. Must have capability to interface with variety interfaces.
5.	Protocol Support	<p>Must have support for TCP/IP, PPP, X.25, Frame relay and HDLC</p> <p>Must support VPN</p> <p>Must have support for integration of data and voice services</p> <p>Routing protocols of RIP, OSPF, and BGP.</p> <p>Support IPV4 & IPV6</p>
6.	Manageability	Must be SNMP manageable
7.	Scalable	<ul style="list-style-type: none"> • The router should be scalable. For each slot multiple modules should be available. • The chassis offered must have free slots to meet the scalability requirement of expansion of the project in the future.
8.	Traffic control	Traffic Control and Filtering features for flexible user control policies

9.	Bandwidth	Bandwidth on demand for cost effective connection performance enhancement
10.	Remote Access	Remote access features
11.	Redundancy	<ul style="list-style-type: none"> Redundancy in terms of Power supply(s). Power supply should be able to support fully loaded chassis All interface modules, power supplies should be hot-swappable
12.	Security features	<ul style="list-style-type: none"> MD5 encryption for routing protocol NAT URL based Filtering RADIUS Authentication Management Access policy IPSec / Encryption L2TP
13.	QOS Features	<ul style="list-style-type: none"> RSVP Priority Queuing Policy based routing Traffic shaping Time-based QoS Policy Bandwidth Reservation / Committed Information Rate

8.2.24 Firewall

#	Item	Minimum Specifications
1.	Physical attributes	<ul style="list-style-type: none"> Should be mountable on 19" Rack Modular Chassis Internal redundant power supply
2.	Interfaces	<ul style="list-style-type: none"> 4 x GE, upgradable to 8 GE Console Port 1 number
3.	Performance and Availability	<ul style="list-style-type: none"> Encrypted throughput: minimum 800 Mbps Concurrent connections: up to 100,000 Simultaneous VPN tunnels: 2000
4.	Routing Protocols	<ul style="list-style-type: none"> Static Routes RIPv1, RIPv2

		<ul style="list-style-type: none"> • OSPF
5.	Protocols	<ul style="list-style-type: none"> • TCP/IP, PPTP • RTP, L2TP • IPSec, GRE, DES/3DES/AES • PPPoE, EAP-TLS, RTP • FTP, HTTP, HTTPS • SNMP, SMTP • DHCP, DNS • Support for Ipv6
6.	Other support	<ul style="list-style-type: none"> • 802.1Q, NAT, PAT, IP Multicast support, Remote Access VPN, Time based Access control lists, URL Filtering, support VLAN, Radius/ TACACS
7.	QoS	<ul style="list-style-type: none"> • QoS features like traffic prioritization, differentiated services, committed access rate. Should support for QoS features for defining the QoS policies.
8.	Management	<ul style="list-style-type: none"> • Console, Telnet, SSHv2, Browser based configuration • SNMPv1, SNMPv2

8.2.25 Intrusion Prevention System

#	Item	Required Specifications
1.	Performance	<p>Should have an aggregate throughput of no less than 200Mbps</p> <p>Total Simultaneous Sessions – 500,000</p>
2.	Features	<p>IPS should have Dual Power Supply</p> <p>IPS system should be transparent to network, not default gateway to Network</p> <p>IPS system should have Separate interface for secure management</p> <p>IPS system should be able to protect Multi Segment in the network, should be able to protect 4 segments.</p>
3.	Real Time Protection	<ul style="list-style-type: none"> • Web Protection • Mail Server Protection • Cross Site Scripting • SNMP Vulnerability • Worms and Viruses • Brute Force Protection • SQL Injection • Backdoor and Trojans

4.	Stateful Operation	<ul style="list-style-type: none"> • TCP Reassembly • IP Defragmentation • Bi-directional Inspection • Forensic Data Collection • Access Lists
5.	Signature Detection	Should have provision for Real Time Updates of Signatures, IPS Should support Automatic signature synchronization from database server on web Device should have capability to define User Defined Signatures
6.	Block attacks in real time	<ul style="list-style-type: none"> • Drop Attack Packets • Reset Connections • Packet Logging • Action per Attack
7.	Alerts	<ul style="list-style-type: none"> • Alerting SNMP • Log File • Syslog • E-mail
8.	Management	<ul style="list-style-type: none"> • SNMP V1, 2C, 3 • HTTP, HTTPS • SSH, Telnet, Console
9.	Security Maintenance	<ul style="list-style-type: none"> • IPS Should support 24/7 Security Update Service • IPS Should support Real Time signature update • IPS Should support Provision to add static own attack signatures • System should show real-time and History reports of Bandwidth usage per policy • IPS should have provision for external bypass Switch

8.2.26 Server Rack at Data Centers (Caged)

- 19” 42U racks mounted on the floor
- Floor Standing Server Rack – 42U with Heavy Duty Extruded Aluminum Frame for rigidity. Top cover with FHU provision. Top & Bottom cover with cable entry gland plates. Heavy Duty Top and Bottom frame of MS. Two pairs of 19” mounting angles with ‘U’ marking. Depth support channels – 3 pairs. With an overall weight carrying Capacity of 500Kgs.
- Front and Back doors should be perforated with atleast 63% or higher perforations.
- All racks should have mounting hardware 2 Packs, Blanking Panel.
- Stationery Shelf (Minimum 2 sets per Rack)
- All racks must be lockable on all sides with unique key for each rack
- Racks should have Rear Cable Management channels, Roof and base cable access
- Wire managers
 - Two vertical and four horizontal

- Power distribution Unit (2 per rack)
 - Power Distribution Unit – Vertically Mounted, 32AMPs with 25 Power Outputs. (20 Power outs of IEC 320 C13 Sockets & 5 Power outs of 5/13Amp Sockets), Electronically controlled circuits for Surge & Spike protection, LED readout for the total current being drawn from the channel, 32AMPS MCB, 3KVAC isolated input to Ground & Output to Ground
- Door
 - The racks must have steel (solid / grill / mesh) front / rear doors and side panels. Racks should NOT have glass doors / panels.
 - Both the front and rear doors should be designed with quick release hinges allowing for quick and easy detachment without the use of tools.
- Fan trays
 - Fan 90CFM 230V AC, 4” dia (4 Nos. per Rack)
 - Fan Housing Unit 4 Fan Position (Top Mounted) (1 no. per Rack) – Monitored – Thermostat based – The Fans should switch on based on the Temperature within the rack. The temperature setting should be factory settable. This unit should also include – humidity & temperature sensor
- Metal
 - Aluminum extruded profile
- Side panel
 - Detachable side panels (set of 2 per Rack)
- Width
 - 19” equipment mounting, extra width is recommended for managing voluminous cables

8.2.27 DG Set

#	Item	Specifications
1	General Specifications	<ul style="list-style-type: none"> • Auto Starting DG Set mounted on a common base frame with AVM (Anti-Vibration) pads, residential silencer with exhaust piping, complete conforming to ISO 8528 specifications and CPCB certified for emissions. • KVA rating as per the requirement
2	Engine	Radiator cooled, multi cylinder, 1500 RPM diesel engine, with electronic/manual governor and electrical starting arrangement complete with battery, conforming to BS 5514/ ISO 3046/ IS 10002
3	Fuel	High Speed Diesel (HSD)
5	Alternator	Self exciting, self regulating type alternator rated at 0.8 PF or better, 415 Volts, 3 Phase, 4 wires, 50 cycles/sec, 1500 RPM, conforming to IS 4722/ BS 5000, Windings of 100% Copper, class H insulation, Protection as per IP 23.

6	AMF (Auto Main Failure) Panel	<p>AMF Panel fitted inside the enclosure, with the following: It should have the following meters/indicators</p> <ul style="list-style-type: none"> • Incoming and outgoing voltage • Current in all phases • Frequency • KVA and power factor • Time indication for hours/minutes of operation • Fuel Level in fuel tank, low fuel indication • Emergency Stop button • Auto/Manual/Test selector switch • MCCB/Circuit breaker for short-circuit and overload protection • Control Fuses • Earth Terminal • Any other switch, instrument, relay etc essential for Automatic functioning of DG set with AMF panel
7	Acoustic Enclosure	<ul style="list-style-type: none"> • The DG set shall be provided with acoustic enclosure / canopy to reduce the sound level and to house the entire DG set (Engine & Alternator set) assembly outside (open-air). • The enclosure must be weather resistant powder coated, with insulation designed to meet latest MOEF/CPCB norms for DG sets, capable to withstand the climate. The enclosure must have ventilation system, doors for easy access for maintenance, secure locking arrangement, complete and
8	Fuel Tank Capacity	<p>It should be sufficient and suitable for containing fuel for 12 hours continuous operation, Complete with level indicator, fuel inlet and outlet, air vent, drain plug, inlet arrangement for direct filling and set of fuel hoses for inlet and return.</p>

8.3 Functional Requirements for the Proposed Surveillance System

Functional Requirement of the overall Surveillance System can be categorized into following components:

- Information to be Captured by Edge Devices
- Information to be Managed at the Command Center
- Information to be made available to different Police Personnel
- Operational Requirements
- Storage / Recording Requirements
- Other General Requirements

8.3.1 Information to be captured by Edge Devices

Cameras being the core of the entire Surveillance system, it is important that their selection is carefully done to ensure suitability & accuracy of the information captured on the field and is rugged, durable & compact. These cameras need to work on 24 X 7 basis and transmit quality video feeds to the centralized data center and would capture the video feeds at **15 FPS** for majority of the time and at **8 FPS** for the lean period. However, Police Department may take the regular review of the requirements for video resolution, FPS and may change these numbers to suit certain specific requirements (for example, there could be a situation when certain cameras are required to be viewed at higher FPS for specific period. It is estimated that not more than 0.5% of the cameras would be required to be viewed at higher FPS at a given point of time).

The complete tracking of a 'wanted' vehicle identified or flagged by Police should be possible on the GIS map.

Benchmark camera specifications are given in **Section 7.2**. It is recommended to clearly identify in SLAs that cameras need to transmit quality video feed (appropriately focused, clear, unblurred, jitter free, properly lit, unobstructed, etc.). Packet loss to be less than 0.5%.

8.3.2 Information to be analyzed at the Command Centers

The proposed Video Management System shall provide a complete end-to-end solution for security surveillance application. The control center shall allow an operator to view live / recorded video from any camera on the IP Network. The combination of control center and the IP Network would create a virtual matrix, which would allow switching of video streams around the system.

As informed in the tender, not all the cameras would be simultaneously viewed at Command Control Centers. Command Center shall from time to time take decisions on utilization of Alerts / Exceptions / Triggers generated by cameras, and specify the client machines where these would get populated automatically.

Police personnel shall have following access to the video feeds of the cameras of their jurisdiction:

- Viewing rights to all the live Camera Feeds
- Viewing rights to the stored feeds
- Access to view Alerts / Exceptions / Triggers raised
- Trail Report on specific person / object / vehicle for a specific period / location

- Personalized Dashboard (depending upon grade of police officer)
- Accessibility to advanced analytics on recorded footages
- Provide search of recorded video. Advanced search should be possible based on various filters like alarm / event, area, camera, etc.

8.3.3 Role Based Access to the Entire System

Various users should have access to the system using single sign on and should be role based. Different roles which could be defined (to be finalized at the stage if SRS) could be Administrator, Supervisor, Officer, Operator, etc. Apart from role based access, the system should also be able to define access based on location. Other minimum features required in the Role Based authentication Systems are as follows:

- The Management Module should be able to capture basic details (including mobile number & email id) of the Police Personnel & other personnel requiring Viewing / Administration rights to the system. There should be interface to change these details, after proper authentication.
- Rights to different modules / Sub-Modules / Functionalities should be role based and proper log report should be maintained by the system for such access.
- Biometric standardized coupled with login name & password should be enabled to ensure that only the concerned personnel are able to login into the system.
- Surveillance System should have capability to map the cameras to the Police Personnel from different Police Stations. There should be interface to change these mappings too.
- For PTZ cameras, there should be provision to specify hierarchy of operators / officers for control of the cameras from various locations.

8.3.4 Storage / Recording Requirements

It is proposed that the storage solution is modular enough to ensure compliance to the changes in storage / recording policy, to be evolved upon initial deployment of the system. As decided in the meetings of <CITY> & Police Officials following storage requirements are proposed for the project:

- **The storage solution proposed is that the video feeds would be available for 30 days.** After 30 days, the video feeds would be overwritten unless it is flagged or marked by the Police for investigation or any other purpose. The video feeds of all relevant cameras capturing the incident in question would be stored until the Police deem it good for deletion.
- For incidents that are flagged by the Police or any court order, the video of the relevant portion from all relevant cameras should be stored/archived separately for investigation purposes and a committee at Police Department can decide when this video feed can be deleted.
- Regardless of the above, the image of the License plate extracted by ANPR software, along with the timestamp and location of the image capture will stored for a period of 3 months
- Full audit trail of reports to be maintained for 90 days.
- Please refer **Section 8.2** for specifications for Storage solution.
- Retrieval time for any data stored should be max. 4 hours for critical data & 8 hours for other data.
- The Recording Servers / System, once configured, shall run independently of the Video Management system and continue to operate in the event that the Management system is off-line.

- The system shall support the use of separate networks, VLANs or switches for connecting the cameras to the recording servers to provide physical network separation from the clients and facilitate the use of static IP addresses for the devices.
- The system shall support H.264 or better, MPEG-4 and MJPEG compression formats for all analog cameras connected to encoders and all IP cameras connected to the system.
- The system shall record the native frame rate and resolution supplied by the camera or as configured by the operator from the System Administration Server.
- The system should not limit amount of storage to be allocated for each connected device.
- The on-line archiving capability shall be transparent and allow Clients to browse and archive recordings without the need to restore the archive video to a local hard drive for access.
- The system shall allow for the frame rate, bit rate and resolution of each camera to be configured independently for recording. The system shall allow the user to configure groups of cameras with the same frame rate, bit rate and resolution for efficient set-up of multiple cameras simultaneously.
- The system shall support Archiving or the automatic transfer of recordings from a camera's default database to another location on a time-programmable basis without the need for user action or initiation of the archiving process. Archiving shall allow the duration of the camera's recordings to exceed the camera's default database capacity. Archives shall be located on either the recording server or on a connected network drive. If the storage area on a network drive becomes unavailable for recording the system should have the ability to trigger actions such as the automatic sending of email alerts to necessary personnel.
- Bandwidth optimization
 - The Recording Server / System shall offer different codec (H.264, MJPEG, MPEG-4, etc) and frame rate (CIF, 4CIF, QCIF) options for managing the bandwidth utilization for live viewing on the Client systems.
 - From the Client systems, the user shall have the option of having video images continually streamed or only updated on motion to conserve bandwidth between the Client systems and the Recording Server.
- The Recording Server / System shall support Camera (analogue and IP cameras) devices from various manufacturers.
- The Recording Server / System shall support the PTZ protocols of the supported devices listed by the camera OEMs.
- The system shall support full two-way audio between Client systems and remote devices.
- Failover Support
 - The system shall support automatic failover for Recording Servers. This functionality shall be accomplished by Failover Server as a standby unit that shall take over in the event that one of a group of designated Recording Servers fails. Recordings shall be synchronized back to the original Recording Server once it is back online.
 - The system shall support multiple Failover Servers for a group of Recording Servers.
- SNMP Support
 - The system shall support Simple Network Management Protocol (SNMP) in order for third-party software systems to monitor and configure the system.
 - The system shall act as an SNMP agent which can generate an SNMP trap as a result of rule activation in addition to other existing rule actions.

8.3.5 Other General Requirements

Management / Integration functionality

- The Surveillance System shall offer centralized management of all devices, servers and users.
- The Surveillance System should not have any limit on the number of cameras to be connected for Surveillance, Monitoring and recording. Any increase in the no. of cameras should be possible by augmentation of Hardware components.
- The Surveillance System shall support distributed viewing of any camera in the system using Video walls or big screen displays.
- The Surveillance System shall support alarm management. The alarm management shall allow for the continuous monitoring of the operational status and event-triggered alarms from system servers, cameras and other external devices.
- It should be possible to integrate the Surveillance System with 3rd-party software, to enable the users to develop customized applications for enhancing the use of video surveillance solution. For e.g., integrating alarm management to initiate SMS, E-Mail, VoIP call etc.
- The Management system shall store the overall network elements configuration in central database, either on the management server computer or on a separate DB Server on the network.
- System should be able to be integrated with Event Management / Incident Management System, if implemented by <CITY> / <City> Corporation in future.

System Administration functionality

- The System Administration Server shall provide a feature-rich administration client for system configuration and day-to-day administration of the system.
- The System Administration Server shall support different logs related to the Management Server.
 - The System Log
 - The Audit Log
 - The Alert Log
 - The Event Log
- Rules

The system shall support the use of rules to determine when specific actions occur. Rules shall define what actions shall be carried out under specific conditions. The system shall support rule initiated actions such as:

- Start and stop recording
- Set non-default live frame rate
- Set non-default recording rate
- Start and stop PTZ patrolling
- Send notifications via email
- Pop-up video on designated Client Monitor recipients

Client system

The Client system shall provide remote users with rich functionality and features as described below.

- Viewing live video from cameras on the surveillance system
- Browsing recordings from storage systems
- Creating and switching between multiple of views.
- Viewing video from selected cameras in greater magnification and/or higher quality in a designated hotspot.
- Controlling PTZ cameras.
- Using digital zoom on live as well as recorded video.
- Using sound notifications for attracting attention to detected motion or events.
- Getting quick overview of sequences with detected motion.
- Getting quick overviews of detected alerts or events.
- Quickly searching selected areas of video recording for motion (also known as Smart Search).

Remote Web Client

- 3 The web-based remote client shall offer live view of up to 16 cameras, including PTZ control and event / output activation. The Playback function shall give the user concurrent playback of multiple recorded videos with date, alert sequence or time searching.
 - a) User Authentication – The Remote Client shall support logon using the user name and password credentials.

Matrix Monitor

- a) Matrix Monitor – The Matrix Monitor feature shall allow distributed viewing of multiple cameras on the system on any monitor.
- b) The Matrix Monitor feature shall access the H.264/MJPEG/MPEG4 stream from the connected camera directly and not sourced through the recording server.

Alarm Management Module

- a) The alarm management module shall allow for continuous monitoring of the operational status and event-triggered alarms from various system servers, cameras and other devices. The alarm management module shall provide a real-time overview of alarm status or technical problems while allowing for immediate visual verification and troubleshooting.
- b) The alarm management module shall provide interface and navigational tools through the client including;
 - i. Graphical overview of the operational status and alarms from servers, network cameras and external devices including motion detectors and access control systems.
 - ii. Intuitive navigation using a map-based, hierarchical structure with hyperlinks to other maps, servers and devices or through a tree-view format.
- c) The module shall include flexible access rights and allow each user to be assigned several roles where each shall define access rights to cameras.
- d) Basic VMS should be capable to accept third party generated events / triggers

Other Miscellaneous Requirements

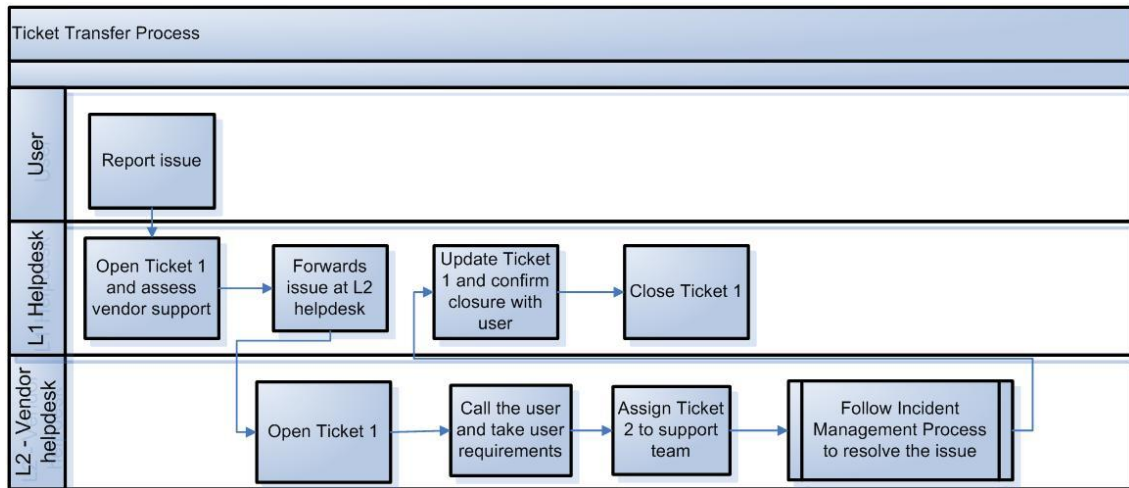
- System should have a facility to create CDs or other storage media for submission to Judiciary, which can be treated evidence for legal matters. Such storage media creation should be tamper proof and SI to provide appropriate technology so that integrity and quality of evidence is maintained as per requirements of the judiciary. Bidder is required to specify any additional hardware / software required for this purpose & the same can be listed in Miscellaneous section of the commercial bid. SI will also prepare the guideline document to be followed by the Police Personnel for the retrieval of Video / images from the CCTV System so as to maintain integrity of the evidence. Such a guideline document should include methods of retrieval of data, check-list to be followed and flowchart of the entire process to be followed.
- All the systems proposed and operationalisation of Video Management System should comply with requirements of IT Acts.
- Bidder shall be required to provide a standardized Mobile Application to integrate smart phones and tablets for 2-way communication with the Video Management System in a secure manner. <CITY> / <City> Police Dept may provide such tablets / smart phones to the designated Police Personnel. It will be responsibility of SI to configure such tablets / Smartphone with the Surveillance System and ensure that all the necessary access is given to these mobile users so that uploading of video / pictures to the surveillance system is possible
- There would be the provision for Third party audit periodically, paid by <CITY> separately

8.3.6 HelpDesk Management

It is envisaged that the centralized helpdesk, functioning as proposed below, would be managed by the Systems Integrator and shall serve following objectives:

- Act as the Point of Contact for the users of Surveillance System
- Own an Incident throughout its Lifecycle
- Communicate effectively with Police / Home Dept Officers and IT support teams.
- Maintain high user satisfaction levels
- Maintain the SLA statistics & submit quarterly report to Police / Home Department

A general process flow for the helpdesk management is depicted in the flow-chart given as follows. Systems Integrator shall prepare a detailed HelpDesk Policy in consultation with the <CITY> & it's Consultant prior to the Go Live date.



System Integrator shall deploy a State-of-Art Enterprise Management System to handle the complexity of Operations & SLA Management defined in the RFP. Benchmark specifications for the Enterprise Management System is given in **Section 7.2**.

8.4 Proposed Benchmark Specifications for Non-IT Components

Proposed specifications for various Non-IT components, required at Command Center and the Edge Level, are given in this section. It is essential that Fire Proof material be used as far as possible and Certification from Fire Department be taken for Command Centers before Go Live.

1. Civil and Architectural work

a. False Ceiling (at Command Center)

- Metal false ceiling with powder coated 0.5mm thick hot dipped galvanised steel tiles 595 x 595 mm with regular edge (10mm) suitable for 25mm grid supported on suitable powder coated galvanised steel grid as per manufacturer specification. The same shall be inclusive of cut outs for lighting, AC grills, Fire detectors, nozzles, etc.
- 12 mm thick fire line Gypsum false ceiling and lighting troughs 300 mm as per design including 100 mm high cornices as lighting pelmets on G.I. frame work, in G.I. vertical supports at every 450mm c/c and horizontal runners at every 900mm c/c self taping metal screws to proper line and level. The same shall be inclusive of making holes and required framing for fixing electrical fixtures, A.C. grills etc. GI vertical supports to be anchored to slab by means of anchor fasteners.

b. Furniture and Fixture

- Workstation size of min. 18” depth made with 1.5mm thick laminate of standard make over 18mm thick commercial board complete with wooden beading including cutting holes & fixing of cable manager etc complete with French polish. Edges shall be factory post-formed. The desk shall have the necessary drawers, keyboard trays, cabinets etc. along with sliding / opening as per approved design with quality drawer slides, hinges, locks etc.
- Storage unit with 18 mm thick MDF board along with 1.5 mm approved laminate colour outside and 2 coat of enamel paint inside the storage of size 1’6”x1’6”x2’4”. The same should be provided with all the required accessories including the handle, lock, sliding channel and necessary hardware, etc. complete with French polish
- Cabin table of min. Depth 2’ made with 1.5mm thick laminate of standard make over 19mm thick commercial board complete with wooden beading including cutting holes & fixing of cable manager etc complete with French polish.
- 6” high laminated strip using 1.5mm thick laminate over 10mm thick commercial board on all vertical surface in the entire server & ancillary areas including low height partition, brick wall, partition wall, cladding etc complete with French polish in all respect.
- Enclosure for gas cylinder of Shutters and Partitions along with wooden support and 18 mm thick MDF board along with 1.5 mm approved laminate colour outside and 2 coat of enamel paint inside the shutter. The same should be provided with all the required accessories including the handle, lock, loaded hinges, tower bolt and necessary hardware etc. complete with French polish.

c. Partitions (wherever required as per approved drawing)

- Full height partition wall of 125 mm thick fireline gyp-board partition using 12.5 mm thick double fireline gyp-board on both sides with GI steel metal vertical stud frame of size 75 mm fixed in the floor and ceiling channels of 75 mm wide to provide a strong partition. Glass wool insulation inside shall be provided as required. Fixing is by self tapping screw with vertical studs being at 610 mm intervals. The same should be inclusive of making cutouts for switch board, sockets, grill etc. It shall also include preparing the surface smoothly and all as per manufacture's specification etc. finally finishing with one coat of approved brand of fire resistant coating.
- With glazing including the framework of 4" x 2" powder coated aluminium section complete (in areas like partition between server room & other auxiliary areas).
- Fire Rated Wire Glass minimum 6 mm thick for all glazing in the partition wall complete. (External windows not included in this).
- All doors should be minimum 1200 mm (4 ft) wide.

d. Painting

- Fire retardant paint of pre-approved make and shade to give an even shade over a primer coat as per manufacturers' recommendations after applying painting putty to level and plumb and finishing with 2 coats of fire retardant paint. Base coating shall be as per manufacturer's recommendation for coverage of paint.
- For all vertical Plain surface.
- For fireline gyp-board ceiling.
- POP punning over cement plaster in perfect line and level with thickness of 10 – 12 mm including making good chases, grooves, edge banding, scaffolding pockets etc.
- Fire retardant coating on all vertical surfaces, furniture etc. as per manufacturer's specification.

2. PVC Conduit

- The conduits for all systems shall be high impact rigid PVC heavy-duty type and shall comply with I.E.E regulations for standardized conduit 1.6 mm thick as per IS 9537/1983.
- All sections of conduit and relevant boxes shall be properly cleaned and glued using appropriate epoxy resin glue and the proper connecting pieces, like conduit fittings such as Mild Steel and should be so installed that they can remain accessible for existing cable or the installing of the additional cables.
- No conduit less than 20mm external diameter shall be used. Conduit runs shall be so arranged that the cables connected to separate main circuits shall be enclosed in separate conduits, and that all lead and return wire of each circuit shall be run to the same circuit.
- All conduits shall be smooth in bore, true in size and all ends where conduits are cut shall be carefully made true and all sharp edges trimmed. All joints between lengths of conduit or between conduit and fittings boxes shall be pushed firmly together and glued properly.
- Cables shall not be drawn into conduits until the conduit system is erected, firmly fixed and cleaned out. Not more than two right angle bends or the equivalent shall be permitted between draw or junction boxes. Bending radius shall comply with I.E.E regulations for PVC pipes.

- Conduit concealed in the ceiling slab shall run parallel to walls and beams and conduit concealed in the walls shall run vertical or horizontal.
- The chase in the wall required in the recessed conduit system shall be neatly made and shall be of angle dimensions to permit the conduit to be fixed in the manner desired. Conduit in chase shall be held by steel hooks of approved design of 60cm center the chases shall be filled up neatly after erection of conduit and brought to the original finish of the wall with cement concrete mixture 1:3:6 using 6mm thick stone aggregate and course sand.

3. Wiring

- PVC insulated copper conductor cable shall be used for sub circuit runs from the distribution boards to the points and shall be pulled into conduits. They shall be stranded copper conductors with thermoplastic insulation of 650 / 1100 volts grade. Color code for wiring shall be followed.
- Looping system of wiring shall be used, wires shall not be jointed. No reduction of strands permitted at terminations.
- Wherever wiring is run through trunking or raceways, the wires emerging from individual distributions shall be bunched together with cable straps at required regular intervals. Identification ferrules indicating the circuit and D.B. number shall be used for sub main, sub circuit wiring the ferrules shall be provided at both end of each sub main and sub-circuit.
- Where, single phase circuits are supplied from a three phase and a neutral distribution board, no conduit shall contain wiring fed from more than one phase in any one room in the premises, where all or part of the electrical load consists of lights, fans and/or other single phase current consuming devices, all shall be connected to the same phase of the supply.
- Circuits fed from distinct sources of supply or from different distribution boards or M.C.B.s shall not be bunched in one conduit. In large areas and other situations where the load is divided between two or three phases, no two single-phase switches connected to different phases shall be mounted within two meters of each other.
- All splicing shall be done by means of terminal blocks or connectors and no twisting connection between conductors shall be allowed.
- Metal clad sockets shall be of die cast non-corroding zinc alloy and deeply recessed contact tubes. Visible scraping type earth terminal shall be provided. Socket shall have push on protective cap.
- All power sockets shall be piano type with associated switch of same capacity. Switch and socket shall be enclosed in a M. S. Sheet steel enclosure with the operating knob projecting. Entire assembly shall be suitable for wall mounting with Bakelite be connected on the live wire and neutrals of each circuit shall be continuous everywhere having no fuse or switch installed in the line excepting at the main panels and boards. Each power plug shall be connected to each separate and individual circuit unless specified otherwise. The power wiring shall be kept separate and distinct from lighting and fan wiring. Switch and socket for light and power shall be separate units and not combined one.
- Balancing of circuits in three phases installed shall be arranged before installation is taken up. Unless otherwise specified not more than ten light points shall be grouped on one circuit and the load per circuit shall not exceed 1000 watts.

4. Earthing

All electrical components are to be earthen by connecting two earth tapes from the frame of the component ring and will be connected via several earth electrodes. The cable arm will be earthen through the cable glands. Earthing shall be in conformity with provision of rules 32, 61, 62, 67 & 68 of Indian Electricity rules 1956 and as per IS-3043. The entire applicable IT infrastructure in the Control Rooms shall be earthed.

- Earthing should be done for the entire power system and provisioning should be there to earth UPS systems, Power distribution units, AC units etc. so as to avoid a ground differential. State shall provide the necessary space required to prepare the earthing pits.
- All metallic objects on the premises that are likely to be energized by electric currents should be effectively grounded.
- The connection to the earth or the electrode system should have sufficient low resistance in the range of 0 to 25 ohm to ensure prompt operation of respective protective devices in event of a ground fault, to provide the required safety from an electric shock to personnel & protect the equipment from voltage gradients which are likely to damage the equipment.
- Recommended levels for equipment grounding conductors should have very low impedance level less than 0.25 ohm.
- The Earth resistance shall be automatically measured on an online basis at a pre-configured interval and corrective action should be initiated based on the observation. The automatic Earthing measurements should be available on the UPS panel itself in the UPS room.
- There should be enough space between data and power cabling and there should not be any cross wiring of the two, in order to avoid any interference, or corruption of data.
- The earth connections shall be properly made .A small copper loop to bridge the top cover of the transformer and the tank shall be provided to avoid earth fault current passing through fastened bolts, when there is a lightning surge, high voltage surge or failure of bushings.
- A complete copper mesh earthing grid needs to be installed for the server farm area, every rack need to be connected to this earthing grid. A separate earthing pit need to be in place for this copper mesh.
- Provide separate Earthing pits for Servers, UPS & Generators as per the standards.

5. Cable Work

- Cable ducts should be of such dimension that the cables laid in it do not touch one another. If found necessary the cable shall be fixed with clamps on the walls of the duct. Cables shall be laid on the walls/on the trays as required using suitable clamping/ fixing arrangement as required. Cables shall be neatly arranged on the trays in such manner that a criss-crossing is avoided and final take off to switch gear is easily facilitated.
- All cables will be identified close to their termination point by cable number as per circuit schedule. Cable numbers will be punched on 2mm thick standard strips and securely fastened to the. In case of control cables all covers shall be identified by their wire numbers by means of PVC ferrules. For trip circuit identification additional red ferrules are to be used only in the switch gear / control panels, cables shall be supported so as to

prevent appreciable sagging. In general distance between supports shall not be greater than 600mm for horizontal run and 750mm for vertical run.

- Each section of the rising mains shall be provided with suitable wall straps so that same the can be mounted on the wall.
- Whenever the rising mains pass through the floor they shall be provided with a built-in fire proof barrier so that this barrier restricts the spread of fire through the rising mains from one section to the other adjacent section.
- Neoprene rubber gaskets shall be provided between the covers and channel to satisfy the operating conditions imposed by temperature weathering, durability etc.
- Necessary earthing arrangement shall be made alongside the rising mains enclosure by Mean of a GI strip of adequate size bolted to each section and shall be earthed at both ends. The rising mains enclosure shall be bolted type.
- The space between data and power cabling should be as per standards and there should not be any criss-cross wiring of the two, in order to avoid any interference, or corruption of data.

1. Comfort Air Conditioning at Command Centers

- Cooling Capacity as per the requirements at each of the control rooms
- Compressor – Hermetically Sealed Scroll Type
- Refrigerant – R 22 Type
- Power Supply – Three Phase, 380-415 V, 50 Hz
- Air Flow Rate – minimum 19 cu m / min
- Noise Level - < 50 dB
- Operation – Remote Control

2. Fire Detection and Control Mechanism

Fire can have disastrous consequences and affect operations of a Control Room. The early-detection of fire for effective functioning of the Control Room.

System Description

- The Fire alarm system shall be an automatic 1 to n (e.g. 8) zone single loop addressable fire detection and alarm system, utilizing conventional detection and alarm sounders.
- Detection shall be by means of automatic heat and smoke detectors located throughout the Control Room (ceiling, false floor and other appropriate areas where fire can take place) with break glass units on escape routes and exits.

Control and indicating component

- The control panel shall be a microprocessor based single loop addressable unit, designed and manufactured to the requirements of EN54 Part 2 for the control and indicating component and EN54 Part 4 for the internal power supply.
- All controls of the system shall be via the control panel only.
- The system status shall be made available via panel mounted LEDs and a backlit 8 line x 40-character alphanumeric liquid crystal display.

- All system controls and programming will be accessed via an alphanumeric keypad. The control panel will incorporate form fill menu driven fields for data entry and retrieval.
- The system will include a detection verification feature. The user shall have the option to action a time response to a fire condition. This time shall be programmable up to 10 minutes to allow for investigation of the fire condition before activating alarm outputs. The operation of a manual call point shall override any verify command.

Manual Controls

- Start sounders
- Silence sounders
- Reset system
- Cancel fault buzzer
- Display test
- Delay sounder operation
- Verify fire condition
- Disable loop

Smoke detectors – Smoke detectors shall be of the optical or ionization type. Devices shall be compatible with the CIE conforming to the requirements of EN54 Part 7 and be LPCB approved. The detectors shall have twin LEDs to indicate the device has operated and shall fit a common addressable base.

- Heat detectors
- Heat detectors shall be of the fixed temperature (58° C) or rate of temperature rise type with a fixed temperature operating point.
- Devices shall be compatible with the CIE conforming to the requirements of EN54 Part 5 and be LPCB approved.
- The detectors shall have a single LED to indicate the device has operated and shall fit a common addressable base.

Addressable detector bases

- All bases shall be compatible with the type of detector heads fitted and the control system component used. Each base shall comprise all necessary electronics including a short circuit isolator.
- The device shall be automatically addressed by the CIE on power up of the loop without the need of the insertion of a pre-programmed EPROM or setting of DIL switches.
- Detector bases shall fit onto an industry standard conduit box.

Audible Alarms – Electronic sounders shall be colored red with adjustable sound outputs and at least 3 sound signals. The sounders should be suitable for operation with a 24V DC supply providing a sound output of at least 100dBA at 1 meter and 75 dBA min, for a bed head or sounder base type device. The sounder frequency shall be in the range of 500Hz to 1000Hz.

Commissioning

- The fire detection and alarm system will be programmable and configurable via an alpha numeric keypad on the control panel.

3. High Sensitivity Smoke Detection System

General – The HSSD system shall provide an early warning of fire in its incipient stage, analyze the risk and provide alarm and actions appropriate to the risk. The system shall include, but not be limited to, a Display Control Panel, Detector Assembly and the properly designed sampling pipe network. The system component shall be supplied by the manufacturer or by its authorized distributor.

Regulatory Requirements

- National Electrical Code (NEC)
- Factory Mutual
- Local Authority having Jurisdiction

4. Access Control System

The Access Control System shall be deployed with the objective of allowing entry and exit to and from the premises to authorized personnel only. The system deployed shall be based on Biometric Technology. An access control system consisting of a central PC, intelligent controllers, power supplies and all associated accessories is required to make a fully operational on line access control system. Access control shall be provided for entry / exit doors. These doors shall be provided with electric locks, and shall operate on fail-safe principle. The lock shall remain unlocked in the event of a fire alarm or in the event of a power failure. The fire alarm supplier shall make potential free contacts available for releasing the locks in a fire condition especially for staircase and main doors. Entry to the restricted area shall be by showing a proximity card near the reader and exit shall be using a push button installed in the secure area. The system shall monitor the status of the doors through magnetic reed contacts. The system should be designed and implemented to provide following functionality:

- Controlled Entries to defined access points
- Controlled exits from defined access points
- Controlled entries and exits for visitors
- Configurable system for user defined access policy for each access point
- Record, report and archive each and every activity (permission granted and / or rejected) for each access point.
- User defined reporting and log formats
- Fail safe operation in case of no-power condition and abnormal condition such as fire, theft, intrusion, loss of access control, etc.
- Day, Date, Time and duration based access rights should be user configurable for each access point and for each user.
- One user can have different policy / access rights for different access points.

5. Rodent Repellant

The entry of Rodents and other unwanted pests shall be controlled using non-chemical, non-toxic devices. Ultrasonic pest repellents shall be provided in the false flooring and ceiling to repel the pests without killing them. However periodic pest control using Chemical spray can be done once in 3 months as a contingency measure to effectively fight the pest menace.




- Configuration : Master console with necessary transducer


- Operating Frequency : Above 20 KHz (Variable)
- Sound Output : 50 dB to 110 dB (at 1 meter)
- Power output : 800 mW per transducer
- Power consumption : 15 W approximately
- Power Supply : 230 V AC 50 Hz
- Mounting : Wall / Table Mounting

6. Standardised Signs for CCTV Camera Locations

It is necessary that the CCTV Camera locations put some standardized signs informing the public of the existence of CCTV cameras. This will bring about the transparency on installation of CCTV cameras and no one would be able to later complaint for breach of privacy. Following tables give draft specifications for the signages to be put at the camera locations.

#	Item	Specifications
1	Size	Board Width = 8" / 12" (For type A and B) Board Width = 12" / 18" / 24" (For type C and D)
2	Plate Material	Corrosion resistant Aluminum Alloy as per IRC 67:2001 (Code of Practice for Road signs)
3	Plate Thickness	Minimum 1.5 mm
4	Retro-Reflective sheeting for sign-plate	Weather-resistant, having colour fastness
5	Other Specifications	As per IRC 67:2001 (Code of Practice for Road signs)
6	Mounting	Can be mounted on wall or pole (appropriate mounting brackets to be provided)
7	Design	As per following signage diagrams

Type	Sign Design	Remarks
A		<p>To be used at 80% of the Places</p>
B		<p>To be used at select places where text can be read. Text should be in Marathi at majority of places</p>
C		<p>This may be used on a select few places in the city, usually on the main pole of the location where multiple cameras are installed. Text should be in Marathi in majority of places.</p>

D		<p>This is an alternative to type C.</p>
---	---	--

7. Camera Poles

#	Parameter	Minimum Specifications
1.	Pole type	Hot Dip Galvanized after Fabrication with Silver coating of 86 micron as per IS:2629; Fabrication in accordance with IS-2713 (1980)
2.	Height	<ul style="list-style-type: none"> • 5 Meter OR higher, As-per-requirements for different types of cameras & Site conditions. • Min. height of camera above the ground should be 10 feet
3.	Pole Diameter	Min. 10 cm diameter pole (bidder to choose larger diameter for higher height)
4.	Bottom base plate	Minimum base plate of size 30 x 30 x 15 cms
5.	Mounting facilities	To mount CCTV cameras, Switch, etc.
6.	Foundation	<p>Casting of Civil Foundation with foundation bolts, to ensure vibration free erection (basic aim is to ensure that video feed quality is not impacted due to winds in different climatic conditions). Expected foundation depth of min. 100cms.</p> <p>Please refer to Earthing standards mentioned in Section 8.4 (pt. 4)</p>
7.	Protection	Lightning arrestors with proper grounding
8.	Sign-Board and	A sign board describing words such as “This area under

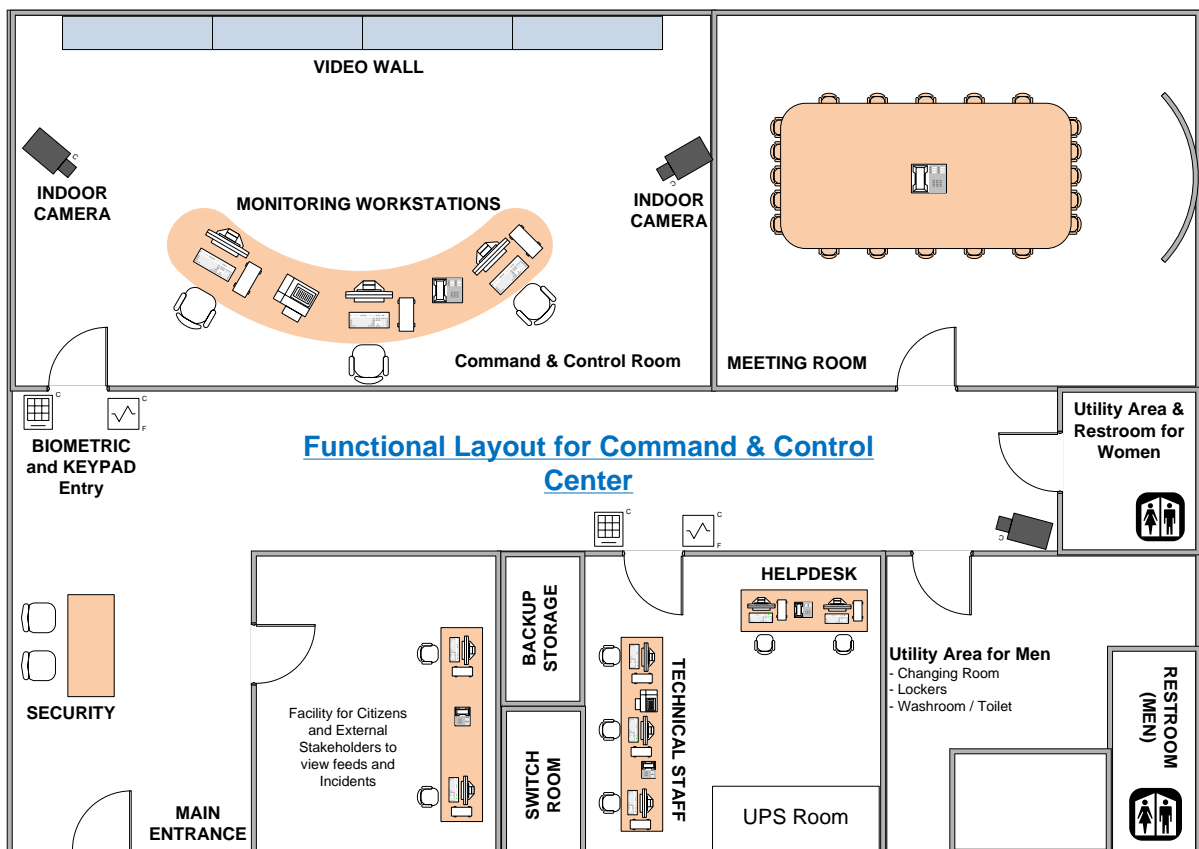
#	Parameter	Minimum Specifications
	Number-Plate	surveillance” and with serial number of the pole.

8.5 Functional Layout for Command & Control Center

Based on the discussions held with <CITY>, it is proposed to have following provisions within the command and control center:

- Command and Control Center room with video wall and workstations for viewing man-power
- Meeting room or Crisis room with overhead projector.
- Separate room/ cabin to allow external stakeholders (like citizens) to watch the video footages, if need arises.
- Changing and locker room (for Gents and Ladies)
- Sitting space for helpdesk support from the vendor & space for technical staff to carry out repairs/ troubleshooting

A broad level representation of above requirements is specified in the suggestive layout below. Please note that based on the actual physical location identified for the command and control center, <CITY> is requested to finalize the detail layout. This layout is indicative and subject to change.



Recommended minimum dimensions for the key space requirements at the Command & Control Center are as follows:

- Command Control Room : 30 sq. mtrs
- Meeting Room : 16 sq. mtrs
- Facility for citizens & external stakeholders to view feeds : 12 sq. mtrs
- HelpDesk & Technical Staff Room : 12 sq. mtrs
- Backup Storage, Switch Room, UPS Room : 6 sq. mtrs each
- Utility Rooms for Men & Women : Based on availability of space

8.6 Proposed Bill of Material (BoQ)

Sr. No.	Item	Ref. Schedule
CAPITAL COST ELEMENTS		
1	Edge Devices	A
2	Data Center	B
3	Central Command Center (at CP Office)	C
4	Viewing Center at <CITY> Municipal Council	D
5	Surveillance System for Police Vans	E
6	Miscellaneous Costs	F
OPERATIONAL COST ELEMENTS		
7	Bandwidth Cost	G
8	Electricity Costs	H
9	Operations & Maintenance for IT / Non-IT Infrastructure	I
10	Managed Hosting Costs	J
11	Technical Manpower	K
10	Costs to connect other establishments for Collaborative monitoring	L

Schedule A – Edge Devices

#	Description	Qty.
1	Outdoor Box Cameras (Normal)	
2	Outdoor Box Cameras (for ANPR)	
3	Outdoor PTZ Cameras	
4	IR Illuminators	
5	Thermal Cameras	
6	Radars for Speed Detection	
7	Emergency Calling Box	
8	Public Address System	
9	Variable Messaging Signs	
10	Poles for Cameras and Equipment	
11	Provisioning of Electrical Power	
12	WiFi Mesh provisioning	
13	Switches / Routers	

14	Networking / Cabling Cost (Passive Components) (Towards cost components like digging & re-filling, Junction Box, Patch Panel, LIU, OFC, CAT 6 cable, Patch cords, Pipes, Media Converters, Installation and Labour costs)	
15	RI (approx.. 100mtrs per location, assuming 75% locations for wired)	
16	Digging, Piping & Re-filling (approx.. 500 mtrs per location, assuming 75% locations for wired)	
17	Wireless Equipment for 25% locations	
18	Cost of connectivity for collaborative monitoring (50 sites)	

Schedule B – Data Center

#	Description	Qty.
1	Servers (inclusive of Operating System)	
1.a	Application Servers	
1.b	Recording Server	
1.c	Analytics Server	
1.d	Database Server	
1.e	Management Server	
1.f	Enterprise Backup Server	
1.g	Domain Controller	
1.h	Antivirus Server	
1.i	Server load balancer	
2	Application & System Software	
2.a	Video Management System	
2.b	Updated Base Map for <CITY> Area (min. 1:1000)	
2.c	Viewing Software for GIS	
2.d	Backup Solution	
2.e	Enterprise Management System (including SLA Mgmt, HelpDesk Mgmt, Network Mgmt, BMS)	
2.f	Anti-virus Software	
2.g	LDAP Software	
2.h	Customized Software (Dashboard for Police Department (for various levels))	
2.i	ANPR (software + license)	
2.j	Emergency Calling Box	
2.k	Public Address System	
2.l	Variable Messaging Signs	
2.m	Parking Lot Management Software	
3	Desktop for Mgmt staff	
4	Storage solution	
5	Storage Management System	

6	Tape Library	
7	Core Router	
8	Switches	
8.1	L2 Switches	
8.2	L3 Switches	
9	Firewall	
10	Intrusion Prevention System	
11	Racks (Caged)	
12	Indoor Fixed Dome Cameras	
13	Fire Proof Enclosure for Media Storage	
14	Networking Cost (Passive Components) (Pl. specify the details)	
15	Data Backup Solution	

Schedule C – CP Office Command Center

#	Description	Qty.
1	LED Displays – Min. 46” (Full HD) mounted in a 5 X 4 arrangement	
2	Touch Monitors	
3	Monitoring Workstations (Computers)	
4	Network Colour Laser Printers	
5	Min. 46” LED Display (Full HD)	
6	Indoor Fixed Dome Cameras for internal surveillance	
7	Switches / Routers	
8	Networking/IT Racks	
9.	Networking Cost (Passive Components) (Pl. specify the details)	
11	Electrical Cabling & Necessary Illumination Devices	
12	Fire Safety System with alarms	
13	Access Control System (RFID/Proximity based, for all staff)	
14	Office Workstations (Furniture and Fixtures)	
15.	Comfort AC	
16.	UPS	
17	DG Set	

Schedule D – <CITY> Viewing Center

#	Description	Qty.
1	Min. 46” LED Displays	
2	Monitoring Workstations	
3	Switches / Router	

4	Office Workstations (Furniture and Fixtures)	
5	UPS	
7	Networking Cost (Passive Components)	

Schedule E – Mobile Vans (For Mobile Video Surveillance) – 3 Vehicles

Sr. No.	Description	Qty. (for each vehicle)
1	Laptop for viewing	
2	Outdoor Fixed Box Cameras (2 per Van)	
3	Full HD Handycam (meeting all the basic parameters of Fix Box Camera) with wireless capability	
4	Equipments for Wireless Connectivity	
5	Router, Modem	
6	Mounting Accessories	
7	Cabling	
8	Installation, Testing and Training	
9	Local Storage for 16 hours	

Schedule F – Miscellaneous Cost

#	Description	Qty.
1	Customized Mobile Application to integrate smartphones / tablets for 2-way communication	
2	Training Costs (per batch)	
2.a	Functional Training	
2.b	Administrative Training	
2.c	Sr. Management Training	
3	Hardware, Software for supporting creation of legal evidence on CDs / DVDs in an untampered manner	
4	Mobile App for Parking Lot availability	
5	Handheld Devices for Parking Managers	
6	PDA/Tablets/iPads for the Officers	
7	Project Management by the SI	
8	Project Management Consultancy for <CITY>	
9	Local Storage for 16 hours for 20 buses	

Schedule G –Bandwidth

#	Description	Qty.
1	Bandwidth for Outdoor Box Cameras (Cameras – Data Center)	
2	Bandwidth for Outdoor PTZ Cameras (Cameras – Data Center)	
3	Bandwidth for Thermal Cameras (Cameras – Data Center)	
4	CP Office – Data Center	
5	Viewing Center at <CITY> Municipal Council – Data Center	

Schedule H –Electricity

#	Description	Qty.
1	Electricity at Viewing Centers (2)	
2	Electricity at CP Office Control Centre	
4	Electricity for Edge Devices	

Schedule I –Operations and Maintenance for IT/ Non-IT Infrastructure

#	Description	Qty.
1	Edge Devices & related Infrastructure	
2	Servers Side Infrastructure (Hardware & Software)	
3	Client Side Hardware	

Schedule J –Managed Hosting

#	Description	Qty.
1	Server and Network Racks	
2	Seating Space for Project Team at DC	

Schedule K – Technical and Operational Manpower

#	Description	Qty.
1	Project Manager	
2	Asst. Project Manager	
3	Technical Expert – Network	
4	Technical Expert – Security	
5	Technical Expert – Server	
6	Technical Expert – Storage	
7	Technical Expert – EMS	
8	Technical Expert – VMS	
9	BMS Support	
10	Helpdesk Manager	
11	Helpdesk Staff	
12	FMS for CP Office	
13	FMS for Viewing Centers (optional)	
14	FMS for Police Stations (optional)	
15	Video Technician	

Schedule L – Cost to Connect Other Establishments

Sr. No	Description	Qty. #
1	Bandwidth cost for establishing 10 Mbps connection to one establishment (for 5 Cameras simultaneously on average 1 day)	XX instances every year

The SI will need to ensure the bandwidth is available for 24 X 7, in order to make the feed available to police in case of any security breach related incidences. Approx. estimates for such incidences are 5 per year.

This DPR document has been prepared by using the data and information provided by various stakeholders in the meetings held at <CITY> / at <City> Commissioner of Police HQ and publicly available information for dissemination for research, analysis, review and reference purposes. Whilst due care and caution has been taken in compilation and processing of data, but does not guarantee the accuracy, reasonableness or completeness of, or for any errors, omissions or misstatements, negligent or otherwise, relating to the project, or makes any representation or warranty, express or implied, in relation to the information furnished in the documents submitted.

This document has been prepared for and only for <CITY> and for no other purpose. We do not accept or assume any liability or duty of care for any other purpose or to any other person to whom this report is shown or into whose hands it may come save where expressly agreed by our prior consent in writing.