INVITATION OF BIDS

For

Design, Development, Implementation and Maintenance of IP Camera based Surveillance solution, City Network Solution, Emergency Communication System, Smart Lighting Solution and Connected Fleet Solution with Facility Management Services at selected locations in Ujjain City

Ujjain Municipal Corporation

February 2016

1. Disclaimer

All information contained in this Request for Proposal (RFP) provided/ clarified are in the good interest and faith. This is not an agreement and this is not an offer or invitation to enter into an agreement of any kind with any party. Though adequate care has been taken in the presentation of this RFP document, the interested bidders shall satisfy themselves that the document is complete in all respects.

The information published in this document is not intended to be exhaustive. Interested bidders are required to make their own enquiries and assumptions wherever required. Intimation of discrepancy, if any, should be given to the specified office immediately. If no intimation is received by this office by the date mentioned in the document, it shall be deemed that the RFP document is complete in all respects and firms submitting their bids are satisfied that the RFP document is complete in all respects.

Ujjain Municipal Corporation reserves the right to reject any or all of the applications submitted in response to this RFP document at any stage without assigning any reasons whatsoever. Ujjain Municipal Corporation also reserves right to withhold or withdraw the process at any stage with intimation to all who have submitted their bids in response to this RFP. Ujjain Municipal Corporation reserves the right to change/ modify/ amend any or all of the provisions of this RFP document without assigning any reason. Any such change would be communicated to the bidders by posting it on the website http://www.mpeproc.gov.in

Neither Ujjain Municipal Corporation nor their employees and associates will have any liability to any prospective respondent interested to apply or any other person under the law of contract to the principles or resolution or unjust enrichment or otherwise for any loss, expense or damage which may raise from or be incurred or suffered in connection with anything contained in this RFP document, any matter deemed to form part of this RFP document, the award of the assignment, the information and any other information supplied by or on behalf of Ujjain Municipal Corporation or their employees and Bidder or otherwise arising in any way from the selection process for the Assignment.

Information provided in this document or imparted to any respondent as part of RFP process is personal to Ujjain Municipal Corporation and shall not be used by the respondent for any other purpose, distributed to, or shared with any other person or organization.

2. Acronyms

BG	Bank Guarantee
EMD	Earnest Money Deposit
GoMP	Government of Madhya Pradesh
GoI	Government of India
RFP	Request for Proposal
STQC	Standardization Testing and Quality Certification
O&M	Operations and Maintenance
PQ	Pre-Qualification
PBG	Performance Bank Guarantee

Table of Contents

3. Notice Inviting Bids

NIT NO. : DATE: 01/02/2016

1. Ujjain Municipal Corporation intends to appoint a firm for **Designing, Development, Implementation & Maintenance of IP Camera based Surveillance solution, City Network Solution, Emergency Communication System, Smart Lighting Solution and Connected Fleet Solution with Facility Management Services at selected locations** to create a Unified Smart City Network for connecting various citizen services under a common platform that will provide and enable the Simhasth Mela administration to monitor, manage and act faster and in a smarter way during the Mela apart from providing the basic and necessary services to the citizens and the visitors.
2. It shall smoothen, control and regulate the number of Travellers/pilgrims in the city of Ujjain and avoid any inconvenience to the travellers/pilgrims in Simhasth, which among other facilities effecting a congestion free public transportation on roads, pathways entering Ujjain city.
4. UMC invites online bids in three envelope system from competent bidders having sound technical and financial capacity for implementation of the assignment.
5. The key dates and other details are as under:

1	Tender No.	UMC/.....2016
2	Name of the Work	Design, Development, Implementation & Maintenance of IP Camera based Surveillance solution, City Network Solution, Emergency Communication System, Smart Lighting Solution and Connected Fleet Solution with Facility Management Services at selected locations in Ujjain City
3	Name of the issuer of this tender	Ujjain Municipal Corporation
4	Joint Ventures or Consortium are permissible:	Yes
5	Date of issue of tender document	1st February 2016
6	Last Date for Purchase of Bids	23rd February 2016, up to 15:00 hrs.
7	Last Date for sending Pre Bid Queries only through E-mail, if any	8th February 2016 till 17:30 hrs
8	Pre-Bid Meeting	9th February 2016 at Ujjain Municipal Corporation at 15:00 hrs.
9	Last Date for Submission of Bids	24th February 2016, up to 12.00 hrs.

10	Submission of EMD (Online)	24th February 2016, up to 12.00 hrs.
11	Date of Opening of Bids – Technical	24th February 2016 at 14.00 hrs
12	Date of Commercial Bid opening	Opening after Technical Evaluation (Communicated to the Qualified bidders)
13	Address of Communication	Commissioner, Ujjain Municipal Corporation, Kshatrapati Shivaji Bhavan, Agar road, Ujjain M.P – 456001
14	Cost of Tender Document	Rupees 25,000 (Twenty Five Thousand only) online through e-procurement portal. (RTGS/ NEFT not applicable)
15	Earnest Money Deposit (EMD)	Rs. 10,00,000/- (Rs. Ten Lakhs (RTGS/ NEFT not applicable)
16	Performance Bank Guarantee	5% of the Contract value in the form of BG/ DD/FDR as per the means agreed with UMC valid for the duration of the contract ie; 5 years.
17	EMD Validity Period	90 days
18	Bid submission	Technical Bids: Online through mpeproc.gov.in as well as in Physical Hardcopy Financial Bids: Only Online Through mpeproc.gov.in
19	Validity of Proposal	180 days from date of submission
20	Method of Selection	Least Cost basis amongst all technical qualified bidders.

6. The contractor will be under obligation to operate and maintain the system.
7. The tender document can be obtained online at http://www.mpeproc.gov.in. The fee of tender document is Rs. 25,000/- (Rs. Twenty Five Thousand Only) which must be paid online.
8. The Ujjain Municipal Corporation reserves right to cancel the tender process without assigning any reason and reject any or all tenders without assigning any reason or to call any other information from the tenderer.
9. The Bidder should undergo the terms and conditions contained in the tender documents.
10. Any further changes or corrigendum would be published only online at http://www.mpeproc.gov.in, separate advertisement would not be published in newspapers.
10. The mode of submission of Financial bid is only online through e-procurement portal (www.mpeproc.gov.in). However the technical bids will be submitted both in Physical Hard copy as well as Online.. In case of any dispute between Online and Hardcopy Proposal, Hardcopy Proposal will be considered as final.

Superintending Engineer
Ujjain Municipal Corporation (M.P.)

Ujjain

4. Instructions to Bidder

4.1. Scope of Bid

4.1.1. Project Background and Overview

Cities around the world are facing a plethora of complex challenges. As the world's population shifts to urban areas, leaders are pressed for answers to overcrowding, pollution, budget, and resource constraints, and the need for continuing growth. These issues can be mitigated through the adoption of scalable solutions that take advantage of information and communications technology (ICT) to increase efficiencies, reduce costs, and enhance quality of life. Cities that take this approach are commonly referred to as Smart Cities, a concept highly discussed in urban planning and city policy circles worldwide.

However, the key obstacle in implementing such scalable solutions is the complexity of how cities are operated, financed, regulated, and planned. For example, every city department makes investments independently, resulting in:

- Isolation of infrastructure and IT resources
- No sharing of intelligence and information such as video feeds, data from sensors, etc.
- Waste and duplication in investment and effort
- Difficulty in scaling infrastructure management

Cities have an opportunity to use the network as the platform to offer urban services and to be sustainable. Using the network as the fourth utility - along with electricity, water, and natural gas, cities can integrate multiple systems to deliver on-demand services over a highly secure Internet-enabled cloud infrastructure. Such services and related networks can help cities address urban challenges as well as improve their livability index.

State-of-the-art systems, such as intelligent transportation, parking, safety, and energy management, are helping cities to implement Smart City services.

Municipal Corporation and Simhasth Mela Administration in Ujjain carries a vision to leverage on cutting edge technologies to run the Mela in a Smart way and provide better citizen experience. At the same time they also have a vision to make Ujjain City smarter in most of these aspects. The City administration team launched initiatives, which aim at achieving excellence in all walks of life and focus on community building through teamwork.

Firstly, Ujjain Municipal Corporation team along with Simhasth Mela administration would like to establish some key strategically important initiatives in identified locations to

provide basic citizen services and monitor all aspects of those in terms of service availability, incident reporting and management.

This proposal describes design, build, and implement a common infrastructure with some key citizen centric amenities/Solutions deployment at prime locations of Ujjain City. The services covered under this proposal is as mentioned below:

1. A city network in identified locations
2. Parking management at specific areas
3. Smart Lighting along the Ghat area of Ujjain that is considered to be the most visited place during the Simhasth Mela.
4. Smart and connected fleet management i.e. Smart Buses, bus stops and Municipal Solid Waste fleet.
5. Video surveillance in identified locations in the City
6. Integrated dashboard and central command and control center

The vision of the future city, a city with a pervasive overlay of ICT connecting things, organizations, and people. For example, imagine sensors in bus connected to transportation management systems that analyze day-to-day traffic flow data. In addition to providing drivers with better routes to their destinations, these systems could provide public safety and other city departments with what-if scenarios in case of events or accidents to improve response times. It is the aggregation of data available from thousands of devices connected to a foundation city network that delivers significant value. This is called as IoE, or the Internet of Everything.

Objectives of Smart City Network Solution at Ujjain

Simhasth Kumbh Mahaparv is one of the four "Kumbh Melas" celebrated by largest spiritual gathering on Planet Earth. Simhasth Kumbh Mahaparv is rejoiced by holy dip in the sacred river Kshipra in ancient and religious city Ujjain (Madhya Pradesh). Simhasth Kumbh Mahaparva is based on the celestial line-up of Planets and the Signs of the Zodiac, which occurs every 12 years.

Around 5 Crore (50 Millions) pilgrims from all walks of life are expected to join and take holy dip. Pilgrims visit the "Mahakaleshwar" Jyotirlinga and other ancient temples in and around Ujjain and thereafter they find spiritual solace in 'Satsang' and 'Sankirtan' in Mahaparv Kshetra (Mela Kshetra) with great Sadhus.

The intent to create a Unified Smart City Network in Ujjain is to connect various citizen services under a common platform that will provide and enable the Ujjain Municipal Corporation and Simhasth Mela administration to monitor, manage and act faster and in a smarter way during the Mela apart from provide the basic and necessary services to the citizens and the visitors. Essentially the Smart City Network will help the Mela Administration in the following way:

1. Provide basic services optimally and effectively to the pilgrims and visitors.
2. Effectively provide situational awareness to the mela administration and take necessary action.
3. Smart and fast response to incidents through central command and control center.
4. Citizen experience through various smart city infrastructure solutions via Smart lighting, Smart parking and Smart transport.
5. Provide with right information about various City situations to the pilgrims and visitors effectively that in turn will help in crowd management
6. Most importantly, utilize the infrastructure during the period of Simhasth Mela and then re-deploy the same infrastructure appropriately to Make Ujjain a smart and connected city.

It is important to note that 's Smart + Connected City Network solution will help Ujjain city build a converged network, bringing together different city management vertical solutions on a single foundational network infrastructure. The converged network facilitates information exchange between resources and applications across different domains. It is an end-to-end open platform enabling IoE services for cities. Its key objectives are to provide:

- IP connectivity to things, people, devices, and vehicles in the city street
- Wired and wireless, scalable, and highly secure network platform
- A data management framework to help enable data collection, organization, and sharing

- Distributed compute and storage services, location services, and security services

- The UMC envisaged solution requirement for is listed below;

1. IP Camera based Monitoring solution
2. City Network Solution
3. Smart Lighting Solution
4. Connected Fleet Solution
5. Data Center Solution , Emergency Communication System and City Command Control Centre

4.1.2. Project Objective

IP Camera based Monitoring envisaged below objectives;

a) This Solution helps to monitor public areas, analyze patterns, and track incidents and suspects, enabling quicker response.
b) Traffic situation awareness
c) Quicker response to incidents
d) Increased situational awareness of major roads approaching to Ujjain City
e) Increased attractiveness to businesses and workers
f) Improved planning and resource allocation
g) Improved communications about incidents

City Network Solution envisaged below objectives;

The city network is the most important part of a Smart City Infrastructure. The aggregation layer of the city important aggregation nodes that will aggregate various service locations. The Pre-aggregation/Access layer of the city network that will be used for Ujjain Smart City. These nodes connects all the service points of the Smart city network as well as Mela services like Lighting, Parking, Monitoring etc. The Network that will be built will remain as the most important layer of the smart city infrastructure and the same can grow as and when the services grow across the city as part of the smart City initiative in multiple phases.

Smart Lighting Solution envisaged below objectives;

Electric streetlights are essential elements of a municipal environment. They affect residents' sense of safety and place while influencing a city's ability to create an inviting environment for business and tourism. Unfortunately, outdoor lights are also a major energy draw.

- Reduce energy consumption, cost, and maintenance

- Enhance situational awareness, real-time collaboration, and decision making across city

- Add intelligent IT innovations to transportation, utilities, public safety, and environmental monitoring without adding significantly more physical infrastructure

- Real-time data communications The entire lighting solution comprises of three components.

The WiFi infrastructure, the Control noded and the underlying city network. The controller nodes will be able to control each light individually e.g. On/OFF, maintenance status, scheduled lighting and also integrate to the central command and control center for a consolidated dashboard of the lighting operation. The Wireless infrastructure not only connects and controsl the wireless nodes but also can be used for wireless communication for the field operators who will be there to manage various incidents and communicate to the command and control center.

Connected Fleet Solution envisaged below objectives;

a) Locate and track vehicles

b) Identify route diversion during any event

c) Video feeds from the fleet to the central command and control

d) Content display system into the bus can be used for revenue generation

e) Can be used for display ETA for vehicles at the bus stops

f) The same solution can also be used for Waste management vehicles and can be tracked along with video feeds.

Emergency Communication System, Data Center Solution and City Command Control Center,

Data Center and Command Control Center and Communication System envisaged below objectives;

a) Operation Center will provide Consolidated Dashboard for Smart City Services like Smart Lighting , GIS Services etc.
b) Maximizes real-time monitoring and control efficiency from one workstation through the synchronized control
c) Provides a single- pane-of glass view for operations centers
d) Reduced bandwidth and simplified integration of various systems
e) Ability to report city safety incidents
f) "Improved communications about incidents"

g) CUG and Multichannel communication to enable the Mela and City command center to communicate with all the zonal and sector office employees for incident management and can also get integrated with the Police communication system to be built by Tetra.

h) Centralized helpdesk for incident reporting and management

4.1.3. Scope Summary

Solution wise scope is summarized below and indicative Bill of material is also provided in commercial format, However bidder should consider necessary equipment to complete the solution.

S. No.	Solution Type	High Level Scope
A	IP Camera based Monitoring solution	32 Major Points to be covered with road side cameras especially in entry/exit roads of the city and also to cover all the Zonal and sector offices
B	City Network Solution	City wide network to connect to identified aggregation locations and access locations
C	Smart Lighting Solution	300 light poles along the Ghat area covering 8.4 Km. 4x120W lights per pole, hence 1200 total lights to be connected under smart connected lighting platform.
D	Connected Fleet Solution	50 Buses to be automated for Automatic vehicle Location tracking, Vehicle telemetry data collection and Passenger information Systems in all the 50 the Buses and in 50 bus shelters.
E	Data Center Solution, Emergency Communication System and City Command Control Center	Setting up Data Center infrastructure and Operation Center - Command Control Center and Communication System and Integrated Smart City Management Platform & Smart City Services with 25 operators Control Room
F	Integrated Smart City Management Platform	Solution should have central City Infrastructure and Services management platform to centrally monitor and manage all the services. The Smart lighting, connected transport and the field operation application will be able to integrate to this platform and show up as alerts and status on

S. No.	Solution Type	High Level Scope
		the dashboard/city map etc.

The entire hardware & software infrastructure to be proposed by the bidder will be installed & made operational in the mela area as per the timelines specified in the RFP and maintained during Simhastha 2016 for a period of 90 days (3 months). Post Mela event, the entire infrastructure needs to be decomminssioned & reinstalled in the area to be identified locations across Ujjain City. The whole decommissioning & reinstallation process will have to be carried out by the bidder as instructed by UMC authority & bidder has to provision any charges in this bid, if necessary. All necessary harware, software, licenses etc & IPR will be in the name of UMC.

Note: The Solution documents must be submitted alongwith Technical proposal. Below should be the content of solution document.

1 Understanding of Project requirement
2 Proposed solution
3 High Level Design
4 Details of devices/ Equipments

4.1.4. Bidder's Major Responsibility

Below is high-level responsibility in Deployment and Support Phase:

A) Deployment Phase Services

The Bidder shall be responsible for the following activities:

1) Project Management
2) Network Readiness Assessment
3) Network Implementation Development
4) System Acceptance Test Plan Development
5) Onsite Support Services
6) L1 Engineer resource
7) Cabling and Infrastructure support
8) Setting up Command Center and Data Center as per requirement

B) Support Phase Services:

- The Bidder Shall be responsible for complete service and support management pertaining to the project as per RFP
- The Bidder to ensure the entire infrastructure is supported back to back by OEM support services

- The Bidder has to provide support for all the offered hardware & software from the date of supply within 24 hrs. Any down time beyond 24 hrs may invite penalty as decided by UMC. Bidder has to provide detailed escalation matrix for support services.

4.1.5. Project Implementation Timelines

Bidder Must ensure the Project is implemented as per the following timelines. In case of Delays Late delivery penalty at the rate of 2% of the tender cost per day will be imposed on the bidder, or UMC may take a decision as follows.

Failure to meet project milestones / deliverables, shall entitle UMC :

a. Encashment of bank gurantee; and/ or
b. Terminate this contract; and / or
c. levy penalty charges as given in RFP; and / or
d. proceed with blacklisting of the bidder for all future projects.

S. No.	Name of the deliverable	Timelines in Months (M= Contract Signing Date)
1	Preparation of Sites Survey Reports	**M + 7 Days**
2	Evaluation & Approval of Sites Survey Reports	**M + 10 Days**
3	Submission of applications for permissions to and getting permissions, NOCs etc. issued by ULB's in favour of purchaser	**M + 11 Days**
4	Submission of Training Plan & Material along with Submission of Standard Operating Procedures.	**M + 12 Days**
5	Delivery of Equipment	**M + 21 Days**
6	Installation, commissioning and operationalizing of Equipment at Data Center	**M + 30 Days**
7	Installation, commissioning and operationalizing of Equipment at Sites	**M + 40 Days**
8	Functional Acceptance Test by District Inspection Committee / RHQ committee; declaration of system 'go live'	**M + 45 Days**

4.2. General

4.2.1. Procedure for Participation in E-tendering

The procedure for participation in e-tendering is given in the Bid Data Sheet.

4.2.2. One Bid Per Bidder

4.2.2.1 The bidder can be an individual entity or a joint venture (if permitted as per Bid Data Sheet). In case the J.V. is permitted, the requirement of joint venture shall be as per the Bid Data Sheet.

4.2.2.2 No bidder shall be entitled to submit more than one bid whether jointly or severally. If he does so, all bids wherein the bidder has participated shall stand disqualified.

4.2.3. Cost of Bidding

The bidder shall bear all costs associated with the preparation and submission of his bid, and no claim whatsoever for the same shall lie on the Government.

4.2.4. Site Visit and examination

The bidder is advised to visit and inspect the Site and its surroundings and obtain for itself on its own responsibility all information that may be necessary for preparing the bid and entering into a contract for construction of the work. All costs in this respect shall have to be borne by the bidder.

4.3. Bid Documents

4.3.1. Content of Bid Documents

The Bid Document comprises of the following documents:

1. NIT with all amendments.
2. Instructions to Bidders.
3. Conditions of Contract
   - i) Part I General Conditions of Contract and the Contract Date; and
   - ii) Part II Special Conditions of Contract.
4. Technical and Functional Requirements
5. Letter of Acceptance.
6. Bid Data Sheet
7. Format for AFFIDAVIT
8. Format for JOINT VENTURE (J.V.)
9. Format for ORGANIZATIONAL DETAILS
10. Format for Financial Capability of the Consultant
11. Format for Technical Personnel's
12. Formats of Commercial Bid
13. Proposed Payment Terms
14. Project Implementation Timelines
15. Service Level Agreement (SLA)

16. General Terms and Conditions for Simhastha
17. Any other document(s), as specified.
18. The bidder is expected to examine carefully all instructions, conditions of contract, the con Intel data, forms, terms and specifications, bill of quantities, forms and drawings in the Bid Document. Bidder shall be solely responsible for his failure to do so.

4.3.2. Pre-bid Queries

All enquiries from the bidders relating to this RFP must be submitted by email to nagarnigamujjain@yahoo.com . The queries should necessarily be submitted in the following format:

Sr. No.	RFP Document Reference (Section No., Page No.)	Content of the RFP requiring clarification	Clarification Sought
1 2 …			

Queries submitted post the above-mentioned deadline or which do not adhere to the above-mentioned format may not be responded to.

4.3.3. Amendment of Bid Documents

4.3.3.1 Before the deadline for submission of bids, the Employer may amend or modify the Bid Documents by publication of the same on the website.

4.3.3.2 All amendments shall form part of the Bid Document.

4.3.3.3 The Employer m ay, at its discretion, extend the last date for submission of bids by publication of the same on the website.

4.4. Preparation of Bid

The bidders have to prepare their Financial bids online, encrypt their Bid Data in the Bid Forms and submit Bid Seals (Hashes) of all the envelopes and documents related to the Bid required to be uploaded as per the time schedule mentioned in the key dates of the Notice Inviting e-Tenders after signing of the same by the Digital Signature of their Authorized representative.

4.4.1. Documents Comprising the Bid

The bid submitted online by the bidder shall be in the following parts:

Part 1 - This shall be known as Envelope A. Envelop A shall contain the following as per details given in the Bid Data Sheet:

i. Certificates of incorporation and/ or Registration Certificates.
ii. Earnest Money; and
iii. An affidavit duly notarized.

Part 2 - This shall be known as Envelope B and required to be submitted only in works where pre-qualification conditions and/or special eligibility conditions are stipulated in the Bid Data Sheet, Envelop B shall contain a self -certified sheet duly supported by documents to demonstrate fulfilment of pre-qualification conditions.

Part 3 - This shall be known as Online Envelope C and would apply to this bid. Envelop C shall contain financial offer in the prescribed format enclosed with the Bid Data Sheet.

4.4.2. Language

The bid as well as all correspondence and documents relating to the bid exchanged by the Bidder and the Employer shall be in English or Hindi. Supporting documents and printed literature that are part of the Bid may be in another language provided they are accompanied by an accurate translation of the relevant passages in English. In such case, for the purposes of interpretation of the bid, such translation shall govern.

The bidder is required to submit online bid duly signed digitally, prescribed in the Bid Data Sheet.

4.4.3. Qualifying Criteria for Technical Bid

Prior to the detailed evaluation of the Technical Bids, UMC shall determine whether each bid is (a) complete, (b) is accompanied by the required information and documents and (c) is substantially responsive to the requirements set forth in the RFP documents.

UCM has formed a Technical Committee, which will evaluate both technical & commercial bids received in response to this RFP. The findings of the said Committee and subsequent decision of State Government shall be final and binding on all the bidders. Only those bidders, who fulfil all the Eligibility / Pre-qualification criteria mentioned in the bid, shall be eligible and qualified for technical scrutiny as per the Evaluation Framework given below.

Bidders should obtain minimum 70% in the overall technical evaluation, to qualify for opening of the Commercial Bid. UMC evaluation in this regard shall be final and binding on the Bidder.

UMC may in its sole discretion, waive any informality or non-conformity or irregularity in a Bid Document, which does not constitute a material deviation, provided such a waiver does not prejudice or affect the relative ranking of any Bidder.

4.5. Technical Scoring and Evaluation Criteria

4.5.1. Eligibility Criteria (Envelope A)

The bidder shall be evaluated based on the Eligibility Criteria mentioned below. The bidder shall submit all the documents as mentioned below as per the formats mentioned in different section of RFP. Only eligible bidders would be qualified for Technical Evaluation (Envelope B).

S. No.	Basic Requirement	Specific Requirements	Documents Required
1	General Requirement	Bidder should be an established System Integrator/ consortium and should have been engaged in Supply, Installation, Commissioning and Operations & Maintenance Services of Wi-FI, Lighting, CCTV, Transport network, Data Center and Command control Center / ICT projects for a period of at least 3 financial years as on Dec 2015	Client Certificates confirming year and area of activity should be enclosed.
	Bidder Entity	Consortium/Joint Venture is allowed, one of the parties in the consortium/JV partner will be the Prime Bidder/Lead Bidder. Prime Bidder/Lead Bidder shall be treated as "Bidder" Any of the parties of the consortium /JV partner or the Prime Bidder/Lead Bidder may meet the technical criteria. However, the Prime Bidder/Lead Bidder alone should meet the financial criteria.	Copy of the consortium/JV in case of consortium/JV, clearly specifying the role and area of specialization of the individual parties of consortium/JV, duly signed by Consortium/JV parties on Rs. 100 non-judicial stamp paper should be enclosed.
	Legal Entity	Any legal entity duly registered in India is allowed. In case of consortium/JV, the Prime Bidder/ Lead Bidder should meet this criterion.	a) Certificates of incorporation and/ or b) Registration Certificates
	Turnover	The Prime Bidder/Lead Bidder must have Avg annual turnover of at least Rs. 100 Crores solely from ICT Business and IT Services during each of	Audited and Certified Balance Sheet and Profit/Loss Account

S. No.	Basic Requirement	Specific Requirements	Documents Required
		the last Three financial years as on 31.03.2015.	for the last three Financial Years should be enclosed. CA Certificate be enclosed.
	Technical Capability	The Bidder or any of the parties of the consortium/ Technology Partner must have successfully completed, during last Five financial years as on 31.03.2015, at least the following numbers of Wi-Fi systems & CCTV Monitoring System of value specified herein: Two projects of similar nature for not less than 200 Access Points (AP) in a single work order **OR** Three projects of similar nature for not less than 100 Access Points (AP) in a single work order **AND** One Project of similar nature for not less than 100 IP Cameras in a single work order	Copies of work order or contract agreement or the client certificates/Project Sign-off Certificate from client for satisfactory completion of project and showing order value and cost or OEM undertaking.
	Net Worth	The Bidder or the Prime Bidder/Lead Bidder must have positive net worth of Rs 10 Crores & profit making in each of the last three financial years as on 31.03.2015	CA Certificate mentioning net profit should be enclosed.
	Certification	The Bidder or consortium/JV should possess below Certifications at the time of bidding: a) ISO 9001:2008 Certification for System Integration.	The Bidder is required to furnish the copy of valid certification.
	Tax	The Bidder or the Prime Bidder/Lead Bidder should have a registered number of	Copies of relevant(s) Certificates of

S. No.	Basic Requirement	Specific Requirements	Documents Required
	Registration	a. VAT/Sales Tax where his business is located b. Service Tax c. Income Tax PAN d. The ESI & EPF registration as per Labour Law. e. Registration of Labour License f. Valid Electrical Contractor License	Registration.
	Technical Specifications of BOQ items	The quoted product/item should fulfil all the technical specifications laid out in the tender document mentioned in the Annexure (Technical specifications of BOQ items). The Bidder is required to furnish Make, Model / Part number of the quoted item. Items with equivalent or better Specs will also be accepted.	The Bidder should enclose relevant catalogues, brochures, etc. in support of all the items quoted in the Bid.
		As on date of submission of the proposal, the bidder and any of the consortium members should not be blacklisted/ debarred/ terminated by Central/ State Government Department/ PSU/ Corporation/ Board and Private Sector entity in India for unsatisfactory past performance, corrupt, fraudulent or any other unethical business practices.	Undertaking by the authorized signatory as well as all member of consortium as per the form mentioned in Annexures.
		The bidder and all members of the consortium should have presence in the State with a local office (CITY). However, if the local presence is not there in the CITY, the selected bidder and its consortium members should give an undertaking for arranging the same within one month of the award of the Contract.	Proof of Local presence or A Self Declaration letter by an authorized signatory for local office presence (in absence of local presence).

1. Any bid failing to meet the above eligibility criteria shall be disqualified and will not be considered for Technical Evaluation.

2. Change in Eligibility Criteria: If there is a change in the status of the bidder with reference to any of the eligibility criterion specified above, during the bid process till the award of the project, the bidder should immediately bring the same to the notice of UMC.

3. For the purpose of the criterion, turnover of only the bidding entity will be considered.

Turnover of any parent, subsidiary, associated or other related entity will not be considered. Moreover, the Bidder should provide the experience details of Projects undertaken by it only. Project experience of the Individual Bidder's parent company or its subsidiary or Consortium Members parent company or its subsidiary (who are not Members of the Consortium) will not be considered. Implementation or operation and maintenance experience of parent/subsidiary/associate company(ies) of the Bidder would not be considered for evaluation.

4. In addition, the Solution documents must be submitted alongwith Technical proposal. Below should be the content of solution document.

- **Understanding of Project requirement**
- **Proposed solution**
- **High Level Design**
- **Details of devices/ Equipments**

4.5.2. Technical Evaluation

Bidders who qualify in Envelope A would be considered as qualified to move to the next stage of Technical evaluations. The Technical Evaluation of Bidders' proposals (Envelope B) shall be based on:

1. Technical Proposal Evaluation
2. Technical Presentation

4.5.3. Technical Scoring

1. This is on Least Cost Basis.
2. Minimum Technical Score for qualifying for commercial bid opening is 70%.
3. For the purpose of arriving at Technical Score, the bid shall be evaluated against the Technical Parameters, with respective weightages, as given in RFP.
4. The Total Technical Score will be calculated out of 100 Marks, and shall be evaluated as below:

The Bidder has to score Minimum Qualifying Marks as below:

Minimum qualifying marks in Individual TE criteria will be 70%.

5. The Bidders scoring marks less than the minimum qualifying marks as mentioned above shall be disqualified for Commercial Bid Opening (Envelope C).

4.5.4. Technical Evaluation Matrix

The table below describes the Technical Evaluation criteria along with the weightages for each parameter. Technical Evaluation criteria is defined below:

S. No.	Capability	Criteria for Technical Evaluation	Max marks
1	Experience: Public Wi-Fi including Related Network Infrastructure	The lead bidder/OEM or its consortium members (if any) should have completed at least two Public Wi-Fi of 200 AP'S each and related network infrastructure projects in the last 3 years. For every completed project of 200 AP's-2 marks per project. For every completed project of 400 AP's -4 marks per project.	10
2	Connected Fleet Management	1. For every completed project of 20 fleet or stops -5 marks per project. 2. For every completed project of 5 fleet or stops -2 marks per project.	10
3	Experience of CCTV.	The bidder or its consortium members/ technology partner should have completed at least one outdoor CCTV installation of 500 IP based digital cameras with Central monitoring system. For every project of 500 IP based digital cameras -2.5 marks per project. **OR** The bidder or its consortium members/ technology partner should have completed at least one outdoor CCTV installation with	10

S. No.	Capability	Criteria for Technical Evaluation	Max marks
		Proposed Camera, Server and Storage with 100+ camera and same architecture in India (Project Sign-off Certificate or OEM undertaking) (10 Marks)	
4	Experience: Smart City wide network with Command and Control Centre	The bidder or its consortium members/ technology partner should have completed atleast one City wide network with ruggedized Ethernet+ Wireless access layer +Command and Control Centre project. Projects shall qualify only if it covers capability of centralized communication, integrated management and monitoring of outdoor sensors, devices, and smart equipment including Collection of Data for MIS reporting. (Project Sign-off Certificate or PO Copy or OEM undertaking). For every such project- 5marks	25
5	OEM	Solutions being proposed in the RFP : OEM Qualification as per Gartner Magic Quadrant for the products available in Gartner evaluation: Marks would be awarded as per the following criteria: Magic Quadrant for the Wired and Wireless LAN Access Infrastructure: 5 Marks Leaders (5 Marks) Challenger (4 Marks) Visionaries (3 Marks) Niche Players (2 Marks) Not present in Quadrant (0 Marks) Magic Quadrant for Data Center Networking: 5 Marks	20

S. No.	Capability	Criteria for Technical Evaluation	Max marks
		Leaders (5 Marks) Challenger (4 Marks) Visionaries (3 Marks) Niche Players (2 Marks) Not present in Quadrant (0 Marks) Magic Quadrant for Enterprise Network Firewalls: 5 Marks Leaders (5 Marks) Challenger (4 Marks) Visionaries (3 Marks) Niche Players (2 Marks) Not present in Quadrant (0 Marks) Magic Quadrant for Intrusion Prevention Systems: 5 Marks Leaders (5 Marks) Challenger (4 Marks) Visionaries (3 Marks) Niche Players (2 Marks) Not present in Quadrant (0 Marks) Note: If any bidder is proposing firewalling & IPS solution in a single chassis/box, the OEM should minimum be in Challenger Quadrant for both Firewall & IPS	
6	Approach, Methodology, Project Management, Execution	The Technology Architecture blue print with various components asked (3 Marks), Correlation and analytics of data, integration	15

S. No.	Capability	Criteria for Technical Evaluation	Max marks
	Methodology, SLA management	Architecture (3 Marks), Technical and functional specifications compliance(3) , Make and model(3), Response to SLAs and plans to manage uptime (3Marks). **Bidder has to offer best quality of products. Lower the quality, Lesser the marks.	
7	Manpower deployment	Proposed of manpower at various stages of project and CV of Key professionals Key personnel of the project as per the requirement and profile given in the RFP: Project Manager- 4 marks Team Leader for Smart City Solutions - 3 marks Technical Head- 2 marks Network Admin - 1 mark	10
		Total Marks	**100**

4.5.5. Financial Evaluation

(i). This is a Least cost basis.

(ii). The Financial Bids of Technically Qualified bidders will be opened after communicating to the qualified bidders.

(iii). The Financial Bids of Bidders who have secured Technical Score of 70 marks or above, shall be tabulated for the Project

4.6. Period of Validity Of Bids

The bids shall remain valid for a period specified in the Bid Data Sheet after the date of "close for biding" as prescribed by the Employer. The validity of the bid can be extended by mutual consent in writing.

4.7. Earnest Money Deposit (EMD)

4.7.1 The Bidder shall furnish, as part of the Bid, Earnest Money Deposit (EMD), in the amount specified in the Bid Data Sheet.

4.7.2 The EMD shall be shall be submitted online as per Bid Data Sheet.

4.7.3 Bid not accompanied by EMD shall be liable for rejection as non - responsive.

4.7.4 EMD of bidders whose bids are not accepted will be returned within fifteen working days of the decision on the bid.

4.7.5 EMD of the successful Bidder will be converted into required Performance Security.

4.7.6 Failure to sign the contract by the selected bidder, within the specified period, for whatsoever reason, shall result in forfeiture of the earnest money deposit.

4.8. Confidentiality

6.3.1 Information relating to examination, evaluation, comparison and recommendation of contract award shall not be disclosed to bidders or any other person not officially concerned with such process until final decision on the bid.

6.3.2 Any attempt by a bidder to influence the Employer in the evaluation of the bids or contract award decisions may result in the rejection of his bid.

4.9. Award of Contract

The Employer shall notify the successful bidder by issuing a 'Letter of Acceptance' (LOA) that his bid has been accepted.

4.9.1. Performance Security

4.9.1.1 Prior to signing of the Contract the bidder to whom LOA has been issued shall have to furnish performance security of the amount in the form and for the duration, etc. as specified in the Bid Data Sheet,

4.9.1.2 Additional performance security, if applicable, is mentioned in the Bid Data Sheet.

4.9.2. Signing of Contract Agreement

4.9.2.1 The successful bidder shall have to furnish Performance security and sign the contract agreement within 15 days of issue of LOA.

4.9.2.2 The signing of contract agreement shall be reckoned as intimation to commencement of work. No separate work order shall be issued by the Employer

to the contractor for commencement of work.

4.9.2.3 In the event of failure of the successful bidder to submit Performance Security or sign the Contract Agreement, his EMD shall, stand forfeited without prejudice to the right of the employer for taking any other action against the bidder.

4.10. CORRUPT PRACTICES

The Employer requires that bidders observe the highest standard of ethics during the procurement and execution of contracts. In pursuance of this policy, the Employer:

i. may reject the bid for award if it determines that the bidder recommended for award has, directly or through an agent, engaged in corrupt, fraudulent, collusive, or coercive practices in competing for the Contract; and

ii. may debar the bidder declaring ineligible, either indefinitely or for a stated period of time, to participate in bids, if it at any time determines that the bidder has, directly or through an agent, engaged in corrupt, fraudulent, collusive, or coercive practices in competing for, or in executing, a contract.

For the purposes of this provision, the terms set forth above are defined as follows:

a. "corrupt practice" means the offering, giving, receiving, or soliciting, directly or indirectly, anything of value to influence improperly the actions of another party;

b. "fraudulent practice" means any act or omission, including a misrepresentation, that knowingly or recklessly misleads, or attempts to mislead, a party to obtain a financial or other benefit or to avoid an obligation;

c. "coercive practice" means impairing or harming, or threatening to impair or harm, directly or indirectly, any party or the property of the party to influence improperly the actions of a party;

d. "collusive practice" means an arrangement between two or more parties designed to achieve an improper purpose, including influencing improperly the actions of another party.

4.11. Payment Terms

4.11.1. Material with 1 Yr Supoort Payment Term:

i. 40% Payment will be released after material delivery and Installation in good condition & as per the Proposed specification

ii. 30% Payment will be released after successful Functional Acceptance Test by committee; declaration of system 'go live'

iii. 20% payment will be released after Third Party Verification by an agency appointed by UMC..

iv. 10% payment will retained till period of 1 (one) year and paid after successful support in warranty period of one year.

4.11.2. Additional Four (4) Yrs Support Payment Term:

I. To be paid quarterly in equal installments at the end of each quarter

5. Bid Data Sheet

1	Tender No.	UMC/.....2016
2	Name of the Work	Design, Development, Implementation & Maintenance of IP Camera based Surveillance solution, City Network Solution, Emergency Communication System, Smart Lighting Solution and Connected Fleet Solution with Facility Management Services at selected locations in Ujjain City
3	Name of the issuer of this tender	Ujjain Municipal Corporation
4	Joint Ventures or Consortium are permissible:	Yes
5	Date of issue of tender document	1st February 2016
6	Last Date for Purchase of Bids	23rd February 2016, up to 15:00 hrs.
7	Last Date for sending Pre Bid Queries only through E-mail, if any	8th February 2016 till 17:30 hrs
8	Pre-Bid Meeting	9th February 2016 at Ujjain Municipal Corporation at 15:00 hrs.
9	Last Date for Submission of Bids	24th t February 2016, up to 12.00 hrs.
10	Submission of EMD (Online)	24tht February 2016, up to 12.00 hrs.
11	Date of Opening of Bids – Technical	24th February 2016 at 14.00 hrs
12	Date of Commercial Bid opening	Opening after Technical Evaluation
13	Address of Communication	Commissioner, Ujjain Municipal Corporation, Kshatrapati Shivaji Bhavan, Agar road, Ujjain M.P – 456001
14	Cost of Tender Document	Rupees 25,000 (Twenty Five Thousand only) online through e-procurement portal. (RTGS/ NEFT not applicable)
15	Earnest Money Deposit (EMD)	Rs. 10,00,000/- (Rs. Ten lakhs only) (RTGS/ NEFT not applicable)
16	Performance Bank Guarantee	5% of the tender Value in the form of DD/BG/FDR or any other means agreed by UMC. Valid for entire 5 years duration project period.

17	EMD Validity Period	90 days
18	Bid submission	Technical: Online through mpeproc.gov.in as well as Physical Hardcopy Financial Bid: Only Online Through mpeproc.gov.in
19	Validity of Proposal	180 days from date of submission
20	Method of Selection	Least Cost basis amongst all technical qualified bidders.

Notes:

1. Ujjain Municipal Corporation reserves the right to change any schedule of bidding process. Please visit e-Procurement website http://www.mpeproc.gov.in mentioned in document regularly for the same.
2. Proposals must be received not later than time, date and venue as mentioned in the Fact Sheet. Proposals that are received after the deadline WILL NOT be considered in this procurement process.
3. The mode of submission of Financial bid is only online through e-procurement portal (www.mpeproc.gov.in). However the technical bids will be submitted both in Physical Hard copy as well as Online. In case of any dispute between Online and Hardcopy Proposal, **Online** Proposal will be considered as final.
4. Any future Corrigendum/Information shall be posted only on our website http://www.mpeproc.gov.in.
5. Rejected / disqualified bidders would only be intimated post final selection of successful bidder/ completion of Bid process. Along with such intimation, EMD retuning process would be initiated for disqualified bidders and the same would be affected within 30 days of issuing letter of intent to successful bidder.

Annexure-A

6. Key Dates – Annexure-A

Purchase of Tender Start Date:	01-02-2016
Purchase of Tender End Date:	23-02-2016 till 15:00 hrs
Bid Submission End Date:	24th-02-2016 till 12.00 hrs
Mandatory Submission (Envelope A) Open Date:	24-02-2016 upto 12.00
Technical Proposal (Envelope B) Open Date:	24-02-2016 upto 12.00 hrs
Commercial Bid (Envelope C) Open Date:	Opening after Technical Evaluation

Annexure-B

7. Format for Affidavit – Annexure-B

(with self seal signed)

I/.....who is/ are (status in the firm/ company) and competent for submission of the affidavit on behalf of M/S

(contractor) do solemnly affirm an oath and state that:

I/we am/are fully satisfied for the correctness of the certificates/records submitted in1 support of the follo wing inform ation in bid docum ents which are being subm itted in response to notice inviting e-tender No. for (name of work) dated issued by the (name of the department).

I/we am/ are fully responsible for the correctness of following self -certified information/ documents and certificates:

1. That the self-certified information given in the bid document is fully true and authentic.

2. That:

   a. Term deposit receipt deposited as earnest money, demand draft for cost of bid document and other relevant documents provided by the Bank are authentic.

   b. Information regarding financial qualification and annual turnover is correct. c. Information regarding various technical qualifications is correct.

3. No close relative of the undersigned and our firm/company is working in the department.

OR

Following close relatives are working in the department:

Name ..... Post..... Present Posting

Signature with Seal of the Deponent (bidder)

I/ W e,.....above deponent do hereb y certif y that the f acts mentioned in above paras 1 to 4 are correct to the best of my knowledge and belief. Verified today .....(dated) at ..... (place).

Signature with Seal of the Deponent

(bidder)

Note: Affidavit duly in original shall reach at least one calendar da y before opening of the bid.

8. Formats for Compliance to the Benchmark / Minimum Specification (Technical and Functional Requirements) – Annexure-C

8.1. IP Camera based Monitoring Solution

8.1.1. HD Fixed Camera Type 1

S.NO.	Camera Characteristics	Description	Compliance (Yes/No)
1	Requirement Overview	High-definition IP Box Camera for outdoor	
2	Sensor Type	1/2.7" Progressive Scan CMOS with additional digital signal processor (DSP) to support complex applications such as real-time video analytics	
3	Max Resolution	1920x1080 @ 30fps	
4	Dynamic Range	69db	
5	Lens/Iris	3.1-8mm- P-Iris	
6	Audio I/O	The camera supports full-duplex audio and options for half-duplex operation. Suould support Audio compression G.711 A, Law, G.711 U, Law, G.726, Audio in x 1	
7	Digital I/O	(3.5-mm miniature jack)	
8		Audio out x 1	
9		(3.5-mm miniature jack)	
10		DI x 1	
11		DO x 1	

S.NO.	Camera Characteristics	Description	Compliance (Yes/No)
12	Max Illumination	Color: 0.3 lux	
13		B/W: 0.05 lux	
14	Day/Night	Automatic, manual, scheduled	
15	Local Storage	Should support MicroSD -min 32 GB	
16	Video Compression & Video Streaming	● Single stream H.264 or MJPEG up to 1080p (1920 x 1080) @ 30 fps ● Dual stream H.264 and MJPEG ◦ Primary stream programmable up to 1280 x 720 @ 30 fps ◦ Secondary stream programmable up to 960 x 544 @15 fps	
17	ONVIF	Should support for ONVIF 2.0 allows for standards based interoperability	
18	POE and External Power	12V DC, 24V Ac and PoE- 802.3af compliant (Class 3)	
19	Power Consumption (in watts)	Max 10 Watt at DC	
20	Supported Protocol	Dynamic Host Control Protocol (DHCP), Hypertext Transfer Protocol (HTTP), Secure HTTP (HTTPS), Network Time Protocol (NTP), Real-Time Transport Protocol (RTP), Real-Time Streaming Protocol (RTSP), Simple Mail Transfer Protocol (SMTP), Secure Sockets Layer/Transport Layer Security (SSL/TLS), TCP/IP, Secure Real-Time Transport Protocol (SRTP), Bonjour, Simple Network Management Protocol (SNMP),and Secure Shell (SSH) Protocol. Differentiated-services-code-point (DSCP) marking and class-of-service (CoS) marking	
21	Operating Temperature	14° to 122°F (-10° to 50°C)	

S.NO.	Camera Characteristics	Description	Compliance (Yes/No)
22	Certifications Safety	UL60950-1 2nd edition CSA22.2-No.60950-1 IEC/EN60950-1 2nd edition	
23	Certifications EMC-Requirements	CISPR22 Class B ICES-003 EN55022 EN55024 EN61000-3-2/-3-3 Class A	
24	Auto Detection & Configuration	The camera should be automatically discovered and configured when connected to VMS or Network Switch, to set the right network parameters for the video stream on the network .	

8.1.2. HD PTZ Camera Type 2

S. No.	Camera Characteristics	Description	Compliance (Yes/No)
1	Requirement Overview	IP Camera Should allows up to 20x optical zoom while viewing and recording at 1080p resolutions.	
2	Sensor Type	1/2.8" CMOS Sensor	
3	Max Resolution	1920x1080 @ 30fps	
4	Dynamic Range	86db	
5	Lens/Iris	4.7-94mm	
6	Field of View	Horizontal Angle of View : 55.4° (W) – 2.9° (T)	
7	Audio I/O	Audio in x 1	
8	Digital I/O	(3.5-mm miniature jack)	
9		Audio out x 1	
10		(3.5-mm miniature jack)	

S. No.	Camera Characteristics	Description	Compliance (Yes/No)
11		DI x 4	
12		DO x 2	
13	Max Illumination	Color: 0.05 lux	
14		B/W: 0.05 lux	
15	Day/Night	The camera should provides true day/night functionality and includes an IR filter that automatically switches to night mode in low-light scenes. This function can be set to manual, automatic, or scheduled control.	
16	Local Storage	MicroSD	
17	PTZ Speed	Pan speed: 0.05° to 450°/sec Tilt speed: 0.05° to 450°/sec	
18	Video Compression & Video Streaming	● Single-stream H.264 or MJPEG up to 1080p (1920 x 1080) @ 30 fps ● Dual-stream H.264 and MJPEG ◦ Primary stream programmable up to 1280 x 720 @ 30 fps ◦ Secondary stream programmable up to 960 x 544 @15 fps	
19	ONVIF	Should support for ONVIF 2.0 allows for standards based interoperability	
20	Motion Detection	Should be Integrated	
21	External Power	24V AC	
22	Power Consumption (in watts)	Max 20 Watt at PoE+	
23	Environmental Certification	IP66	

S. No.	Camera Characteristics	Description	Compliance (Yes/No)
24	Operating Temperature	-40 to 55°C at High POE	
25	Certifications Safety and Certifications EMC-Requirements	CE, Class A FCC, Class A UL/cUL Listed C-Tick	
26	Auto Detection & Configuration	The camera should be automatically discovered and configured when connected to VMS or Network Switch, to set the right network parameters for the video stream on the network .	

8.1.3. Dome Camera – Type 3

S. No.	Camera Characteristics	Description	Compliance (Yes/No)
1	Requirement Overview	IP Camera should be a high-definition, full-functioned video endpoint with industry-leading image quality and processing power. The camera is capable of resolutions up to 1280 x 960 at 30 frames per second (fps) while optimizing network usage with either H.264 or MJPEG compression. Contact closures allow integration with access control systems.	
2	Max Resolution	1280 x 960 @ 30fps	
3	Dynamic Range	69db	
4	Lens/Iris	3-9mm-DC-Iris	
5	Minimum illumination	● Color mode: F1.4 @ 0.4 lux ● Black and white mode: F1.2 @ 0.2 lux	

S. No.	Camera Characteristics	Description	Compliance (Yes/No)
6	Remote Autofocus	Yes	
7	Field of View	93° to 31.7° (horizontal)	
8		68.4° to 23.8° (vertical)	
9		118.9° to 39.6° (diagonal)	
10	Camera Adjustment	Pan: 350°	
11	Range	Tilt: 80°	
12	Privacy regions	The camera supports up to four user-defined privacy regions. Any video within a privacy region is masked in the video stream.	
13		Rotate: 350°	
14	Audio I/O	Audio in x 1	
15	Digital I/O	(3.5-mm miniature jack)	
16		Audio out x 1	
17		DI x 1	
18		DO x 1	
19	Number of streams	The camera can stream H.264 and MJPEG video simultaneously. Each video stream can be configured with individual resolution, quality, and frame-rate settings, ● Single-stream H.264 or MJPEG up to 1280 x 960 @ 30 fps ● Dual-stream H.264 and MJPEG ◦ Primary stream programmable up to 1280 x 960 @ 30 fps ◦ Secondary stream programmable up to 800 x 600 @ 15 fps	
20	Day/Night	Automatic, manual, scheduled	
21	Local Storage	MicroSD	

S. No.	Camera Characteristics	Description	Compliance (Yes/No)
22	Video Compression	H.264 & Motion JPEG	
23	ONVIF	Profile S	
24	External Power	12V DC	
25		24V AC	
26	Power Consumption	Max 9 Watts at DC	
25	Environmental Certification	IIP67- and IK10-rated housing	
28	Operating Temperature	- 40 to 122°F (-40 to 50°C)	
29	Protocols	Dynamic Host Control Protocol (DHCP), Hypertext Transfer Protocol (HTTP), Secure HTTP (HTTPS), Network Time Protocol (NTP), Real-Time Transport Protocol (RTP), Real-Time Streaming Protocol (RTSP), Simple Mail Transfer Protocol (SMTP), Secure Sockets Layer/Transport Layer Security (SSL/TLS), Transmission Control Protocol/Internet Protocol (TCP/IP), Secure Real-Time Transport Protocol (SRTP), Discovery Protocol, Bonjour, Simple Network Management Protocol (SNMP), and Secure Shell (SSH)	
30	Quality of service (QoS)	Differentiated services code point (DSCP) marking and class of service (CoS) marking	
31	Certifications Safety	● UL60950-1 2nd edition ● CSA22.2-No.60950-1 ● IEC/EN60950-1 2nd edition ●	
32	Certifications EMC-Requirements	: ● CISPR22 Class B ● ICES-003 ● EN55022 ● EN55024 ● EN61000-3-	

S. No.	Camera Characteristics	Description	Compliance (Yes/No)
		2/-3-3 Class A ●	
33	Auto Detection & Configuration	The camera should be automatically discovered and configured when connected to VMS or Network Switch, to set the right network parameters for the video stream on the network .	

8.2. Video Analytics for IP Camera

The System should support Video Analytics at camera edge; these video analytics should enable an IP camera to perform various analytic. Analytic functions trigger events when a camera detects activities or behaviors that match predefined rules. Counting functions count people.

Crowd Monitoring—Camera should provide below features for estimating the size and the relative density of a crowd of people. Bidder has to quote software License as per RFP requirement, however camera should support for below characteristics;

S.NO.	Characteristics and Description		Compliance (Yes/No)
3	Object Size Filters	Yes	
4	Object Density Level	Yes	
6	Flow Violation	Yes	

8.3. City Network Solution

The bidder must ensure Bandwidth & necessary Links at field locations on its own to make the System Live, however the cost will be reimbursed to the successful bidder by UMC authority.

8.3.1. City Network Aggregation Node

S. No.	Technical Specifications	Compliance (Yes/NO)
1	Router should support 64 Gbps of switching capacity	

S. No.	Technical Specifications	Compliance (Yes/NO)
2	The Router shall be standalone fixed configuration Chassis or stackable system with redundant power supply.	
3	A single point failure on the equipment shall not result in network or network management system downtime	
4	Router should support Quality of service for marking, Prioritising and assuring bandwidth Guarantee. Classification can be done based on DSCP, Priority, IP address and 802.1p.	
5	Router should also support RSVP for end to end bandwidth guarantee.	
6	Router should support modular qos with Multilevel Priority Queue along with weighted fair queuing.	
7	Router should also support Policy for control plane protection	
8	The route r should have 4Gb DRAM and 2GB flash	
9	The router should support 12 Mb buffers	
10	The Router should support multilevel priority scheduling for voice and video applications with minimal jitter, latency and packet loss.	
11	The Router shall support fault-tolerant connections to other network or shared media segment to protect against a primary link failure. If the primary link fails, the backup path shall be automatically activated to maintain network connectivity and throughput.	
12	The Router should support the following protocols: BGP,MPBGP,OSPF ,RFC 3107 ,OSPFv2 and v3,Loop free alternate ,IP FRR,6PE,6VPE,VPLS,Layer2 VPN, uRPF, PIMSM and PIM SSM.	
13	The router should support fast convergence protocols like G.8032, IPFRR, MPLS FRR, BGP prefix independent convergence, VRRP or equivalent and BFD for Routing protocols.	
14	The Router should support Point to Point and Point to Multipoint LSP for Unicast and Multicast traffic.	
15	The proposed router shall support 3 level H-QoS	
16	The proposed router shall support Layer 2 and Layer 3 multicast	
17	It shall support Ethernet Ring protection based on ITU-T G.8032 v2	

S. No.	Technical Specifications	Compliance (Yes/NO)
18	It shall support the following protocols:-	
19	The Router shall support both IPv4 and IPv6	
20	The router should suport Internet Group Management Protocol versions 2 and 3 (IGMPv2 and v3) ,IP/MPLS,IP FRR,BGP PIC,MPLS LDP,MPLS TE	
21	The Router should support layer 2 and layer 3 MPLS VPN.	
22	Shall support Frame sizes from 64 bytes to 1600 and to 9216 bytes on all ports	
23	Router shall work as DHCP relay agent	
24	Router should support Eight No of hardware queues are required for per port for flow treatment of traffic, Policy Based QOS, WRED, WFQ, HQOS, Ethernet OAM and Y.1731 performance management	
25	The router should support Zero touch provisioning for ease of management	
26	The Router must support the following security features:-	
27	Security through ACL filters for layers 2 and layer 3 traffic, MAC address limits and storm control for broadcast, multicast and unknown unicast, Authentication, authorization, and accounting (AAA) with TACACS+ and RADIUS,URPF	
28	Operating Environmental Requirements::-40ºC to 65ºC operating temperature and 5 to 95%, noncondensing	
29	Router should support 12 xGE SFP and 2 x 10G Ports. Each loaded 4 x 1G Copper RJ 45 / Copper SFP port, 6 x 1G SFP ports loaded with 1G x LX SFP with 10 Kms range	
30	The proposed router should be EAL4+ or NDPP certified from day one	

8.3.2. Pre-aggregation/Access Switch for Cameras

S. No.	Item	Specifications	Compliance (Yes/NO)
1		The switch should be Industrial Grade ruggedized in nature that provides minimum 8 x 10/100BASETX PoE access ports	

S. No.	Item	Specifications	Compliance (Yes/NO)
		& additional 2 x 1000 BaseX SFP Uplink ports.	
2		Switch should have non-blocking wire-speed architecture with support for both IPv4 & IPv6 from day one with wire rate switching fabric of minimum 8 Gbps or more with forwarding rate of minimum 6 Mpps	
3		Switch have Dual Field Replaceable & upgradable Power Supplies	
4	**Layer 2 Features**	802. 1Q VLAN on all ports with support for minimum 1000 active VLANs & minimum 2k MAC address	
5		Spanning Tree Protocol as per IEEE 802.1d, Multiple Spanning-Tree Protocol as per IEEE 802.1s, Rapid Spanning-Tree Protocol as per IEEE 802.1w	
6		Should support Jumbo frames up to 9000 bytes & Link Aggregation Control Protocol (LACP) as per IEEE 802.3ad.	
7		Switch should support IGMP v1/v2/v3 as well as IGMP snooping.	
8		Static, Inter-VLAN routing must be enabled from day one	
9		Switch should support Dynamic Routing – RIPv1/v2, OSPF for both IPv4 & IPv6, BGP, PBR etc protocol by enabling/upgrading the license.	
10	**Quality of Service (QoS) Features**	Switch should support classification and scheduling as per IEEE 802.1P on all ports with minimum four egress queues per port	
11		Switch should provide traffic shaping and rate limiting features (for egress as well as ingress traffic) for specified Host, network, Applications etc.	
12		Strict priority queuing guarantees that the highest-priority packets are serviced ahead of all other traffic.	
13		Switch should support ACLs, Extended IP ACLs, support RADIUS and TACACS+ for access restriction and authentication.	

S. No.	Item	Specifications	Compliance (Yes/NO)
14		Should support a mechanism to shut down Spanning Tree Protocol Fast-enabled interfaces when BPDUs are received to avoid accidental topology loops.	
15		Switch should support static ARP, Proxy ARP, UDP forwarding and IP source guard, DHCP Snooping, DHCP Option 82, Dynamic ARP Inspection (DAI)	
16		Switch should be SNMP manageable with support for SNMP Version 1, 2 and 3.	
17		Support for Automatic Quality of Service or equivalent for easy configuration of QoS features for critical applications.	
18		Switch should support NTP (Network Time Protocol)], FTP/TFTP	
19		• -40 ºF to 140ºF (-40 to +58ºC) continuous operating temperature range	
20		• -40 ºF to 185ºF (-40 to +80ºC) test under exception conditions short time	
21		• Operating relative humidity: 5% to 95% noncondensing	
22	**Mechanical Conditions:**	Protection Class -minimum IP 20	
23		19" rack-mount design and 1 RU form factor for rack installation and wall mount options.	
24		• Compliance to NEMA TS2 for extended temperature, vibration, shock, surge, and noise environments, UL 60950 or IEC 60950 • Switch shall conform to EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B Standards	
25		EMC interface immunity:	
26		• IEC61000-4-2 [Criteria A], • IEC61000-4-3/ENV50204 [Criteria A], • IEC61000-4-4 [Criteria A]	
27		Electromagnetic emissions certifications:	
28		• EN 61000-6-2, •EN 61000-6-4, • EN 61131-2, • EN 61326-1, • CISPR11	

8.3.3. Access Switch (Indoor)

S. No.	Description	Compliance (Yes / No)
1	19" Rack Mountable stackable switch with min 24 Nos. 10/100/1000 copper input POE ports and additional minimum 2x1G SFP fiber uplink Ports populated with 1G Base-T transceivers from day 1. Switch & transceiver should be from same OEM.	
2	Should support redundant power supplies	
3	Switch should have minimum 52 Gbps of switching throughput & minimum 38 Mpps of forwarding rate.	
4	Switch should have dedicated stacking ports with minimum 80 Gbps of stacking bandwidth (in addition to above asked ports and bandwidth) to put minimum 8 switches into a single stack group. Across stack Ether Channel functionality should be available within the switch itself for high resiliency.	
5	Should have IPv4 & IPv6 Static routes, default routes from day one.	
6	Should support 802.1d, 802.1s, 802.1w & 802.3ad layer 2 protocols	
7	Should support IEEE 802.3az EEE (Energy Efficient Ethernet)	
8	Switch should have feature to protect access ports using port security, TACACS/TACACS+, Radius, storm control, Dynamic ARP Inspection, BPDU and Root Guard security features, Access Control List both port , vlan based.	
9	Should support enterprise class CLI, console, Telnet, SSH and Web Management	
10	Should support RADIUS / TACACS, 802.1x, SNMP versions 1, 2, and 3 from day one	
11	Switch should have minimum of 512MB of internal memory/ DRAM and 128 MB of internal Flash memory	
12	The switch should have IPv6 RA-Guard, DHCP-Guard, Source-Guard features and IPv6 fast-hop security feature	

S. No.	Description	Compliance (Yes / No)
13	Switch should support autoconfig services to determine the level of network access provided to an endpoint based on the type of the endpoint device. Switch also shall have capability to install image etc, with minimal-touch deployment by providing automated image installation and configuration feature when new switches are connected to the network.	
14	Switch shall have functionality to enable automatic configuration of switch ports as devices connect to the switch, with settings optimized for the device type resulting in zero-touch port-policy provisioning. Switch shall have built-in capability for automatic configuration of QoS that allows switch to manage QoS policies based on traffic types resulting in zero-touch traffic engineering.	
15	The proposed switch should be EAL4+ or NDPP & the switch OEM should be listed in Gartner Magic Leaders Quadrant from day one	

8.4. Smart Lighting Solution

The solution should be plug and play and should have following capabilities:

S.No.	Minimum required specification	Compliance (Yes/No)
1.	The specific nodes as per the Bill of Material Annexure on the smart street lighting system should be able to give the real time,	
2.	a. Motion sensing capabilities	
3.	b. Ambient light sensing capabilities	
4.	The smart street lighting system should be able to operate at any weather conditions	
5.	The smart street lighting system should be communicating using wireless technology(preferably)	
6.	The smart street lighting system should be able to communicate to the Lighting Operations Management software hosted on the cloud (Preferably)	

S.No.	Minimum required specification	Compliance (Yes/No)
7.	The smart street lighting system should have the capability to receive the instruction from the Lighting Operations Management software and act accordingly	
8.	The Lighting Operations Management software should be able to send commands to the smart street lighting system based on the data analytics to increase/decrease the luminosity as per the Day light and weather conditions if needed.	
9.	The smart street lighting system should be able to operate the lights switch on/off, increase/decrease luminosity as per the command received from the Lighting Operations Management software	
10.	The Lighting Operations Management software should have the capability to apply policies to the smart lighting system.	
11.	Example: set up policies like light up alternate lights during low traffic density, increase the luminosity of the lights as per the dullness of the day lights	
12.	The city administration should be able to see the real time status of the Smart Lighting System on a city map view of the City Infrastructure Management Dashboard.	
13.	The city administration should be able to operate the Smart Lighting System manually too.	
14.	The smart lighting system should be able to communicate the system issue or failure to the Lighting Operations Management software.	
15.	The smart lighting system should have a combination of different type of LED control nodes as mentioned in the bill of materials Annexure.	
16.	The smart lighting system are preferably a combination of LED lights, Luminaire Control node and sensors	
17.	The individual lights are to be monitored by electronic controller using a long range radio frequency communication technology	

S.No.	Minimum required specification	Compliance (Yes/No)
18.	The specific controllers as mentioned in the bill of materials annexure should be able to operate autonomously as per the defined schedules and light level sensors	
19.	The controller should be battery operated in case of a grid failure	
20.	Should provide an external infrared interface for security keys transfer and local configuration	
21.	Should enable Over the Air (OTA) firmware update	
22.	**Technical Specifications of Lighting Management Platform:**	
23.	The rule engine set up on the Lighting Operations Management software should run on the real time data and apply the policies automatically	
24.	At any time, these policies can be overridden by human intervention with the system	
25.	At any point in time, the map view should give the details of the status, luminosity of the lights in city map view	
26.	The data transmitted by and received from the sensors should be encrypted and tamper proof end to end (from sensor to application)	
27.	The system should allow to automatically or manually assign a GPS location to each sensor for placing on a GIS map.	

8.4.1. Luminaire technical specification:

S.No.	Specification	Range/Value	Compliance (Yes/No)
1.	**120W LED**		
2.	ELECTRICAL		
3.	System Wattage (W)	120+/-5%	
4.	LED Wattage (W)	105+/-2%	
5.	AC Input Voltage Range (V)	120-280	

S.No.	Specification	Range/Value	Compliance (Yes/No)
6.	Operating Frequency Range (Hz)	47-53	
7.	Total Harmonic Distortion (%)	<10%	
8.	Power Factor	>0.95	
9.	Over Voltage Protection	Yes	
10.	Under Voltage Protection	Yes	
11.	Short Circuit Protection	Yes	
12.	Open Load Protection	Yes	
13.	Surge Protection (Both CM & DM)	5KV Ext. 10 KV series	
14.	Driver Details	Analog Dimmable driver	
15.	OPTICAL		
16.	LED Make	CREE	
17.	Luminous Flux(Lumen)	10200 lumens	
18.	Luminous Efficacy (Lm/W)	85 lm/w	
19.	Color Temperature Range (K)	5700+/-300	
20.	CRI (Typ.)	>70	
21.	Secondary individual Lens	Yes-provided	
22.	ENVIRONMENTAL		
23.	Working Temp. Range	-10 ° C ~ +45 ° C	
24.	Working Humidity Range	0 - 95%	
25.	Max Recommended Junction Temperature	85 ° C	
26.	Max Allowable Junction Temperature	120° C	
27.	Life Time at Junction Temperature of	50000 Hours	

S.No.	Specification	Range/Value	Compliance (Yes/No)
	85 ° C based on LM-80		
28.	MECHANICAL		
29.	Housing	Aluminium PDC	
30.	Housing dimension (mm)	580x287x108	
31.	Lens	Batwing Profile, PC	
32.	Front Glass	Toughened Glass	
33.	IP Grade	IP 66	
34.	Frame	Aluminium die-cast frame	

8.5. Connected Fleet Solution

8.5.1. Fleet Solution Technical and functional requirement

S.No.	Specification	Description	Compliance (Yes/No)
1	**Overall requirement**	The system should be able to Automatically Locate vehicles as per their real time location on the route.	
2		The system should be able to display route info and location of the vehicle in the passenger information system	
3		Should be able to integrate with the City Digital Management platform with all the available data like Location, route information, Vehicle telemetry information's, Speed etc. The City Digital Management platform should display all these into the central dashboard.	
4		The system should allow programmability, allowing actions to be triggered based on events. e.g. speed metric can triggers API call to ESRI Maps pulling speed limit on the road based on GPS or	

S.No.	Specification	Description	Compliance (Yes/No)
		GTFS location.	
5		All the vehicles will be fitted with GPS Controller and will send information to Central Control room as well as Passenger information displays	
6		The system will essentially comprise of the following	
7		1. On-board GPS Controller node 2. On-board and off- Board Passenger Information System	
8		The passenger information system will display ETA/ETD of the buses	
9	**Controller node**	**Minimum Requirement**	
10		Should be dedicated hardened device with hardened Operating System	
11		The device should have standalone GPS to track real time location of the bus based on GPS coordinates	
12		The device should have dual SIM 3G/4G interfaces to be used as backhaul for sending and receiving data.	
13		The device should have built in 802.11a/b/g/n wireless radio	
14		The device should have VPN capabilities for security of data transmitted.	
15		Apart from the 3G backhaul, the device should have more than 1 no of standard Ethernet interfaces to be connected to other components inside the bus.	
16		The device should be IP41 rated for Vertical fall, water and dust as per IEC-60529	

S.No.	Specification	Description	Compliance (Yes/No)
17		Operational Temperature range -25°C to +60°C	
18		Should support 12V/24V DC power supply	
19		Should be able to Acquire data related to the bus real- time scenarios and transmit it to the control center.	
20		Receive messages and voice communications from the command center.	
21		Data received from controller shall provide following (this is minimum list and actual list may vary depending on requirement finalization):	
22		1. Geographic position of the bus, calculated with the GPS receiver and odometer	
23		2. Service related data: driver number, line, route etc.	
24		3. Real-time Stop information.	
25		4. Current speed.	
26		5. Over speeding alert	
27		An integrated or external interface should be available to collect vehicle telemetry data and send all the data real time to the central control center.	
28		The controller should have adequate intelligence and programmability to run custom edge applications and analytics on the edge device.	
29		The controller should have embedded storage and compute and should offer SDK for custom tools and application portability into the same.	
30	**Bus & bus stop PIS System**		
31		Route related information should be available on the PIS display screen inside the bus.	
32		The display should be standard LCD/LED display supporting alphanumeric, digital and multimedia	

S.No.	Specification	Description	Compliance (Yes/No)
		content.	
33		The display should preferably be within 26'	
34		GPS triggered next stop display on Inner sign with synchronized voice announcement.	
35		Emergency 'stop'/Panic function-by pressing an emergency switch placed anywhere in the bus the inner sign should display 'stop' message and buzzer located near the driver makes the sound alerting the driver to stop the bus.	
36		Activation of the Emergency/Panic button should send alert to the central control room during such event.	
37		The PIS system in the bus stops should display the Route information and the ETA information of the buses.	
38		It should be possible to use the same display to be used for pushing digital contents like Promotional video/Ad content etc, as and when needed.	
39		There should be an IP based Camera installed inside the bus for Monitoring as well as sending crowd information to the central control center.	
40	**Software Platform Features**	The central Software platform should be able to receive all the real time information of the buses as below	
41		1. Location of the vehicles 2. Speed of the vehicles 3. Route information of the vehicles 4. Should be able to plot all the vehicles in the city map as per their real time locations 5. Should be able to plot vehicle telemetry data on the control room dashboard	
42		The system should support integration with Web as well as non web sensor interfaces	

S.No.	Specification	Description	Compliance (Yes/No)
43		The platform should offer an Application builder for developing custom Applications as needed.	
44		Should support an Interactive Development Environment that can facilitate in-house expertise to develop widgets and create API extensions on the fly	
45		The platform should be able to integrate with the Central Command and Control center dispatch functions by integrating with the Multichannel communication systems at the Mela control room. This will allow communication with the driver through various channels, like GSM, VHF/UHF radio. IP voice etc.	

8.5.2. IP Camera for Fleet Solution

S.NO.	Camera Characteristics	Description	Compliance (Yes/No)
1	Requirement Overview	IP Camera should be a high-definition, ruggedized, Vibration resistant and Outdoor ready	
2	Max Resolution	1080p (1920 x 1080) at 30 fps	
3	Dynamic Range	69db	
4	Lens/Iris	2.8mm - Fixed Iris	
5	Minimum illumination	● Color mode: 0.5 lux ● Black and white mode: 0.05 lux	
6	Field of View	37.5° to 103.7° (horizontal)	
7		21.6° to 71.2° (vertical)	
8		42.6° to 111.21° (diagonal)	
9	Camera Adjustment	Tilt range: 90° (0°~90°)	

S.NO.	Camera Characteristics	Description	Compliance (Yes/No)
10	Privacy regions	The camera supports up to four user-defined privacy regions. Any video within a privacy region is masked in the video stream.	
11	Number of streams	The camera can stream H.264 and MJPEG video simultaneously. Each video stream can be configured with individual resolution, quality, and frame-rate settings	
12	Local Storage	MicroSD	
13	Video Compression and Video streaming	H.264 & Motion JPEG: ● Single-stream H.264 or MJPEG up to 1080p (1920 x 1080) @ 30 fps ● Dual-stream H.264 and MJPEG ◦ Primary stream programmable up to 1280 x 720 @ 30 fps ◦ Secondary stream programmable up to 960 x 544 @15 fps	
14	ONVIF	Profile 2.0	
15	Powering Camera	The camera should supports Power over Ethernet (PoE) 802.3af	
16	Power Consumption	Max 8 Watts	
17	Environmental	Camera should be Ruggedized, IK10 and IP67-rated housing	
18	Operating Temperature	-13 to 122°F (-25 to 50°C)	

S.NO.	Camera Characteristics	Description	Compliance (Yes/No)
19	Protocols	Dynamic Host Control Protocol (DHCP), Hypertext Transfer Protocol (HTTP), Secure HTTP (HTTPS), Network Time Protocol (NTP), Real-Time Transport Protocol (RTP), Real-Time Streaming Protocol (RTSP), Simple Mail Transfer Protocol (SMTP), Secure Sockets Layer/Transport Layer Security (SSL/TLS), Transmission Control Protocol/Internet Protocol (TCP/IP), Secure Real-Time Transport Protocol (SRTP), Discovery Protocol, Bonjour, Simple Network Management Protocol (SNMP), and Secure Shell (SSH)	
20	Quality of service (QoS)	Differentiated services code point (DSCP) marking and class of service (CoS) marking	
21	Certifications Safety	UL60950-1 2nd edition CSA22.2-No.60950-1 IEC/EN60950-1 2nd edition IEC/EN60825	
22	Certifications EMC-Requirements	CISPR22 Class B ICES-003 EN55022 EN55024 EN61000-3-2/-3-3 Class A EN50121-4 VCCI Class B KN22 Class B KN24	
23	Auto Detection & Configuration	The camera should be automatically discovered and configured when connected to VMS or Network Switch, to set the right network parameters for the video stream on the network.	
24	Activity detection	Camera should support User-definable alerts with configurable sensitivities and thresholds, email alert, and HTTP notifications. Camera should also support for IEEE 802.1X authentication	
25	Dimensions and Housing	Max 6x5x2 inch with Aluminium Housing	
26	OEM Criteria	All proposed Cameras should be from single OEM and OEM should have Registration in India min from 10 Years	

8.5.3. Network Switch for Fleet Solution

S. No.	Item	Specifications	Compliance (Yes/NO)
1		The switch should be Industrial Grade ruggedized in nature that provides total 4 10/100 BaseT ports with additional 2 x 1000 BaseX SFP Uplink ports.	
2		Switch should have non-blocking wire-speed architecture with support for both IPv4 & IPv6 from day one with wire rate switching fabric of minimum 8 Gbps or more with forwarding rate of minimum 6 Mbps. Switch should have minimum 128 MB RAM/DRAM	
3	**Layer 2 Features**	802. 1Q VLAN on all ports with minimum 2k MAC address	
4		Spanning Tree Protocol as per IEEE 802.1d	
5		Should support Jumbo frames up to 9000 bytes & Link Aggregation Control Protocol (LACP) as per IEEE 802.3ad.	
6		Switch should support IGMP v1/v2/v3 & upto 1000 IGMP groups as well as IGMP snooping.	
7		Static, Inter-VLAN routing must be enabled from day one	
8		Switch should support Dynamic Routing – RIPv1/v2, OSPF for both IPv4 & IPv6, BGP, PBR etc protocol by enabling/upgrading the license.	
9	**Quality of Service (QoS) Features**	Switch should support classification and scheduling as per IEEE 802.1P on all ports with minimum four egress queues per port	
10		Switch should provide traffic shaping and rate limiting features for specified Host, network, Applications etc.	
11		Switch should support ACLs, Extended IP ACLs, support RADIUS and TACACS+ for access restriction and authentication.	
12		Should support a mechanism to shut down Spanning Tree Protocol Fast-enabled interfaces when BPDUs are received to avoid accidental topology loops.	
13		Switch should support static ARP, Proxy ARP, UDP forwarding and IP source guard, DHCP Snooping, DHCP	

S. No.	Item	Specifications	Compliance (Yes/NO)
		Option 82, Dynamic ARP Inspection (DAI)	
14		Switch should be SNMP manageable with support for SNMP Version 1, 2 and 3.	
15		Support for Automatic Quality of Service or equivalent for easy configuration of QoS features for critical applications.	
16		Switch should support NTP (Network Time Protocol)], FTP/TFTP	
17		• -40 ºF to 140ºF (-40 to +58ºC) continuous operating temperature range	
18		• -40 ºF to 185ºF (-40 to +80ºC) test under exception conditions short time	
19		• Operating relative humidity: 5% to 95% noncondensing	
20	**Mechanical Conditions:**	Protection Class -minimum IP 20	
21		19" rack-mount design and 1 RU form factor for rack installation and wall mount options.	
22		• Compliance to NEMA TS2 for extended temperature, vibration, shock, surge, and noise environments, UL 60950 or IEC 60950 • Switch shall conform to EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B Standards	
23		EMC interface immunity:	
24		• IEC61000-4-2 [Criteria A], • IEC61000-4-3/ENV50204 [Criteria A], • IEC61000-4-4 [Criteria A]	
25		Electromagnetic emissions certifications:	
26		• EN 61000-6-2, •EN 61000-6-4, • EN 61131-2, • EN 61326-1, • CISPR11	

8.6. Data Center Solution, Emergency Communication System and City Command Control Center

8.6.1. Core Network Switch for Data Center

Item	Specifications	Compliance (Yes/No)
1	Layer-3 Switch. 19" Rack Mountable with minimum 32 no of SFP+ ports so that 1G/10G SFP/SFP+ interfaces can be installed as & when required.	
2	1+1 Redundant and hot swappable, load sharing Power supply &redundant FAN	
3	Two core switches will be connected in 100% redundancy with support for active/active configuration to avoid single point of failure in network.	
4	The Switch Should support atleast 320 Gbps of switching capacity from day one.	
5	The switch should support 48K IPv4 and IPv6 unicast routes, 24K multicast routes, 48K MAC address and 20k ACL	
6	The Switch Should support IEEE 802.1D Spanning Tree Protocol, IEEE 802.1w Rapid Reconfiguration of Spanning Tree, IEEE 802.1s Multiple VLAN Instances of Spanning Tree, IEEE 802.3ad LACP, IEEE 802.1p CoS Prioritization, IEEE 802.1Q VLAN, IEEE 802.1X User Authentication	
7	The Switch Should support MLD Snooping for IPv6 in hardware, Unicast Reverse Path Forwarding for IPv6 in hardware	
8	The Switch Should support Internet Group Management Protocol (IGMP) Snooping, IPv6 Multicast Listen Discovery (MLD), Multicast Listen Discovery snooping, IEEE 802.1AB LLDP	
9	The Switch should have OSPF, RIP, Policy-Based Routing, BGP enabled for both IPv4 & IPv6 from day one	
10	The Switch Should support Unicast Reverse Path Forwarding (Unicast RPF, support distributed and customized approach to event detection and recover, Dynamic Host Control Protocol server (DHCP)	
11	The switch should have IPv6 RA-Guard, DHCP-Guard, Source-Guard features and IPv6 fast-hop security feature	

Item	Specifications	Compliance (Yes/No)
12	The Switch should have 125K IPv4 & IPv6 Routing entries, upto 24K multicast routes, 50K MAC addresses, 128K Security & QoS hardware entries	
13	The switch should support 4 GB Dynamic RAM (SDRAM) & upto 2G flash	
14	Switch should be loaded with 8x1GE ports, 12x10G SFP+ multimode SFP+, 4x10G SFP+ single mode SFP+ & 8x1G single mode SFP from day one.	
15	The proposed switch should be EAL4+ or NDPP & the switch OEM should be listed in Gartner Magic Leaders Quadrant from day one	

8.6.2. PoE Access Switches

S. No.	Description	Compliance (Yes / No)
1	19" Rack Mountable stackable switch with min 48 Nos. 10/100/1000 copper input POE ports and additional minimum 2x1G SFP fiber uplink Ports populated with 1G Base-T transceivers from day 1. Switch & transceiver should be from same OEM.	
2	Should support redundant power supplies	
3	Switch should have minimum 102 Gbps of switching throughput & minimum 74 Mbps of forwarding rate.	
4	Switch should have dedicated stacking ports with minimum 80 Gbps of stacking bandwidth (in addition to above asked ports and bandwidth) to put minimum 8 switches into a single stack group. Across stack EtherChannel functionality should be available within the switch itself for high resiliency.	
5	Should have IPv4 & IPv6 Static routes, default routes from day one.	
6	Should support 802.1d, 802.1s, 802.1w & 802.3ad layer 2 protocols	
7	Should support IEEE 802.3az EEE (Energy Efficient Ethernet)	

S. No.	Description	Compliance (Yes / No)
8	Switch should have feature to protect access ports using port security, TACACS/TACACS+, Radius, storm control, Dynamic ARP Inspection, BPDU and Root Guard security features, Access Control List both port , vlan based.	
9	Should support enterprise class CLI, console, Telnet, SSH and Web Management	
10	Should support RADIUS / TACACS, 802.1x, SNMP versions 1, 2, and 3 from day one	
11	Switch should have minimum of 512MB of internal memory/ DRAM and 128 MB of internal Flash memory	
12	The switch should have IPv6 RA-Guard, DHCP-Guard, Source-Guard features and IPv6 fast-hop security feature	
13	Switch should support autoconfig services to determine the level of network access provided to an endpoint based on the type of the endpoint device. Switch also shall have capability to install image etc with minimal-touch deployment by providing automated image installation and configuration feature when new switches are connected to the network.	
14	Switch shall have functionality to enable automatic configuration of switch ports as devices connect to the switch, with settings optimized for the device type resulting in zero-touch port-policy provisioning. Switch shall have built-in capability for automatic configuration of QoS that allows switch to manage QoS policies based on traffic types resulting in zero-touch traffic engineering.	
15	The proposed switch should be EAL4+ or NDPP & the switch OEM should be listed in Gartner Magic Leaders Quadrant from day one	

8.6.3. Core Routers

S. No.	Item	General Specification	Compliance (Yes/No)
1	Architecture	The router shall facilitate all applications like voice, video and data to run over a converged IP infrastructure along with hardware assisted IPSEC & Network Address Translation (NAT) capability. The	

S. No.	Item	General Specification	Compliance (Yes/No)
		router should also support hitless interface protection or equivalent technology, In-band and out-band management, Software rollback feature, Graceful Restart for OSPF, BGP, LDP, MP-BGP etc.	
		The router line card must support following interface: Fast Ethernet, Gigabit Ethernet, 10G Ethernet	
2	Performance	Backplane Architecture: The back plane architecture of the router must be modular. The back plane bandwidth must be 5 Gbps from day one	
		The Router architecture should have individual dedicated control plane processor and data plane processor modules. Data plane Processor module should be independent of the control plane Processor. Control plane Processor should have support for internal memory to support multiple software images for backup purposes and future scalability.	
		The router should support the IPv4 and IPv6 DUAL-stack in hardware and software. The router should support minimum 250K IPv4 & 250K IPv6 active FIB (Forwarding Information Base) routes from day one so that these routes can be utilized for traffic forwarding	
3	Protocol Support	The router shall have RIPv1, RIPv2, RIPng, OSPFv2 & v3, Policy Based Routing for both IPv4 & IPv6, IP Multicast Routing Protocols to facilitate applications such as streaming, webcast, command & control including PIM SM, PIM SSM, GRE (Generic Routing Encapsulation) Tunnelling & following MPLS features – LDP, Layer2 VPN such as EoMPLS with LDP signalling, Route Reflector (RR), Traffic Engineering with RSVP-TE, Fast Reroute Link Node & Path protection enabled from day one.	
		The router shall support dual stack IPv6 on all interfaces and IPv6 over IPv4 tunnelling.	

S. No.	Item	General Specification	Compliance (Yes/No)
4	QoS Features	The router shall perform traffic Classification using various parameters like source physical interfaces, source/destination IP subnet, protocol types (IP/TCP/UDP), source/destination ports, IP Precedence, 802.1p, MPLS EXP, DSCP and by some well-known application types through Application Recognition techniques. Router should support upto 100K queues with 3 level of hierarchical queues.	
5	Security Feature	The router shall meet the following requirements for security: Access Control List to filter traffic based on Source & Destination IPSubnet, Source & Destination Port, Protocol Type (IP, UDP, TCP,ICMP etc.) and Port Range etc.	
		The router shall have firewall services enabled from day one in hardware on all interfaces with built-in firewall capacity of 1 Gbps for enhanced security to protect the backbone network from malicious activities.	
6	Management	The router must support management through SNMPv1, v2 and v, support RADIUS and TACACS. The router must role based access to the system for configuration and monitoring. The router shall be provided with IETF standards based Netflow version 9 or equivalent feature so that granular traffic analysis can be performed for advanced auditing, usage analysis, capacity planning or generating security telemetry events, also the router shall have SLA monitoring tools to measure state of the network in real time. The SLA operations shall provide information on TCP/UDP delay, jitter, application response time, VoIP MOS score, Packet Loss etc.	
7	Interface Requirements:	Each Router should be provided with 6 x 1 G SFP based ports out of which 3 ports should be Base-T & 3 should have provision to terminate fiber directly using single mode transceivers.	

S. No.	Item	General Specification	Compliance (Yes/No)
8	Certification:	The proposed router should be EAL4+ or NDPP certified from day one	
9	Others	If any of the mentioned features are not supported on the Router Chassis, additional hardware must be proposed from day 1.	

8.6.4. Wireless Controller Primary and HA

S. No.	Technical Specifications	Compliance (Yes/NO)
1	Must be compliant with IEEE CAPWAP or equivalent secure connectivity for controller-based WLANs.	
2	WLAN Controller should support minimum 1500 Access points and 20,000 clients in a single 1 RU chassis.	
3	WLAN controller must have atleast 2 x 10 Gbps of uplink interfaces.	
4	WLC should have licenses floating on two controllers.	
5	Multiple link aggregation (LAG)/ VRRP support to protect against link failures while maintaining the optimal network connectivity	
6	Must support both 1+1 and N+1 redundancy models.	
7	Must support stateful switchover between active and standby controller in a sub second time frame.	
8	Must have feature for stateful recovery without re-authentication of the client in the event of LAN and WLAN infrastructure disruption to deliver a non-stop client session	
9	Must support redundant power supplies.	
10	Must support an ability to dynamically adjust channel and power settings based on the RF environment.	
11	Radio coverage algorithm must allow adjacent APs to operate on different channels, in order to maximize available bandwidth and avoid interference	
12	Must have Automatic 802.11 interference detection, identification, classification, and mitigation. Classification should support a dynamically	

S. No.	Technical Specifications	Compliance (Yes/NO)
	updatable signature library	
13	Must support coverage hole detection and correction that can be adjusted on a per WLAN basis.	
14	Must support RF Management with 40 MHz and 80 Mhz channels with 802.11n & 802.11ac	
15	WLC should support L2 and L3 roaming of IPv6 clients	
16	WLC should support IPv6 access control lists	
17	WLC should support Guest-access functionality for IPv6 clients	
18	Controller performance must remain the same if encryption is on or off for wireless SSIDs.	
19	Should support ability to adjust Delivery Traffic Indicator Message (DTIM) on a per WLAN basis to improve performance for latency sensitive applications.	
20	Should support Management frame protection for the authentication of 802.11 management frames by the wireless network infrastructure.	
21	Should adhere to the strictest level of security standards, including 802.11i Wi-Fi Protected Access 2 (WPA2), WPA, Wired Equivalent Privacy (WEP), 802.1X with multiple Extensible Authentication Protocol (EAP) types, including Protected EAP (PEAP), EAP with Transport Layer Security (EAP-TLS), EAP with Tunnelled TLS (EAP-TTLS), RFC 4347	
22	Controller should have rogue AP detection, classification and automatic containment feature	
23	Controller should be able to detect attacks like Broadcast de-authentication, NULL probe, Wellenreiter from day one for all access points	
24	Controller should have profiling of devices based on protocols like HTTP, DHCP and more to identify the end devices on the network	
25	Must support internal and external web authentication.	
26	Must be able to set a maximum per-user bandwidth limit on a per-SSID basis.	
27	Must support user load balancing across Access Points.	

S. No.	Technical Specifications	Compliance (Yes/NO)
28	Controller must provide Mesh capability for Mesh supported AP.	
29	Must be able to restrict the no. of logins per user	
30	Must be able to dedicate some APs to monitor-only for Intrusion Prevention Services.	
31	Must support client roaming across controllers separated by a layer 3 routed boundary.	
32	Solution proposed must support clients roaming across at least 1500 APs	
33	Should support the ability to schedule AP power on/off for energy savings	
34	Controller Should support L2 Client Isolation so User cannot access each other's devices. Isolation should have option to apply on AP or SSID's.	
35	Should support encrypted mechanism to securely upload/download software images to and from wireless controllers	
36	Must support 802.11e WMM	
37	Should have Voice and Video Call Admission and Stream prioritization for preferential QOS	
38	Controller should have Deep Packet Inspection for Layer 4-7 traffic for user for all traffic across the network to analyses information about applications usage and prioritization	
39	WLC should support web and console based management including SNMP v1,v2,v2c or higher.	
40	Should support port-based and SSID-based IEEE 802.1X authentication.	
41	Should support MAC authentication to provide simple authentication based on a user's MAC address.	
42	WLC Should support Rogue AP detection, classification and standard WIPS signatures.	
43	WLC should be able to exclude clients based on excessive/multiple authentication failure.	
44	Shall support AES or TKIP encryption to secure the data integrity of wireless traffic	

S. No.	Technical Specifications	Compliance (Yes/NO)
45	Shall able to provide an air quality index for ensuring the better performance	
46	Shall able to provide real time chart showing interference per access point on per radio and per-channel basis.	
47	Should support AP location-based user access to control the locations where a wireless user can access the network	
48	Must be able to set a maximum per-user bandwidth limit on a per-SSID basis.	

8.6.5. Wireless IPS Solution

S. No	Minimum Specifications	Compliance (Yes/No)
1	The system shall offer API to integrate mobile App, to integrate proximity based service, like push notification service	
2	The system shall provide location Analytic service that provides real-time live analytic of demographic information	
3	Data must be hosted in private, On-Premise	
4	The system shall support location accuracy of +/- 1~3 meter. Shall not require special Client App	
5	Vendor shall offer BLE Beacon options that supports Multi-tenancy (Multiple UUID per a Beacon Hardware)	
6	The system shall offers analytic dashboard for guest access usage info	
7	The system shall offer HotSpot 2.0-based Online Sign Up portal	
8	Location Service system shall be independent with Network Management System	
9	The system's location service shall provide clustering option for scalable deployment	

S. No	Minimum Specifications	Compliance (Yes/No)
10	Should support non-Wi-Fi detection for off-channel rogues and Containment for both radio	
11	Should support Rogue AP detection, classification and standard WIPS signatures.	
12	should also support threats like:	
13	Broadcast de-authentication frame signatures	
14	NULL probe response signatures	
15	NULL probe resp 1 (precedence 2)	
16	NULL probe resp 2 (precedence 3)	
17	Management frame flood signatures	
18	Assoc flood (precedence 4)	
19	Auth flood (precedence 5)	
20	Reassoc flood (precedence 6)	
21	Broadcast probe flood (precedence 7)	
22	Disassoc flood (precedence 8)	
23	Deauth flood (precedence 9)	
24	Reserved mgmt 7 (precedence 10)	
25	Reserved mgmt F (precedence 11)	
26	Wallenreiter signatures (precedence 17)	
27	EAPOL flood signature	
28	NetStumbler signature	
29	NetStumbler 3.2.0 (precedence 13)	
30	NetStumbler 3.2.3 (precedence 14)	
31	NetStumbler 3.3.0 (precedence 15)	
32	NetStumbler generic (precedence 16)	

S. No	Minimum Specifications	Compliance (Yes/No)
33	Should scans for threats from data serving AP's location	
34	should scans for "AP Impersonation" in multi-AP deployment	
35	should Automatically blacklisting clients based on DoS/MITM attacks	
36	should detect rough clients/ AP on Wired network by querying routers and switches	
37	should support wireless containment using de-authentication	
38	Should support for Off-channel rogue containment	
39	should support rogue location tracking integrated into the controller/NMS	
40	should provide better location accuracy with the use of hybrid Aps	
41	should support historic data retention	
42	should send alerts in the form of emails, syslog and SNMP traps	
43	should support flexible rogue classification	
44	should provide Integrated PCI reports for easy auditing	
45	Automatically blacklist clients based on authentication failures	
46	Automatically blacklist clients based on policy violations	
47	should Detect WLAN spoof attack based on custom rule	
48	should support Wireline and rule based rogue detection	
49	should Wired and wireless rogue correlation	
50	should contain Rogues based on customizable rules	

8.6.6. Wireless Access Point

Sr No	Technical Specifications	Compliance (Yes/NO)
1	Access Points proposed must include radios for both 2.4 GHz and 5 GHz.	
2	Must include dual band antennas to support both the 2.4GHz and 5GHz	

	operations simultaneously from single antenna.	
3	Access Points must be configurable via software to support dual-band OR single-band antennas.	
4	Must support 2X2 multiple-input multiple-output (MIMO) with two spatial streams	
5	Must support data rates up to 300 Mbps.	
6	Must support 40 MHz wide channels on both radios.	
7	Must support 802.11 dynamic frequency selection (DFS)	
8	Access Point should support Wireless Backhaul , point-to-point, point-to-multipoint bridging	
9	Must support Encrypted and authenticated connectivity between all backhaul components	
10	Mesh Nodes shall provide a 'wired' interface for connection to local area networks or backhaul of local clients.	
11	Access Point must incorporate radio resource management for power, channel, coverage hole detection and performance optimization	
12	Access point shall support powering from AC Adapter, DC and POE(802.3at+).	
13	Access point shall support pole, wall, and roof mounting options.	
14	The Access point shall be IP67 rated for dust and water ingress	
15	The Access point shall be rated for operation over an ambient temperature range up to 60°C.	
16	Should have two RJ-45 auto-sensing 10/100/1000 Mbps ports and a console port.	
17	Should be Wi-Fi alliance certified for interoperability with all IEEE 802.11a/b/g/n client devices.	
18	Should support up to 16 SSID profiles per radio and each profile shall be independently configurable for authentication, encryption, VLANs, and QoS levels.	
19	Should support detection & prevention of wireless threats on 2.4GHz & 5GHz frequency bands.	

20	Should support SNMP, CLI, and web-based management interfaces	
21	Should support self-healing, self-optimizing local mesh extending network availability to areas without an Ethernet infrastructure	
22	Must support both centrally controlled mode (configured and updated via wireless controller) and autonomous mode (without controller) which is software selectable	
23	Should support L2 and L3 controller discovery	
24	Should be able to support Band select to shift 5 Ghz clients on less congested 5 GHz band radio.	

8.6.7. Internet Router

Internet links of 500 Mbps capacity with 99.99% availability must be proposed with redundancy at the DC/CC location. UMC will not provide any Connectivity and bidder has to ensure on its own. However UMC will reimburse the cost.

Sr. No	**Item**	**Specification**	**Compliance (Yes/No)**
1	General Requirements	The router should support security, voice, IP routing, IP multicast, QoS, IP mobility, multiprotocol label switching (MPLS), VPNs, and redundant power supply. Router should be NDPP certified.	
2	Hardware and Interface Requirements	Routers should have at least 2 open slots for LAN or WAN modules	
		Router should have minimum 2 10/100/1000 GE ports & 2 SFP based ports.	
3	Performance Requirements	The router should have a minimum performance of upto 500 Mbps	
		Should support other IP Services like GRE tunneling, ACLs, NAT services	
4	Quality of Service (QoS)	Routers should support marking, policing and shaping	
		Routers should support Voice traffic optimization withfeatures like WRED, QoS, & RSVP	

5	Routing Protocol	IPv4 and IPv6 tunneling enabled from day one	
		HSRP/VRRP, Static Routes, RIPv1, RIPv2, RIPng, OSPFv2, OSPFv3, BGP4, MBGP, BFD, Policy based routing IGMP V1/V2/V3, PIM-DM, PIM-SM enabled from day one	
6	IPv4 Multicast features	Router should support IGMP v1/v2/v3, PIM-DM, PIMSM, Source Specific Multicast (SSM) from day one	
		Should support extensive support for SLA monitoring for metrics like delay, latency, jitter, packet loss	
7	System Management and Administration	Support for accounting of traffic flows for Network planning and Security purposes	
		Should support extensive support for SLA monitoringfor metrics like delay, latency, jitter, packet loss	
		Routers should support SNMPv2 and SNMPv3	
		Routers should support Software upgrades	
8	Security features	Routers should support AAA using RADIUS or TACACS+ Routers should support Packet Filters like: Standard ACL, Extended ACL, ACL that can match arbitrary bits of packet bits of a packet at an arbitrary depth in the packet header and payload	
		Routers should support Tunnels (GRE, IPSec)	
9	Built-In troubleshooting	Extensive debugs on all protocols	
		Shall support Secure Shell for secure connectivity	
		Should have to support Out of band management through Console and an external modem for remote management	
		Pre-planned scheduled Reboot Facility	
		Real Time Performance Monitor – service-level agreement verification probes/alerts	

8.6.8. Firewall with Intrusion Detection /Prevention system

S. No	Specifications	Description	Compliance (Yes/No)
1	Hardware Architecture	The appliance based security platform should be capable of providing firewall, IPS and VPN (IPSec) functionality simultaneously from day one. Bidders can position external hardware boxes but they need to comply with the technical specification.	
2		The appliance should support at least 8x 10/100/1000 Gigabit ports from Day one.	
3		The appliance should support at least one 10/100/1000 dedicated management interfaces to configure/manage the firewall policies, perform image upgrades even in case of failure of the data interfaces. Data ports should not be used for management purpose.	
4		The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory.	
5		Firewall should support integrated or external IPS matching the required specifications	
6		Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats.	
7		The appliance should support redundant inbuilt power supplies from day one	
8	Performance and Scalability	Firewall should support at least 2 Gbps of Multi-protocol real-world throughput based on protocols like HTTP, SMTP, FTP, IMAP (Only UDP based performance nos. will not be considered)	
9		Firewall should support at least 900 Mbps of combined Firewall & IPS throughput	
10		Firewall should support at least 1 million concurrent sessions	
11		Firewall should support at least 40,000 new connections	

S. No	Specifications	Description	Compliance (Yes/No)
		per second	
12		Firewall should support processing at least 1,000,000 64 byte packets per second	
13		Firewall should support at least 400 VLANs	
14		Firewall should support Jumbo Frames up to 9000 bytes	
15	Features	Firewall should support IPv4 & IPv6 dual stack functionality to be able to use IPv4 & IPv6 simultaneously	
16		Firewall should support creating access-rules with IPv4 & IPv6 objects simultaneously e.g. Ipv4 source & Ipv6 destination.	
17		Firewall should support operating in routed & transparent mode. Firewall should also support 802.3ad functionality to increase the bandwidth for a segment across different modules	
18		Firewall should support mixed mode with virtual firewalls where virtual firewall should support routed & transparent mode simultaneously.	
19		In transparent mode firewall should support arp-inspection to prevent spoofing at Layer-2.	
20		Firewall should support passing of BPDU's & filtering of non-IP traffic with ether-type ACLs.	
21		Firewall should provide application inspection for DNS, FTP, HTTP. SMTP,ESMTP, LDAP, MGCP, RTSP, SIP, SCCP, SQLNET, TFTP, H.323, SNMP.	
22		Firewall should provide IPv6 application inspection for DNS, FTP, HTTP, SIP, SMTP & IPv6.	
23		Application inspection engine for HTTP should support enforcing conformance to RFC 2616, filtering based on content-type mismatch, HTTP request method, text matching in http request body, maximum HTTP request	

S. No	Specifications	Description	Compliance (Yes/No)
		message body length & more parameters.	
24		Firewall should support static nat, pat, dynamic nat, pat & destination based nat	
25		Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality.	
26		Firewall should support integration with Radius, TACAS+, RSA, LDAP v3 Directory servers, Kerberos, NT server & Local Database.	
27	High Availability & Routing Features	Firewall should support state full failover of sessions in Active/Standby & Active/Active mode.	
28		Firewall should support port bundling functionality for the failover control & date interfaces for provide additional level of redundancy.	
29		Firewall should support the functionality for allowing Asymmetrically Routed Packets in active/active mode.	
30		Firewall should support redundant interfaces to provide interface level redundancy before device failover.	
31		Firewall should support failover of IPv4 & IPv6 sessions.	
32		Firewall should replicate Nat translations, TCP,UDP connection states, ARP table, HTTP connection states, ISAKMP & IPSec SA's, SIP signalling sessions.	
33		Failover function should ensure that the routes learned via dynamic routing protocols are maintained in the standby unit as well.	
34		Firewall should support IPv4 & IPv6 static routing, RIP, OSPF v2 & v3.	
35		Firewall should support PIM multicast routing.	
36		Should support state full failover for OSPF v3.	
37		Firewall should support SLA monitoring for static routes.	

S. No	Specifications	Description	Compliance (Yes/No)
38	IPS & URL Filtering Capabilities	The integrated IPS functionality should provide real-time threat-detection & prevention capabilities	
39		The Firewall with integrated IPS should provide at least 900 Mbps of combined Firewall + IPS throughput with all signatures turned on.	
40		Support for global correlation and provide real-time updates on the global threat environment beyond the perimeter by adding reputation analysis, reducing the window of threat exposure.	
41		provide signature updates through a global intelligence team working 24 hours a day to help ensure that you are protected against the latest threats	
42		Employs full seven layer protocol analyses of network protocols. Should analyse and decode of all major protocols.	
43		Should identify attacks based on observed deviations in the normal RFC behaviour of a protocol or service	
44		IPS should support the capability of multiple virtual sensors/segments to create different IPS policies for different network segments	
45		The IPS should support syslog/SDEE for logging events & support sending events via SMTP & SNMP	
46		Should support regular expressions to match payloads using custom signatures	
47		IPS should support functionality of creating custom signatures internally on box without requiring any external or conversion tools.	
48		IPS should support the functionality for passive OS fingerprinting to determine the OS that the hosts are running in the network.	
49		IPS should support the functionality to detect & block peer-to-peer applications	

S. No	Specifications	Description	Compliance (Yes/No)
50		The integrated IPS should support automatic fail-open & fail-close functionality in case of failure of the inspection engine	
51		The device must support wide range of applications with minimum 2000 application types being supported & URL categories up to 70.	
		More than 100 MN URL must be categorized.	
52		The device should have minimum of 16GB of Memory & 6 Gb of Flash	
53	Certification	The Firewall solution offered must be rated as 'leaders' or 'Challengers' in the latest Magic Quadrant for Firewall published by Gartner.	
		The proposed device should be EAL4+ or NDPP certified from day one	

8.7. IP Phones for Offices

Sr No	Technical Specifications	Compliance (Yes/NO)
1	Should have high-resolution grayscale / monochrome display with minimum 3.5" or higher screen size	
2	Should have an integrated 2-port 10/100/1000 Ethernet switch	
3	Should have minimum 4 or more line keys, 4 or more soft keys	
4	o SIP support for signalling	
5	o Should support Secure Real-Time Protocol (SRTP) for Media encryption and Transport Layer Security (TLS) Protocol Signalling encryption	
6	o Should provide the directory services to the user by displaying the missed, received and dialled call details including the caller ID	
7	o Audio Codec Support: G.711, G.729, G.722	
8	o Should support wideband / high definition voice, speakerphone	
9	o IP Phone and PBX should be from the same OEM	

8.8. Video Phones For Offices And Control Room

S. No.	Technical Specifications	Compliance (Yes/No)
1	Video & Color Screen IP Phone should meet minimum of following technical specifications	
2	Should have high-resolution 640 x 480 pixel or better, backlit Color display with minimum 5" or higher Screen with video Camera	
3	Should have Intuitive user interface and keypad for quick access to all IP phone and video services	
4	Should have an integrated 2-port 10/100/1000 Ethernet switch	
5	Should have minimum 4 or more line keys	
6	Should have minimum 4 or more programmable soft keys	
7	SIP support for signalling	
8	Should support Secure Real-Time Protocol (SRTP) for Media encryption and Transport Layer Security (TLS) Protocol Signalling encryption	
9	Should provide the directory services to the user by displaying the missed, received and dialled call details including the caller ID	
10	Should support IEEE 802.3af PoE and external AC power adapter option	
11	Audio Codec Support: G.711, G.729, G.722	
12	Should support XML based applications	
13	Should support wideband / high definition voice, speakerphone	
14	Should support Bluetooth interface for headsets	

8.9. Video Phones for Officers

S. No.	Technical Specifications	Compliance (Yes/NO)
2	Should have high-resolution (1920 x 1080) colour display with minimum 12" or higher screen size	
3	Should have inbuilt 1080p Full HD camera, speaker, microphone	
4	Should have an integrated 2-port 10/100/1000 Ethernet switch	

S. No.	Technical Specifications	Compliance (Yes/NO)
5	SIP support for signalling	
6	Should support Secure Real-Time Protocol (SRTP) for Media encryption and Transport Layer Security (TLS) Protocol Signalling encryption	
7	Should provide the directory services to the user by displaying the missed, received and dialled call details including the caller ID	
8	Audio Codec Support: G.711, G.729, G.722	
9	Should support wideband / high definition voice, speakerphone	
10	IP Phone and PBX should be from the same OEM	

8.10. IP Call Control System and Citizen Helpdesk

S. No.	Technical Specifications	Compliance (Yes/NO)
1	· The IP telephony system should be a converged communication System with ability to run TDM and IP on the same platform using same software load based on server and Gateway Architecture.	
2	· The system should be capable of supporting analog and IP Telephones. The single IP EPABX system should be scalable to support up to 1,000 end points to achieve the future capacity.	
3	· All the users to be managed in a single database, which is managed centrally, no multiple databases. CLI facility for all users should be provisioned from day 1.	
4	· The system should be based on server gateway architecture with external server running on Linux OS. No card based processor systems should be quoted.	
5	· The voice network architecture and call control functionality should support both SIP & H.323.	
6	· The call control system should be fully redundant solution with no single point of failure and should provide 1:1 redundancy. The solution must provide geographical redundancy by separating the servers over LAN/WAN. i.e. if the server in the main data center fails, the other server, which may be installed at geographically different location over LAN/WAN	

S. No.	Technical Specifications	Compliance (Yes/NO)
	should take over the entire communication network.	
7	· The system to have distributed architecture and the centralized control for all the IP PBX entities in the network.	
8	· The communication feature server and gateway should support IPv6 from day 1 so as to be future proof.	
9	· The system should support Survivable Call Control functionality so that the survivable system at the remote location shall provide fall back call control service in case the remote site loses all connectivity to the main Call Control system placed at data center. It is expected that the survivability call control system will provide a minimal set of essential telephony features to the end-users that could be a subset of the feature that are available from the main call control system.	
10	Call control server should be Intel based hardware with necessary configuration to support the desired expandability. No proprietary hardware will be acceptable.	
11	The system software version offered should be the latest release as on the date of supply of EPABX as available globally.	
12	System should allow direct registration / profile creation of SIP endpoints onto it and perform all functions of Proxy / Registrar / Redirect etc.	
13	Quality of Services (QoS) should be configured to administer the call and ensure voice traffic get priority over normal traffic.	
14	The System should support Call Admission Control to configure number of calls that can be active between locations.	
15	Should support Active Directory integration for directory synchronization and user authentication.	
16	The supplied telephony solution must support logical / tenant partitioning.	
17	**Support for Call Processing and Call Control:**	
18	Should support signalling standards / Protocols – SIP, H.323, Q.Sig	
19	Voice CODEC support - G.711, G.722, G.729, G.729ab	

S. No.	Technical Specifications	Compliance (Yes/NO)
20	Video codecs: H.261, H.263, and H.264.	
21	Video telephony support (H.323 / SIP)	
22	Support for configuration database (contains system and device configuration information, including dial plan)	
23	Having inbuilt administration web based administration. No additional thick client for administration on the Admin PC. Should also support HTTPS for management.	
24	**Security:**	
25	The protection of signalling connections over IP by means of authentication, Integrity and encryption should be carried out using TLS. Encryption of media (voice traffic) must be possible using SRTP.	
26	o Passwords to prevent the possibility of an aggressor to easily read or deduce system or account access password.	
27	o Secure HTTP support for Call Server Administration, Serviceability, User Pages, and Call Detail Record Analysis and Reporting Tool. Should support Secure Sockets Layer (SSL) for directory.	
28	o The administrator logging on to the call control server needs to authenticate by suitable mechanism such as User Login Information and Passwords / Radius Server.	
29	o Phone Security: TFTP files (configuration and firmware loads) are signed with the self-signed certificate of the TFTP server. The Call Server system admin will be able to disable http and telnet on the IP phones	
30	· **System Features:**	
31	o Hunt groups	
32	o Dial-plan partitioning	
33	o The system should support at least 5 digit numbering scheme.	
34	o Distributed call processing	
35	o Hotline and private line automated ring down (PLAR)	
36	o Interface to H.323 gatekeeper for scalability, CAC, and redundancy	

S. No.	Technical Specifications	Compliance (Yes/NO)
37	o Q.SIG (International Organization for Standardization [ISO])	
38	o SIP trunk (RFC 3261) and line side (RFC 3261-based services)	
39	o SIP trunk Call Admission Control (SIP CAC)	
40	o Time-of-day, day-of-week, and day-of-year routing and restrictions	
41	o Distinctive Ringing: The system should provide audibly different station ringing patterns to distinguish between internal and external calls	
42	o IP Phone Address Book Synchronizer—allows users to synchronize Microsoft Outlook or Outlook Express address books with Personal Address Book.	
43	· **User Features for IP Phone users:**	
44	o User should be able to log in from any IP Phone using username and password and all the privilege should extend to that physical IP phone	
45	o Mobility features providing Simultaneous ringing on both Desk phone and GSM Mobile phone. There should be seamless transfer of a live call from Mobile phone to desk phone and vice-versa.	
46	o Should support at least 8 party meet-me conferencing.	
47	o Message-waiting indicator (MWI)	
48	o Abbreviated Dial	
49	o Click to Dial	
50	o Call back busy, no reply to station	
51	o Call park and pickup	
52	o Call status per line (state, duration, number)	
53	o Calling Line Identification (CLID)	
54	o Calling party name identification	
55	o Direct inward dial (DID)	
56	o Direct outward dial (DOD)	

S. No.	Technical Specifications	Compliance (Yes/NO)
57	o Directory dial from phone—corporate, personal	
58	o Directories—missed, placed, received calls list stored on IP phones	
59	o Distinctive ring (on net vs. off net)	
60	o Shared Line support	
61	o Message waiting indication	
62	o Multiple line appearances per phone	
63	o Music-on-hold	
64	o Station volume controls (audio, ringer)	
65	o Transfer	
66	o Video (SIP / H.323)	
67	o Boss-secretary feature support	
68	o On-hook dialing	
69	o Call waiting	
70	o Call Conference	
71	· **Adhoc Conferencing:**	
72	o Call Control System should be configured for multiparty ad-hoc audio / video conferencing using video IP phones. It should support at least 8 party ad-hoc audio / video conferencing and should be sized to support at least 8 such simultaneous conferences. There should not be any segregation between Audio only conference or Video Phone only conference. There could be a scenario, where all the 6 party conferences are Video Phone only conferences. Video Phone Ad-hoc conference should support active speaker to be displayed on all the participants Video Phone.	
73	· **Upgrade Protection for Software Licenses**	
74	o Bidders should include 5 years Upgrade Protection for all the Software Licenses. During this 5 years bidder to provide software upgrade of any major and minor release free of cost.	
75	· **Voice Gateway equipped with 2 PRI ports**	

S. No.	Technical Specifications	Compliance (Yes/NO)
76	o Voice Gateway should support Class-based queuing	
77	o Voice Gateway should support marking, policing and shaping	
78	o The Voice Gateway should have minimum 2 PRI physical ports & be supplied with required no of DSP's for it to be non-blocking. Voice Gateway can be proposed as an additional solution.	

8.11. Multichannel integration for Emergency Communication

S.NO.	Characteristics and Description		Compliance (Yes/No)
1	Performance Requirements	Integrates disparate push-to-talk systems with other voice systems for emergency personnel.	
2		Integrates server, routing, and IP communications elements to provide on-demand incident communications across multiple agencies.	
3		Allows users to monitor and coordinate emergency response across incompatible radio systems and between multiple agencies, jurisdictions, and departments.	
4		Extends existing push-to-talk (PTT) radio channels so that users with a variety of communication devices can participate in an event.	
7	ACCEPTABLE MANUFACTURER	All modules shall be supplied from a single manufacturer	
8	SYSTEM PERFORMANCE	The system shall create virtual talk groups (VTGs) to facilitate Push-to-Talk (PTT) communications between users of multiple types and technologies of Land Mobile Radios with users of PCs, landline phones, cellular and Android phones, and Unified IP phones.	

S.NO.	Characteristics and Description		Compliance (Yes/No)
9		The system shall provide a High Availability option of adding a secondary hot standby server to provide high availability with no single point of failure. If a primary server fails, the secondary server automatically takes over service without communication interruption. The servers can be geographically separated or located together.	
10		The system shall provide Loop Prevention: As multiple dispatchers patch channels together, there is always the possibility of creating a channel loop that causes audio feedback into the communication path. The system should automatically identify potential audio loops and resolve them before they become an issue. Audio channels and talkgroups shall remain clear without feedback.	
11		The system shall provide radio pooling to enable the system administrator to group dispatch radio assets together into logical radio pools. Dispatchers, when accessing specific radio channels, may select specific channels or talk groups. System shall then locate a radio asset and performs tone/serial control without user intervention.	
12		The system shall provide a web service API to integrate System with third party applications, such as Command and Control, Physical Security Information Management (PSIM) and Computer Aided Dispatch (CAD) applications.	
13		The system shall provide an Incident Management administration console to provide a Web-enabled, easy-to-use interface for orchestrating communications across devices, technologies and locations.	
14		The system shall allow the dispatcher to combine resources, including users and channels, to create Virtual Talk Groups (VTGs) and be able to quickly add or remove resources depending on incident status.	

S.NO.	Characteristics and Description		Compliance (Yes/No)
15		The system shall support role-based management to provide compartmentalized functions for personnel who need to perform different roles. When personnel are added to the system, they shall be assigned a role that defines access privileges. The system shall be able to change user profiles at any time. The following roles, including an "all roles" assignment, shall be supported:	
16		System Administrator	
17		Operational Views Administrator	
18		Operator	
19		Dispatcher	
20		User	
21		The system shall provide license management: The administrator shall be able to use the Web-based interface of the server to manage System feature licenses and to support upgrades or feature additions.	
22		The System Server shall provide an audit trail for analysis, critique, and operations management. Detailed activity logging shall allow administrators to determine which user actions were performed and when they were performed.	
23		The system shall provide a powerful and easy-to-use Web interface: Authorized personnel shall be able to access the System Server from any location by using a supported browser and a network connection.	
24		The system shall provide security features including a hardened Linux operating system, strong passwords, password expiration, and user account lockout after the maximum number of invalid login attempts. The system will include the Security Agent software, installed on the server, to detect anomalous application behaviour that could indicate a security breach.	

S.NO.	Characteristics and Description		Compliance (Yes/No)
25		The system shall provide Unified Media Service which is a way to mix audio through a Linux based application tested and certified on the Unified Computing System.	
26		The system shall provide a High Availability media mixing option of adding a secondary hot standby server to provide high availability with no single point of failure. If a primary server fails, the secondary server automatically takes over service with minimum communication interruption. The servers can be geographically separated or located together.	
28		System Server software shall include, as a minimum, the following features/functions/specifications: A. Ability to have a patching function B. Ability to simultaneously select multiple channels at the same time to make a dispatcher outbound Push to talk to all selected channels C. Ability to administer virtual talk groups (VTG). The VTG's shall be capable of being activated and deactivated by the dispatcher or from an external system such as CAD. D. Ability to authenticate between all servers connecting to the system using certificated based PKI methods.	
29	System Policy Engine	Policy Engine Software shall be a Windows program that shall include, as a minimum, the following features/functions/specifications:	
30		Invite notifications: Dispatchers can quickly invite users to join a System VTG with an Invite Notification. The dispatcher can select some or all members of a VTG and, at the touch of a button, initiate an action to notify or dial participants.	
31		Integrated telephony interface: This feature enables personnel using landline and mobile phones to join a VTG, PTT interoperability conference between disparate land mobile radio systems, PSTN phones, IP phones, and PC clients.	

S.NO.	Characteristics and Description		Compliance (Yes/No)
32		Multipurpose policies: Can define flexible, powerful; multipurpose polices using an intuitive, web-based interface, shown in the following figure. Multipurpose polices enable organizations to codify frequently used or pre-planned communications strategies into standard operating procedures.	
33	Dispatch Console	The System Dispatch Console shall be a Windows program that shall include, as a minimum, the following features/functions/specifications:	
34		The System Dispatch Console shall streamline radio dispatch operations and allow organizations to rapidly respond to incidents, emergencies, and facility events.	
35		The System Dispatch Console eliminate communication barriers between land mobile radio systems and devices including mobile phones, landline phones, IP phones, and PC clients, and enable interoperable communications among users of all devices.	
36		The System Dispatch Console shall be an end-to-end radio dispatching solution designed for mission-critical radio communications.	
37		It shall provide dispatchers with situational awareness.	
38		The system shall run on a standard PC platform, and extend existing push-to-talk (PTT) radio channels so that users with a variety of communication devices can participate.	
39		The System Dispatch Console shall provide control of radio resources through an on-screen interface.	
40		It shall allow users to monitor and coordinate emergency response across incompatible radio systems and between multiple agencies, jurisdictions, and departments.	

S.NO.	Characteristics and Description		Compliance (Yes/No)
41		It shall have a separate tab for Virtual Talk Group's, Policies, and Incidents.	
42		It shall have a 10-line dialer where each dispatcher can patch up to 10 phone calls to channels.	
43		It shall have a directory for phone number lists. There shall be a global, local, and personal list (associated to that user only).	
44		It shall have the ability to tear away the parts of the Graphic User Interface (GUI) so that they can be dragged to other screens. The dispatcher can also attach the screen back to the original setting where all the functions are in one application screen.	
45		The GUI shall provide access to all dispatch features, including:	
46		o PTT and monitor up to 50 talkgroups per System Dispatch Console	
47		o Channel patching	
48		o Integrated telephony client for incoming and outgoing calls	
49		o Radio to telephone patching	
50		o Receive and transmit on-screen indicators for channel activity	
51		o Handset, headset, or desktop microphone operation	
52		o Individual channel mute/All mute	
53		o All talk	
54		o Instant recall recording per channel	
55		o Alert tones	
56		o Channel multi-select	

S.NO.	Characteristics and Description		Compliance (Yes/No)
57		o Unit ID/talker ID	
58		o Emergency alert/acknowledge	
59		o Coded/clear channels	
60		• The System Dispatch Console shall provide rich media incident management support, giving dispatchers the ability to consolidate information relating to an incident and instantly share it among participants, enabling the sharing of multimedia data such as the following: o Live video sent from Monitoring cameras, access control gateways, and mobile clients o Archived videos such as YouTube o Photos o Alarm monitoring o Journal and live statuses o Website links to resources such as FEMA and hazardous material databases, standard operating procedures, and maps	
61		The System Dispatch Console shall integrate with any analog or digital radio system, enabling dynamic any-to-any PTT communications.	
62		It shall be compatible with any dispatch operation that requires radio interoperability including public safety, homeland security, emergency operations centers, defense, and physical security environments.	
70	Mobile Client	Access incident-related PTT channels to communicate between responders and radio users.	
78	IP Phone Client	The system shall enable PTT functionality on select models of Unified IP Phones, allowing users to communicate over and monitor broadcast of communication channels with a push of a button.	
80		The system shall provide remote management, allowing the user to manage the System Phone Client securely and remotely through the System Server. This includes configuration changes, new information	

S.NO.	Characteristics and Description		Compliance (Yes/No)
		or resources, privileges, and other updates.	
81		The system shall support multicast connectivity audio.	
82		The system shall include listen-only channels sp that users with the System Phone Client can monitor channels in listen-only mode even if permission to talk is not provided.	
83		The system shall provide for the extension of traditional PTT networks to IP networks extending voice reachability from PTT radio or broadcast networks to Unified IP Phones.	
84		The system shall support multiple channel types so that users have communication access not only to PTT radio channels, but also to broadcast channels or VTGs made up of multiple channels and communication device types.	
85		The system must be capable of uninterrupted communications should the System Server be unavailable, Unified IP Phone users with the System Phone Client must be able to continue to communicate over the selected channel and operate in an offline mode.	
86		Software Requirements: (none additional, but additional licenses are required)	

8.12. Server& Storage

Bidder has to propose required no's of Servers in Blade/Rack form factor as per the application need & bidder design. All necessary hardware, software, licenses & support for the server's should be taken care by the bidder.

For Monitoring solution, minimum storage capacity for all the IP camera's for a duration of 30 days at 15 fps should be considered by the bidder. Redundancy must be proposed for the storage solution. The recorded video should be retained in the server for 30 days & every 30 days the recorded video should be backed up via NAS or Tape Library based backup system, so that at any given point of time last 30 days data should be available in the server & previous 30 days data is available in the to be proposed

backup system.

Bidder must take into consideration minimum 5 blade server's with below minimum configuration for each Blade:

1. 2x2.6 Ghz 8 Core CPU
2. 64 GB Memory with 2133 Mhz capacity
3. 2x600 GB HDD with 10K RPM rating
4. Blade Server & Blade Chassis should have all necessary power, cooling, network connectivity cables etc.

.

8.12.1. Video Monitoring Workstation

Sl. No	Parameter	Minimum Specifications	Compliance (Yes/No)
1	Operating System (OS)	Windows 7 Pro, Ultimate or Enterprise, 64-bit	
2	CPU	Intel Core i7, 3.07 Ghz or Higher	
3	Memory	16 GB DDR3	
4	Graphics Card	Nvidia GeForce GT430 PCIe Nvidia GeForce GTX460 PCIe or faster.	
5	Network connection	Gigabit Ethernet (GigE) network connection required	

8.12.2. Video Management and Recording Software

S.NO.	Characteristics and Description	Compliance (Yes/No)
1	**General Video Management System requirement**	
2	This organization requires an integrated security solution that includes a command and control style operator console; a Linux-based video management software system, standard and high definition IP-based cameras, and system should meet the following requirements.	
3	The Video MonitoringSystem is intended to effectively monitor all the critical operational areas of the locations & fully cover all the access points. The broad objectives of the Video Management System are as	

S.NO.	Characteristics and Description	Compliance (Yes/No)
	follows:	
4	a) Access points monitoring with Motion Detection Alarms	
5	b) Enhancement of operational control by covering critical areas	
6	c) Recording of camera outputs for analyzing critical events	
7	The Video Monitoring System is required to ensure effective Security & Monitoring of an area as well as create a tamper proof record for post event analysis. The Monitoring System shall provide an on-line display of video images on monitors at local security control room & also at any other place as defined for large locations as per requirement.	
8	It should facilitate viewing of live and recorded images and controlling of all cameras by authorized users.	
9	**VMS shall include, as a minimum, the following features/ functions/ specifications;**	
10	a) The Monitoring system shall provide a scalable and reliable platform to enable customized, network-based Monitoring applications.	
11	b) The Monitoringsystem shall be open standard supporting multiple vendor IP cameras and encoder manufacturers within the same system. The system shall support integration of ONVIF compliant cameras.	
12	c) The system shall support digital pan-tilt-zoom on live video. PTZ cameras should allow operators to use PTZ controls to zoom to a specific region in the viewing pane. Operators should select part of the full image and perform the PTZ controls within that region.	
13	d) The system viewing system should be in thick client for local viewing and thin client through http browser for remote viewing. Both thin and thick client shall provide the capability of viewing single or multiple live and archive cameras, control PTZ camera.	
14	e) VMS Review Player should support stand-alone Windows utility that plays video archive clips without a browser. The Review Player should alos support MP4 files into a tamper-proof MPX (tamper proof MP4 file formats) formats.MPX file should include a password that is entered when the file is created. Application should ask the password to open and	

S.NO.	Characteristics and Description	Compliance (Yes/No)
	view the video file.	
15	f) VMS application should mobile application for Andirod & Apple devices such as the iPad and iPhone. App features should include recorded video playback, thumbnail video preview, and user profiles that allow multiple users to share a single device.	
16	g) The proposed Monitoring system can be supported by the existing network infrastructure	
17	h) The System shall support the scalability of additional camera installation beyond the originally planned capacity. One single Video Management system shall be expandable to 10,000 cameras.	
18	i) The proposed video management system shall support deploying the software on Virtual servers, thus minimizing the hardware foot print for the project.	
19	j) The system shall have capability to stream video at remote sites by optimizing the bandwidth on WAN.	
20	k) The System should support automatic discoverey and configuraction, when any camera connect to network, the switch shoud recognizes the camera as a video endpoint, and then uses Smart Port macros to set the right network parameters for the video stream on the network.	
21	l) The system should allow users to access video streams from remote locations that have limited outbound bandwidth. The video should be delivered to multiple users without placing additional load on the remote locations.	
22	m) The System should support Maps integration in future with below feactures;	
23	i. Adding Image Layers to the location map.	
24	ii. Define the location map for each location.	
25	iii. Add cameras to the map images.	

S.NO.	Characteristics and Description	Compliance (Yes/No)
26	iv. Add image layers to the map.	
27	v. Add a Maps Server	
28	vi. System should support raster format images of jpeg/jpg and png file and Vector (shape files)	
29	n) Video Monitorin Storage System – The video Monitorin storage system should support multiple options to store video. Servers, Direct Attached, shall augment server internal storage. The video Monitoring storage system shall store video in loops, one-time archives, or event clips triggered by alarm systems. It shall support for RAID 6 storage.	
30	o) The system shall provide for integration with other software applications through an open and published Application Programming Interface (API). Such applications shall include, but not be limited to, access control, video analytics, and other alarm and sensor inputs.	
31	p) The system should ensure that once recorded, the video cannot be altered; ensuring the audit trail is intact for evidential purposes.	
32	q) All camera recordings shall have camera ID and location or area of recording and shall be programmable by the system administrator with user ID and password.	
33	r) System shall support camera template to define the resolution, frame rate, recording duration, and then apply to a group of cameras. The modification of the template will be reflected to all the cameras under the template.	
34	s) The system shall supports Bulk Action to allow to search and perform administration activities on multiple camera.	
35	t) The system shall support Bulk import of cameras from file such as excel/.csv, or other standard file format. The files shall include camera name, ip address, server, template, location, camera username and password	
36	u) The System should support LDAP (Lightweight Directory Access Protocol) server	
37	**VMS System**	

S.NO.	Characteristics and Description	Compliance (Yes/No)
38	VMS System should have below application/ Console;	
39	***VMS Server Management Console***	
40	a) VMS Server Management Console should use by system administrators to perform infrequent administration tasks on a single physical or virtual machine. For example, use the Management Console to complete the initial server Setup Wizard, monitor system logs and resources, troubleshoot hardware and system software issues, and gather information about the installed hardware and software components.	
41	b) The VMS Server Management Console user interface should available for each instance of system software installed on either a physical server or as a virtual machine.	
42	c) VMS Server Management sytems should support network time protocol (NTP) on server, which automatically sets the server time and date.	
43	d) VMS Server Management Console should support configurable in a high availability (HA) arrangement that should allows a primary server to be paired with additional Failover, Redundant, or Long Term Storage Media Server. These HA servers should support the primary server with hot standby, redundant stream storage and playback, and long term recording storage to help ensure that functionality and recordings are not lost if the primary server goes offline.	
44	***VMS Operations Management Console***	
45	a) The VMS Operations Management Console should have browser-based configuration and administration tool used to manage the devices, video streams, archives, and policies for Video Management System deployment.	
46	b) The VMS Operations Management Console should have below features ;	
47	i. Manage physical devices - Add, configure and monitor the cameras, servers, and encoders that provide live and recorded video.	
48	ii. Manage server services - Configure, enable or disable server services, such as the recording servers that manage video playback and	

S.NO.	Characteristics and Description	Compliance (Yes/No)
	recording.	
49	iii. Monitor video - View live and recorded video, save video clips, search thumbnail summaries of recorded video, use the camera, Pan, Tilt and Zoom (PTZ) controls, or configure pre-defined video Views and Video Walls.	
50	iv. Define recording and event policies - Create recording schedules, define event-triggered actions, configure motion detection, and other features.	
51	v. Monitor system and device health - View a summary of system health for all devices, or device status, alerts and events.	
52	vi. Backup and restore - Backup the system configuration, and optionally include historical data (such as alerts).	
53	vii. The VMS Operations Management Console should support (if required) configurable as a redundant pair for high availability (HA) and system should ensure uninterrupted system access for users and administrators.	
54	***VMS Monitoring Console***	
55	a) VMS monitoring Console application should allow VMS System users to monitor live and recorded video.	
56	b) VMS monitoring Console should below viewing tool features;	
57	**i. Desktop monitoring application**	
58	ü Allows simultaneous viewing of up to 25 cameras per Workspace, and up to 48 cameras per workstation.	
59	ü Create Video Matrix windows for display in separate monitors.	
60	ü View Video Walls.	
61	ü Create unattended workstations.	
62	ü View and manage alerts.	

S.NO.	Characteristics and Description	Compliance (Yes/No)
63	ü View cameras, video, and alerts based on a graphical map should support (if required)	
64	**ii. Web-based configuration and monitoring tool**	
65	ü Allows simultaneous viewing of multiple video panes:	
66	ü View up to 25 cameras with the 64-bit version of Internet Explorer.	
67	ü Add the users, Views and Video Walls available in the desktop application.	
68	ü Configure the camera, streams and recording schedules.	
69	**iii. Desktop video clip player**	
70	ü Simple player used to view video clip files.	
71	**iv. Web-based server console**	
72	ü Should provide basic viewing features for a single stream (Stream A) from a single camera.	
73	c) VMS monitoring Console should have below features;	
74	i. Client Application - A full-featured monitoring application should provide access to the cameras and video from a single screen should include the following workspaces and features:	
75	• Video workspace	
76	• Wall workspace	
77	• Alert workspace	
78	• Maps workspace support (if required)	
79	• Forensic Analysis Tools should support (if required)	
80	ii. Video Player - monitoring application that includes the following monitoring workspaces:	
81	• Video workspace	

S.NO.	Characteristics and Description	Compliance (Yes/No)
82	• Wall workspace	
83	iii. Video Wall Application – This should launches a monitoring application for unattended workstations. Unattended mode allows video monitoring windows to display Video Walls without access to the monitoring console configuration interface. The unattended screens should remain open even is the keyboard and mouse are disconnected, and can (optionally) re-appear when the workstation is rebooted.	
84	iv. Forensic Analysis Tools - VMS monitoring Console should support (if required) below features ;	
85	• Thumbnail Search—Use Thumbnail Search to quickly locate specific scenes or events in recorded video without fast-forwarding or rewinding. Thumbnail Search should display a range of video as thumbnail images, should allow to identify a portion of the recording to review.	
86	• Clip Management—Use Clip Management to view, download and delete MP4 clips that are stored on the server.	
87	• Motion Analysis—Use Motion Analysis to view a summary of motion events for recorded video.	
88	v. Camera Recording Management	
89	• System should have option to Merge Recorded primary & secondary streams. A camera's recordings from Stream A and Stream B should be played through a single timeline. For example, application should record continuous video throughout the night at a lower quality, but also record higher-quality video whenever an event occurs. The video should displayed in a single timeline.	
90	• System should support recording management to view the recordings available on a camera's local storage device (such as an SD card), and copy them to the server.	

8.13. Functional requirement of City Command Center

8.13.1. Integrated Smart City Platform

Smart City Integrated Operations Platform (SCIOP), Role of the Smart City Integration Operations Platform (SCIOP);

S. No.	Characteristics and Description	Compliance (Yes/No)
1.	It is envisaged that the city will implement multiple Smart City cases over a period of time. The potential example Smart City cases are: • Smart Outdoor Lighting • Smart Energy Metering • Smart Water Metering • Public Safety and Safe City Operations • Connected Public Transport • Public Wi-Fi and Urban Service Delivery over Public Wi-Fi • Kiosks for Citizen Information • Citizen Interactive Kiosks for Urban Service Delivery • Environmental Monitoring	
2.	The City administration intends to use operations applications for monitoring and operating each of the above services. While each agency delivering each of these solutions will have their own operations applications individually, the true value of Smart City is delivered when there is a consolidated and integrated view of all of these operations for the administrators. Also, when one agency application is able to use the data and intelligence gathered from operations of other agency, not necessarily controlling other agencies operations, civic services are delivered lot of efficiently and in an informed fashion. An example is that when police come to know about the real time status of outdoor lighting, then they will be better informed on where to concentrate their patrolling on. Or when citizens come to know where there is good possibility of getting a parking in the city center, they don't spend time looking for parking without any knowledge. This way traffic on the roads is reduced. The integrated operations platform is expected to enable such transformation of the city operations.	
3.	The city will deploy various Urban Services in the future For example, if the City wants to deploy Smart Lighting, Smart Parking solutions, water meters, energy meters, environmental sensors etc the proposed solution should have capability to be integrated with all the future hardware & software infrastructure needed for all these future urban services..	

4.	It is expected that this platform Enables the City and its partners to define a standard data model for each of the urban services domains (i.e. Parking, lighting, kiosks etc….) Enables City and/or its partners to write software adaptors based on the API(s) provided by device vendors and have the ability to control, monitor and collect the data from these street devices Normalizes the data coming from different devices of same type (i.e. Different lighting devices, different energy meters etc...) and provide secure access to that data using data API(s) to application developers Provides urban services API(s) to develop operation applications for each of the Urban Services domains. For example, the lighting operator of the City should be able to develop a City Lighting management application based on the API(s) provided by the platform. This lighting application should also have the ability to access data from other domains like environment based on the access control configured in the system. Enables Querying things directly (not data) Enables to take actions on selected things, which could mean distributed workflows Provides ways to define policies that make applications or things respond to external environments Schedule actions to happen at future time points Subscribe to queries Do all of the above based on real-time relationships between things	
5.	The integrated operations platform should also have the following capabilities Create different users and roles for users. For example, a user who has control over the whole platform or user who can only operate parking solution, a user who has access to parking operations but has read only access to lighting data and so on. The platform should allow different roles to be created and assign those roles to different access control policies. Since this platform is being used for managing Cities, the platform should also allow association of users and locations. For example, the platform should allow creation of locations in the system which correspond to various physical locations in the city and allow the	

	admin to associate different users to different locations with the intent that each user can control only services for a location for which has been given access. The platform should have capability to provide access to real time data and historical data from various connected devices for reporting and analytics. The access to data should be highly secure and efficient. Access to the platform API(s) should be secured using API keys.	
6.	Proposed solution should min below integration; Integration with waste management field operation Integration with Water and sanitation services Field operation Integration with Employee Mobile application Integration with Fleet Management Solution	

8.14. Media Player for Digital Content Delivery

Minimum Specifications	**Compliance (Yes/No)**
1. The media player should have High-performance video and graphics capability with hardware acceleration	
2. Interactive experience with touch and multi-touch support, USB, IR, and remote controller options	
3. Optional wireless deployment option with 802.11a/b/g/n support	
4. Should support integration with digital content management system which serves as content delivery and device management platform.	
5. Unified content and device management with management application programming interface (API) for use with various content management system solutions.	
6. Support HDMI up to 1080p @ 60 Hz	
7. Support VGA up to 1080p @ 60 Hz	
8. Should have a compact appliance design that is fan-less, which reduces power consumption	
9. Hardware-accelerated High Definition (HD) and standard-definition (SD) video decoding	

10. Should support MPEG 2 and 4, H.264, and VC-1 hardware decoding up to	
30 frames per second (fps)	
11. Multiple video zoning and planes	
12. Up to two simultaneous HD video streams	
13. MP3, AAC, AC3, PCM, WAV, WMA	
14. Audio in and out interfaces	
15. Audio data rate 32-512 kbps	
16. High-Definition Multimedia Interface (HDMI) audio	
17. 32 GB built-in SSD storage	
18. One no. of SD card slot	
19. Should have Linux based OS or equivalent	

8.15. Operation Center - Command Control Center and Communication System (C4S)

Command Control Center and Communication System should support for software modules

S. No.	Functionality	Description	Compliance (Yes/No)
1.	Convergence of multiple feeds	Assimilate and assess inputs from different sources such as CCTV, Video Analytics, and sensors further to assist with actionable intelligence.	
2.	Command and Control Center Platform	Provide configurable rules with tailored alerts, dashboard visualizations, intelligent role based work flow, response tools and situation collaboration.	
3.	Intelligent Dispatch Center	Assess the common operating picture, identify & dispatch mobile resources available nearby the incident location. Augment resources from multiple agencies for coordinated response.	
4.	Intelligent Operator Console	Provide configurable intelligent operator console based on the jurisdiction, critical area or sensors to monitor as per situation demands for focused Monitoring.	

5.	Remote User Module	Supervisors remotely can access the system and monitor the alerts received, action taken status, response etc.	
6.	Reporting Module	Generate Customized reports based on the area, sensor type or periodic or any other customer reports as per choice of the administrators	
7.	Mass Notification System	Provide a single web based dashboard to send notifications to target audiences using multiple communication methods including voice-based notification on PSTN/Cellular, SMS, Voice mail, E-mail and Social Media	
8.	Social Media & Open Source Intelligence	Provide analytics based on the social media feed collected from the open source intelligence and collate with the monitoring inputs to alert the responders for immediate action on the ground.	
9.	Field Responder Mobile Apps	Provide integrated Mobile Application for Android and Windows for capturing real-time information from the field response team(i.e; the simhastha operational team administered by the mela authority) using Mobile-Standard Operating Procedure.	

8.15.1. Functional requirement of C4S software

S. No.	Specifications	Compliance (Yes/No)
Operator Module		
1	Command Control Center and Communication System (C4S) **operator module** Should have module for any 3rd party applications alerts, like Video Loss Alarm, Loitering, Vehicle counting etc.	
2	Application should provide the following information related to VMS alert: o show the criticality of the alert o Time the alert was created o Description of the alert o Camera which created the alert o It will have provision to facilitate the operator to locate the Camera on GIS map o Provision to close the alert	

3	Application should zoom to the camera location on the map	
4	Application map should open up the submenu with the option for Create Incident, Live Stream, Recorded Stream, Image and Abandon Incident etc.	
5	Application should be able to create incident for the alert	
6	Application should be able to generate unique incident id and tag the recorded video and image to the incident	
7	Application should show the created incident in the Incident Register panel.	
8	Application Incident Register Panel should show the following details of the incident: 1. Incident ID 2. Camera Location 3. Type of Alert 4. Alert Time 5. Trigger option to initiate the SOP 6. Status/ progress of the incident etc.	
9	Application should option to start SOP	
10	Application should be able to generate SOP based on the type of alert and criticality	
11	SOP should help the operator to take action for the created incident and notify through SMS or E-mail to the concerned person for taking immediate action	
12	SOP should help the operator to dispatch the nearest field responder	
13	Application should allow the field responder to perform the following actions through mobile users :- a. Acknowledge the incident b. Update the status of the incident c. View the camera location on the map d. Navigation option provided to reach the incident location e. Able to view video/ image of the incident f. Able to view the live stream of the camera g. Update the Action Taken Report (Audio/ Video/ Image) for the incident	
14	Application should allow the operator to generate Action Taken Report for the Incident to view the complete details of the incident	
15	Application should provide Event Log option to search incidents based on Incident Id, Camera ID, date time etc. to view more details of incident like Alert details, priority, dispatch details, action taken, incident status, recorded video, alert image, etc.,	
16	Command Control Center and Communication System application should support API integration with existing Dial 100 or CCTNS etc.	
17	Application should have option to correlate the extracted message from the social media in future.	
18	Close the Incident by giving proper comments	
GIS Map		
19	All CCTV Cameras should be accessible through the GIS map by using GIS Filters.	

20	Should be able to select any cameras and play the live stream.	
21	The Graphical User Interface of GIS map should clearly reflect all functional and non-functional camera installed.	
Supervisor Operator		
22	Command Control Center and Communication System should provide for authoring and invoking un-limited number of configurable and customizable standard operating procedures through graphical, easy to use interface.	
23	The users should be able to edit the SOP, including adding, editing, or deleting the activities.	
24	The SOP Tool should have capability to define the following activity types: 1. Manual Activity - An activity that is done manually by the owner and provide details in the description field. 2. Automation Activity - An activity that initiates and tracks a particular work order and selects a predefined work order from the list. 3. If-Then-Else Activity - A conditional activity that allows branching based on specific criteria. Either enter or select values for Then and Else. 4. Notification Activity - An activity that displays a notification window that contains an email template for the activity owner to complete, and then sends an email notification. 5. SOP Activity - An activity that launches another standard operating procedure.	
25	It should be possible for the Supervisor to generate reports	
Web Remote Supervisor		
26	It should be possible for the Supervisor to have a overview of the Event based performance through Dashboards	
27	It should be possible for the supervisor to generate event wise action taken report	
28	It should be possible for the supervisor to view the recorded stream and image of the event	
Mass Notification		
29	Provide a single web based dashboard to send notifications to target audiences using multiple communication methods including voice-based notification on SMS,E-mail and Social Media	
30	Provide integrated dashboard with an easy to navigate user interface for managing profiles, groups, message templates and communications	
31	Provide tools to assemble personalized dashboard views of information pertinent to incidents, emergencies & operations of command center	
32	Provide historical reports, event data & activity log. The reports can be exported to “pdf” or html formats.	
33	Provide dashboard filtering capabilities that enable end-users to dynamically filter the data in their dashboard	
Integrated Mobile Application for Field Response Team		
37	Provide integrated Mobile Application for Android and Windows for capturing real-time information from the field response team using Mobile-Standard Operating Procedure.	

38	Field Responder should be able to acknowledge the incident and provide real time updates from the incident site.	
39	Field Responder should be able to view the recorded stream and image of the event	
40	Field Responder should be able to view live stream of the camera	
41	Field Responder should be able to send action taken for the event to the command and Control application	

8.16. Video wall Display for Command Control Center and Communication System

8.16.1. Video-wall Screen

S. No.	Specification Item	Detailed Specification Description	Compliance (Yes/No)
1	**Configuration**	CUBES OF 70" DIAGONAL IN A 3 (C) X 2 (R) CONFIGURATION COMPLETE WITH COVERED BASE STAND	
2	**Cube & Controller**	Cube & controller should be from the same manufacturer	
3	**Reputed Company**	The OEM should be an established multinational in the field of video walls and should have installations around the world	
4	**Chip Type**	1-chip 0.95" Digital micro mirror device	
5	**Resolution**	1920x 1080 native DMD chip resolution	
6	**Light Source Type**	LED light source with separate LED array for each colour (RGB)	
7	**Brightness**	Minimum 700 lumens	
8	**Brightness Uniformity**	≥ 90 %	
9	**Dynamic Contrast**	1400000:1 or more	
10	**Control**	IP based control to be provided	
11	**Remote**	IR remote control should also be provided for quick access	

S. No.	Specification Item	Detailed Specification Description	Compliance (Yes/No)
12	**Screen to Screen Gap**	≤ 1.0 mm	
13	**Screen Support**	Screen should have an anti reflective glass backing to prevent bulging	
14	**Control BD Input terminals**	Input: 2 x Digital DVI	
15		Input: 1 x HDMI	
16		Input: 1 x HD-BaseT	
17		Input: 1 x Display Port	
18		Output: 1 x Digital DVI	
19	**Auto color adjust function**	Should provide auto color adjustment function	
20		Should be sensor based	
21	**Maintenance Access**	Front	
22	**Cube Size**	Each cube should have a screen size of 1550 mm wide and 872 mm high (+-2%)	
23	**Cube control & Monitoring**	Video wall should be equipped with a cube control & monitoring system	
24		Provide video wall status including Source , light source ,temperature, fan and power information	
25		Should provide a virtual remote on the screen to control the video wall	
26		Input sources can be scheduled in " daily", "periodically" or "sequentially" mode per user convenience	
27		System should have a quick monitor area to access critical functions of the video wall	

S. No.	Specification Item	Detailed Specification Description	Compliance (Yes/No)
28		User should be able to add or delete critical functions from quick monitor area	
29		Automatically launch alerts, warnings, error popup windows in case there is an error in the system	
30		User should be able to define the error messages as informational, serious or warning messages	
31		Automatically notify the error to the administrator or user through a pop up window and email	
32		Status log file should be downloadable in CSV format as per user convenience	

8.17. Video-wall Controller & Software

8.17.1. Video Wall Controller

S. No.	Parameter	Indicative Specifications	Compliance (Yes/No)
1	Controller	Controller to control Video wall in a matrix as per requirement along with software's	
2	Chassis	19” Rack mount	
3	Processor options	Single Quad Core Intel® Core™ i7 Quad Core 3.4 GHz processor) or better	
4	OS	Supports 64-bit Operating System Windows 7	
5	RAM Capacity	16 GB or more	
6	HDD	500 GB or more	
7	Networking	Dual-port Gigabit Ethernet	
8	RAID	RAID 1, 5, 10 supports	
9	Power Supply	(1+1) Redundant hot swappable	
10	Cooling	Any Advanced Proven cooling mechanism	

S. No.	Parameter	Indicative Specifications	Compliance (Yes/No)
11	Input / Output support	DVI/HDMI/USB/ LAN/ VGA/SATA port	
12	Accessories	DVD +RW, Keyboard and mouse	
13	Voltage	100-240V @ 50/60 Hz	
14	Redundancy support	Power Supply, HDD, LAN port & Controller	
15	Scalability	Display multiple source windows in any size, anywhere on the wall	
16	Control functions	Brightness / contrast / saturation/ Hue/ Filtering/ Crop / rotate	
17	Universal Inputs	Minimum 2	
18	Formats	DVI /RGB/Component	
19	Input Format	NTSC/ PAL/SECAM	
20	Operating Temperature	10°C to 35°C , 80 % humidity	
21	Cable & Connections	Vendor should provide all the necessary cables and connectors	

8.17.2. Video Wall Management Software

Sl. No	Parameter	Minimum Specifications	Compliance (Yes/No)
1	Display & Scaling	Display multiple sources anywhere on display up to any size	
2	Input Management	All input sources can be displayed on the video wall in freely resizable and movable windows	
3	Scenarios management	Save and Load desktop layouts from Local or remote machines	
4	Layout Management	Support all Layout from Video, RGB, DVI, Internet Explorer, Desktop and Remote Desktop Application	

Sl. No	Parameter	Minimum Specifications	Compliance (Yes/No)
5	Multi View Option	Multiple view of portions or regions of Desktop, Multiple Application Can view from single desktop	
6	Other features	SMTP support	
7		Remote Control over LAN	
8		Alarm management	
9		Remote management	
10		Multiple concurrent client	
11		KVM support	
12	Cube Management	Cube Health Monitoring	
13		Pop-Up Alert Service	
14		Graphical User Interface	
15	Cube ,Controller & Wall Management Software	Cube , Controller and Wall management Software should be from the same manufacturer	
16	Manufacturing	OEM should have a manufacturing setup in India for Video Walls running successfully for the last 3 years or more	
17	Manufacturer Authorisation	The Bidder must be authorised by OEM to bid	
18	Reputed Company	The OEM should be an established multinational in the field of video walls and should have installations in India	

8.18. Cyber Security Solution

S no	*Feature*	*Compliance*

1	*The Cyber Security solution should be appliance based and should offer a minimum throughput of 500 Mbps*	
2	*Appliance should support at least 8-1Gbps ports*	
3	*Appliance should support both Copper and Fibre Interfaces*	
4	*Appliance shall provide a separate management port*	
5	*Appliance should be capable of working in Inline Blocking mode*	
6	*Appliance shall offer both fail-open*	
7	*Appliance should have dual hot-swappable power supplies*	
8	*Solution should be capable of blocking callbacks to CnC Servers*	
9	*Solution should be capable of blocking threats based on both signatures and behavior*	
10	*Solution should be capable of employing an extensive set of contextual information (e.g., pertaining to the composition, configuration, and behavior of the network and its hosts) to improve the efficiency and accuracy of both manual and automatic analysis of detected events.*	
11	*Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.*	
12	*Solution should be capable of blocking threats on the following protocols: HTTP, HTTPS, SMTP, IMAP, POP3, FTP & NetBIOS-ssn*	
13	*The solution should be capable of inspecting MS Office Documents, Portable Documents, Archive Files, Multimedia Files and executable binaries*	
14	*The solution should be capable of protecting against spear phishing attacks*	
15	*The solution should have blocked at least 99% of threats in the NSS Labs Breach Detection test*	
16	*The solution should be capable of exempting specific hosts from specific compliance rules and suppressing corresponding compliance events and alerts.*	
17	*The solution should be capable of whitelisting trusted applications from being inspected to avoid business applications from being affected & in turn productivity*	
18	*The Solution should provide visibility into how network bandwidth is consumed to aid in troubleshooting network outages and detecting Advanced Malware related DoS & DDoS activity from within the network*	

Note: All the above technical specification mentioned in Section 8 under "Formats for Compliance to the Benchmark / Minimum Specification" section should be of equivalent/ better specs

Annexure-D Format of JV

9. Format for Joint Venture (J.V.) – Annexure-D

If J.V. is allowed following conditions and requirements must be fulfilled -

1. Bids submitted by a joint venture of two or more firms as partners shall comply with the following requirements:
   a. one of the partners shall be nominated as being *Lead Partner,* and this authorization shall be evidenced by submitting a power of attorney signed by legally authorized signatories of all the partners;
   b. the bid and, in case of a successful bid, the Agreement, shall be signed so as to be legally binding on all partners;
   c. the partner in charge shall be authorized to incur liabilities and receive instructions for and on behalf of any and all partners of the joint venture and the entire execution of the contract, including payment, shall be done exclusively with the partner in charge;
   d. all partners of the joint venture shall be liable jointly and severally for the execution of the contract in accordance with the contract terms, and a statement to this effect shall be included in the authorization mentioned under [c] above, as well as in the bid and in the Agreement [in case of a successful bid];
   e. The joint venture agreement should indicate precisely the role of all members of JV in respect of planning, design, construction equipment, key personnel, work execution, and financing of the project. All members of JV should have active participation in execution during the currency of the contract. This should not be varied/modified subsequently without prior approval of the employer;
   f. The joint venture agreement .should be registered, so as to be legally valid and binding on al! partners; and
   g. a copy of the Joint Venture Agreement entered into by the partners shall be submitted with the bid.
2. The figures for each of the partners of a joint venture shall be added together to determine the Bidder's compliance with the minimum qualifying criteria required for the bid. All the partners collectively must meet the criteria specified in full. Failure to comply with this requirement will result in rejection of the joint venture's bid.
3. The performance security of a Joint Venture shall be in the name of the partner ***Lead*** Partner/joint venture.
4. Attach the power of attorney of the signatory[ies] of the bid authorizing signature of the bid on behalf of the joint venture
5. Attach the agreement among all partners of the joint venture [and which is legally binding on all partners], which shows the requirements as indicated in the Instructions to Bidders'.

6. Furnish details of participation proposed in the joint venture as below;

DETAILS OF PARTICIPATION IN THE JOINT VENTURE

PARTICIPATION DETAILS	*FIRM 'A' (Lead Partner)*	*FIRM 'B'*	*FIRM 'C*
Financial			
Name of the Banker(s)			
Planning			
Construction Equipment			
Key Personnel			
Execution of Work (Give details on contribution of each)			

10. Format for Organizational Details – Annexure-E

(To be enclosed with technical proposal)

S. No.	Particulars	Details
1.	Registration number issued by Centralized Registration System of Govt. of M.P. or Proof of application for registration.	
2.	Valid Registration of bidder in appropriate class through Centralized Registration of Govt. of MP	Registration No. Date (Scanned copy of Registration to be uploaded)
3.	Name of Organization/ Individual	
4.	Entity of Organization Individual/ Proprietary Firm/ Partnership Firm (Registered under Partnership Act}/ Limited Company (Registered under the Companies Act-1956)/ Corporation/ Joint Venture	
5.	Address of Communication	
6.	Telephone Number with STD Code	
7.	Fax Number with STD Code	
8.	Mobile Number	
9.	E-mail Address for all communications	
	Details of Authorized Representative	
10.	Name	
11.	Designation	
12.	Postal Address	
13.	Telephone Number with STD Code	
14.	Fax-Number with STD Code	
15.	Mobile Number	
16.	E-mail Address	

Annexure-F Average Annual Turnover

11. Format for Financial Capability of the Consultant – Annexure-F

(Equivalent in Rs. crores)

Name of Firm					
FY	**2012-13**	**2013-14**	**2014-15**	**Total**	**Average**
Annual Turnover					
Net Profit					

Certificate from the Statutory Auditor

This is to certify that .....(name of the Consultant) has received the payments and earned net profit shown above against the respective years.

Name of the audit firm:

Seal of the audit firm

Date:

(Signature, name and designation of the authorised signatory)

Annexure-G List of Key Personnel

12. Format for Technical Personnel – Annexure-G

(As per the requirement of scope of work)

S. No.	Name of Personnel	Key Position	Qualification	Age	Similar work experience	Total Work Experience

Note: The above list of key personnel provided by the bidder shall have the specialised experience as per the requirement of Scope of work.

13. Formats of Commercial Bid – Annexure-H

13.1. Summary of all Cost Components

S.No.	Solution Type	Ref. Schedule
A	IP Camera based Monitoring solution	**Part A**
B	City Network Solution	**Part B**
C	Smart Lighting Solution	**Part C**
D	Connected Fleet Solution	**Part D**
E	Data Center Solution, Emergency Communication System and City Command Control Center	**Part E**
F	Outdoor Wireless Coverage for Employee App across Mela Area	**Part F**
G	**Total (A+B+C+D+E+F)**	
H	**Total Cost for Required Services with Operation and Maintenance Cost for additional 4 Yrs Warranty Support & Maintenance**	
	GROSS TOTAL (G+H)	

The evaluation of Bids will be done against Price Mentioned at Gross Total.
The Prices should be inclusive of all Taxes, duties, Service Tax etc.
Prices for additional 4 years support and mainrenance will be paid quarterly at the end of each quatrter after initial one year warranty is over.
For All the items specification mentioned in this RFP , material supplied should comply or / better and equivalent specs will also be accepted.

Annexure-I Team Plan

The expected minimum inputs for the key team members are provided below. However as per bidder's assessment of the scope of work, bidders may include additional team members as well as additional inputs of the key team members, as considered necessary.

Experts Title	No.	Qualifications & Skills	Experience	Total Person Months
Team Leader	One	• MCA / B.E/B.Tech / Post Graduate degree in IT • Excellent IT Project Management Skills • Good communications and inter personal skills and fluency in written and spoken Hindi and English	• At least 10 years experience on large IT projects • Managed similar projects for at least 7 years Extensive exposure to government projects	12
Project manager	One	• MCA / Post Graduate in any discipline with diploma / degree in IT/ BE/Btech with MBA • Excellent IT Project Management Skills • Good communications and inter personal skills and fluency in written and spoken Hindi and English	• At least 7 years experience on large IT projects • Managed similar projects for at least 5 years • Extensive exposure to government projects	12
Networking & IT Infrastructure Specialist	One	• MCA/ B Tech / M Tech in IT • Excellent skills in designing city wide networks • Extensive experience of defining hardware specifications • Experience of installation and configuration of Servers, routers and other networking devices	• At least 5 years experience on large IT projects • Worked in a similar capacity for at least 3 years	12

Experts Title	No.	Qualifications & Skills	Experience	Total Person Months
FMS Specialists	Two	• Post Graduate in any discipline with diploma / degree in IT • Certified for Hardware/ Operating system/ Networking • Good communications and inter personal skills and fluency in written and spoken Hindi and English • Knowledge of MP an advantage	• At least 5 years experience on providing FMS services • Worked in a similar capacity for at least 2 years • Extensive exposure to government projects	48

Note: All members of the team mentioned above should be in the field in person for the minimum period mentioned in the above table. The bidders will increase any inputs requirement or add any additional position as per the Go live support and maintenance Plan proposed by the bidder. Bidders will submit the timesheets of the people deployed on the project every month.

13.2. Costing of all solutions

13.2.1. Part A- IP Camera based Monitoring solution including Installation

S. No.	Product Description	Make/Model	Qty	Price Per Unit with one year warranty (INR)	Total (INR)
1	State Road/Traffic Monitoring - HD Fixed Camera Type 1		32		
2	State Road/Traffic Monitoring -with PTZ functionality- HD PTZ Camera Type 2		16		
3	Indoor and Control Room Monitoring - Dome Camera - Type 3		4		
4	Zonal Office (Qty-6) and Sector office MOnitoring - Dome Camera - Type 3		28		

S. No.	Product Description	Make/Model	Qty	Price Per Unit with one year warranty (INR)	Total (INR)
5	Video Analytics for IP Camera		32		
6	Field Network Switch with 4 Port POE Switch with 2 Fiber Port		16		
7	Backup Solution (NAS/Tape based) with adequate disk space & interfaces		1		
8	Video Management Server with necessary storage with redundancy		2		
7	Fixed Camera Housing and Mounting		32		
8	Poles as specified dia > 6 INCH ,concrete filled ,with gi wire inside pole for camera cables. Height 10 meters above ground ,1 meter below ground . Material of pole :GI (For PTZ Camera)		16		
9	Poles as specified dia > 6 INCH ,concrete filled ,with gi wire inside pole for camera cables. Height 6 meters above ground , 1 meter below ground . Material of pole :GI (For Fixed Camera at Boundary)		16		
10	Supply & Laying of Cable and other passive components including fibre, PVC, HDPE Pipe, Outdoor Enclosure, Network Rack with accessories etc.		80		
11	Online UPS with 30 Mins backup for Cameras. (Bidder has to size UPS capacity)		16		
12	Project Management Cost		1 job		
13	4 Yr AMC & Maintenance Contract				
	Total				

13.2.2. Part B- City Network Solution including installation

S. No.	Product Description	Make/Model	Qty	Price Per Unit with one year warranty(INR)	Total (INR)
1	City Network Aggregation Node		30		
2	Pre-aggregation/Access Switch for Cameras		40		
3	Access Switch (Indoor)		28		
4	Plugable optics		80		
5	Plggables Optics		40		
6	Pluggable optics		56		
7	Outdoor enclosures		40		
8	4 Yr AMC & Maintenance Contract				
	Total				

13.2.3. Part C- Smart Lighting Solution including installation

S. No.	Product Description	Make/Model	Qty	Price Per Unit with one year warranty support(INR)	Total (INR)
1	Individual Light Control Solution		1,200		
2	Wireless Access Points		50		
3	Software subscription Services		1		
4	120 Watt LED Light		1200		
5	Supply & Laying of Cable and other passive components including PVC, HDPE Pipe, Power Cable, Network Cable with required accessories etc. as		1 Job		

	required				
6	4 Yr AMC & Maintenance Contract				
	Total				

13.2.4. Part D- Connected Fleet Solution including installation

S. No.	Product Description	Make/Model	Qty	Price Per Unit (INR) with one year warranty	Total (INR)
1	Bus Router 3G/4G/WiFi		50		
2	Monitoring Camera for Bus		50		
3	Digital Media PlayerHardware		150		
4	Digital Media Client Software		150		
5	Fleet Management Application		1		
6	Fleet Management Database & Other required Software		1		
7	20" LED Screen/Panel for Signage in buses		50		
8	LED/Digital Signage in Bus Stops		100		
9	Required Vehicle Interface Hardware		50		
10	Digital Signage Content Related Integration Charges		1		
11	Fleet Management Application and Digital Signage Integration as required		1 job		
12	Wireless Access points for Bus Stops		50		
13	4 Yr AMC & Maintenance Contract				

S. No.	Product Description	Make/Model	Qty	Price Per Unit (INR) with one year warranty	Total (INR)
	Total				

13.2.5. Part E- Data Center Solution, Emergency Communication System and City Command Control Center including installation

S. No.	Product Description	Make/Model	Qty	Price Per Unit (INR) with One year Support	Total (INR)
1	Core Network Switch for Data Center		2		
2	Access Switches		4		
3	Core Routers		2		
	Internet Router		2		
	Server		5		
4	Wireless Controller Primary		1		
5	Wireless Controller for HA		1		
6	Firewall with Intrusion Detection /Prevention system		2		
7	IP Phones for Offices		56		
8	IP Phones for Operator		30		

S. No.	Product Description	Make/Model	Qty	Price Per Unit (INR) with One year Support	Total (INR)
9	Video Phones for offices and Control Room		30		
10	IP Call Control System and Citizen helpdesk		1		
11	Multichannel integration for Emergency Communication System		1		
12	Failover Server Requirement (N:1)		1		
13	Cyber Security Items		2		
14	Monitoring Workstations with OS & Video Wall Software		1		
15	Video Operation, Control, Management, Recording, Mobile User application and Processing Software up to 500 Cameras at 2 Mbps/Camera		1		
16	3rd Party Cameras License for connection with VSM		20		
17	Digital Media Player for content distribution, management and Required Client license		10		
18	Fleet management Solution		1		
19	Integrated Smart City Management Platform & Smart City Services As per RFP Requirement		1		
19.1	Integration with waste management field operation		1		

S. No.	Product Description	Make/Model	Qty	Price Per Unit (INR) with One year Support	Total (INR)
19.2	Integration with Water and sanitation services Field operation		1		
19.3	Integration with Employee Mobile application		1		
19.4	Integration with Fleet Management Solution		1		
20	Operation Center - Command Control Center and Communication System (C4S) Base Software for 10 Operators		1		
21	Monitoring Solution Integration Gateway for Cameras and Instant video/Image incident report (200 Cameras)		1		
22	Base Integration Gateway Smart City Services (SOP and Alert base Workflow Management module)		1		
23	Integration Gateway for Emergency Communication Application & IP Telephony		1		
24	Mobile Client Access License (20 users)		1		
25	GIS 2D/GIS Software Integration		1		
26	Integration Module for Video Wall		1		
27	Video wall Display for Command Control Center and Communication System		1		
28	3 Screen –Operators Client Workstations for Command Control Center and Communication System		5		

S. No.	Product Description	Make/Model	Qty	Price Per Unit (INR) with One year Support	Total (INR)
29	2 Screen – Video Monitoring Operators, Major Services- Waste Management, Lighting, Emergency Communication System		15		
30	1 Screen – Admin Operators		2		
31	War Room/Meeting Room/Training room (5 Sitting Capacity)		1		
32	On line UPS 20 KVA with 1 hr backup (At Control Room)		2		
33	Data Center Site Preparation		1		
34	Suitable rack solution for stacking Servers having complete electrical connections		1		
35	Multi-Function Laser Printer		2		
36	Control Room Site Preparation covering Partitioning, Enclosures , Earthing, Power Cabling etc (safety)		1		
37	Cubicles with Table and Chair for operators (As required) - for 25 operators		25		
38	Project Management as required		1 job		
39	4 Year AMC and Maintenance contract				
	Total				

13.2.6. Part F- Outdoor Wireless Coverage for Employee App across Mela Area

S. No.	Product Description	Make/Model	Qty	Price Per Unit with 1 Yr Warranty (INR)	Total (INR)
1	Wireless Access Point		200		
2	4 Yr AMC & Maintenance Contract		-		
	Total				

Note: Bidder has to mention Unit rate againast each item. For additional items UMC reserves the right to increase or decrease the quantity based on the actual requirement & bidder has to supply the defined quantity of equipments at the offered unit rate. All items provided should be under Insurance & all the prices to be included of all taxes. The Insurance should be for entire duration of the Project for 5 Years and comprehensive covering damages for Theft, Fire, Natural Calamities, Riots and Terrorists activities etc.

Annexure-I - LoA

14. Format for LoA – Annexure-I

To,
M/s.
(Name and address of the contractor)

Subject:
(Name of the work as appearing in the bid)

Dear Sir (s),
Your bid for the work mentioned above has been accepted on behalf of the Governor of Madhya Pradesh at your bided percentage below/ above or at par the Bill of Quantities and item wise rates given therein.
You are requested to submit within 15 (Fifteen) days from the date of issue of this letter:

a. the performance security/ performance guarantee of Rs. (in figures) (Rupees in words only).

The performance security shall, be in the shape of term deposit receipt/ bank guarantee of any nationalized / schedule commercial bank valid up to three months after the expiry of defects liability period.
b. Sign the contract agreement.
Please note that the time allowed for carrying out the work as entered in the bid is _____ months including/ excluding rainy season, shall be reckoned from the date of signing the contract agreement.

Signing the contract agreement shall be reckoned as intimation to commencement of work and no separate letter for commencement of work is required. Therefore, after signing of the agreement, you are directed to contact the Engineer-in-charge for taking the possession of site and necessary instructions to start the work.

Yours Faithfully
Additional Commissioner

15. Format for Performance Security – Annexure-J

To

[name of Employer] [address of Employer]

WHEREAS _____[name and address of Contractor] (hereinafter called "the Contractor") has undertaken, in pursuance of Letter of Acceptance No. _____ dated _____ to execute _____ [name of Contract and brief description of Works] (hereinafter called "the Contract").

AND WHEREAS it has been stipulated by you in the said Contract that the Contractor shall furnish you with a Bank Guarantee by a recognized bank for the sum specified therein as security for compliance with his obligation in accordance with the Contract;

AND WHEREAS we have agreed to give the Contractor such a Bank Guarantee:

NOW THEREFORE we hereby affirm that we are the Guarantor and responsible to you on behalf of the Contractor, upto a total of [amount of guarantee]*

(in words) , such sum being payable in the types and proportions of currencies in which the Contract Price is payable, and we undertake to pay you, upon your first written demand and without cavil or argument, any sum or sums within the limits of

__amount of guarantee] as aforesaid without your needing to prove or to show grounds or reasons for your demand for the sum specified therein.

We hereby waive the necessity of your demanding the said debt from the contractor before presenting us with the demand.

We further agree that no change or addition to or other modification of the terms of the Contract of the Works to be performed thereunder or of any of the Contract documents which may be made between you and the Contractor shall in any way release us from any liability under this guarantee, and we hereby waive notice of any such change, addition or modification.

This guarantee shall be valid until 3 (three) months from the date of expiry of the Defect Liability Period.

Signature and Seal of the guarantor Name of Bank

Address

Date

* An amount shall be inserted b y the Guarantor, representing the percentage the Contract Price specified in the Contract including additional security for unbalanced Bids, if any and denominated in Indian Rupees.

16. Service Level Agreement

Enclosed At Annexure-I

17. Draft Standard Contract Agreement

Enclosed At Annexure-II