



## *Home Department, Government of Gujarat*



### *“Safe & Secure Gujarat” – SASGUJ Project*

Request for proposal (RFP) for selection of  
Implementing agency for Supply, Installation and  
Operations & Maintenance of State Wide  
Surveillance and ITMS project across the State of  
Gujarat

(RFP No: GIL/Home Dept./SASGUJ Project/2017-18)

**Bid issued by:**



**Gujarat Informatics Ltd**

Block no. 1, 8th floor, Udyog Bhavan, Sector-11, Gandhinagar-382017,  
Gujarat, Ph No. 23259237, 23259240 Fax: 23238925 [www.gil.gujarat.gov.in](http://www.gil.gujarat.gov.in)

## **DISCLAIMER**

The information contained in this Request for Proposal (RFP) document or subsequently provided to Bidder(s), whether verbally or in documentary or any other form by or on behalf of the Home Department, Government of Gujarat or any of their employees or consultants, is provided to Bidder(s) on the terms and conditions set out in this RFP and such other terms and conditions subject to which such information is provided.

The purpose of this RFP is to provide interested parties with information that may be useful to them in eliciting their financial offers (the "Proposal") pursuant to this RFP. This RFP includes statements, which reflect various assumptions and assessments arrived at by the Home Department, Government of Gujarat, in relation to the RFP. Such assumptions, assessments and statements do not purport to contain all the information that each Bidder may require. This RFP may not be appropriate for all persons, and it is not possible for Home Department, Government of Gujarat, its employees or Consultants to consider the investment objectives, financial situation and particular needs of each party who reads or uses this RFP. The assumptions, assessments, statements and information contained in this RFP, may not be complete, accurate, adequate or correct. Each Bidder should, therefore, conduct its own surveys and analysis and should check the accuracy, adequacy, correctness, reliability and completeness of the assumptions, assessments, statements and information contained in this RFP and obtain independent advice from appropriate sources before filling up the RFP. Any deviation in the specification or proposed solutions will be deemed as incapability of the respective Agency and shall not be considered for final evaluation process.

Information provided in this document to the Bidder(s) is on a wide range of matters, some of which depends upon interpretation of law. The information given is not an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law. Home Department, Government of Gujarat accepts no responsibility for the accuracy or otherwise for any interpretation or opinion on law expressed herein.

Home Department, Government of Gujarat- its employees and advisors make no representation or warranty and shall have no liability to any person, including any Applicant or Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, completeness, delay or reliability of the RFP and any assessment, assumption, statement or information contained therein or deemed to form part of this RFP or arising in any way during the Bidding process.

**SECTION-I**  
**KEY INFORMATION**  
**&**  
**INSTRUCTIONS**

## Important Dates

### **Request for proposal (RFP) for selection of Implementing agency for Supply, Installation and Operations & Maintenance of State Wide Surveillance and ITMS project across the State of Gujarat**

1	Contract Period	5 Years
2	Pre-Bid Meeting	27/04/2017 at 1500 hours Gujarat Informatics Limited, Block No. 1, 8th Floor, Udyog Bhawan, Gandhinagar-382010
3	Bid Due date	16/05/2017 up to 1500 hours
4	Date of Opening of Un-priced bid	16/05/2017 at 1530 hours
5	Date & Time of opening of Technical & Commercial stage	Will be intimated to the qualified bidders at a later date.
6	Venue of opening of Technical & Commercial Bid/s	Gujarat Informatics Limited, Block No. 1, 8th Floor, Udyog Bhawan, Gandhinagar-382010
7	Bid Processing Fees (Non-refundable)	Rs. 15,000/- (Rupees Fifteen Thousand only)
8	Bid security (EMD)	Rs. 4,00,00,000/- (Rupees Four Crores Only)
9	GIL Contact person	DGM (Technical)

#### **1.1 Information Regarding RFP:**

Proposal in the form of BID is requested for the item(s) in complete accordance with the documents/attachments as per following guidelines.

- Bidder shall upload their bids on <https://www.gil.nprocure.com>
- The Bid Security and non-refundable bid processing fees in a separate sealed envelope super scribed with the bid document number to GIL office.
- Bids complete in all respects should be uploaded on or before the BID DUE DATE.
- Technical Bids will be opened in the presence of Bidders' or their representatives who choose to attend on the specified date and time.
- In the event of the date specified for receipt and opening of bid being declared as a holiday for GIL office, the due date for submission of bids and opening of bids will be the next working day at the appointed time.
- Services offered should be strictly as per requirements mentioned in this Bid document.
- Please spell out any unavoidable deviations, Clause/ Article-wise in your bid under the heading Deviations.
- Once quoted, the bidder shall not make any subsequent price changes, whether resulting or arising out of any technical/commercial clarifications sought regarding the bid, even if any deviation or exclusion may be specifically stated in the bid. Such price changes shall render the bid liable for rejection.
- The bid submitted should be valid for a period of 180 days.
- The duration of the Contract period for this activity will be of 5 years.
- In addition to this RFP, the following sections attached are part of Bid Documents.

Section – 1	Key Information & Instructions
Section – 2	Introduction and Eligibility Criteria
Section – 3	Scope of Work
Section – 4	Technical Specification
Section – 5	Instruction to Bidders
Section – 6	Price Bid
Section – 7	Annexures & Formats

## 1.2 Instruction to the bidders for online bid submission:

- Tender documents are available only in electronic format which Bidders can download free of cost from the website [www.gil.gujarat.gov.in](http://www.gil.gujarat.gov.in) and <https://gil.nprocure.com>
- The bids have been invited through e-tendering route i.e. the eligibility criteria, technical and financial stages shall be submitted online on the website <https://gil.nprocure.com>
- Bidders who wish to participate in this bid, will have to register on <https://gil.nprocure.com> such bidders will have to procure Digital Certificate as per Information Technology Act 2000 using which they can Sign their electronic bids. Bidders can procure the same from (n) code solutions – a division of GNFC Ltd., or any other licensed by Controller of Certifying Authority, Govt. of India. Bidders who already have a valid Digital Certificate need not procure a new Digital Certificate.
- Interested and eligible Bidders are required to upload the eligibility related document in eligibility bid section, Technical related document in Technical bid section & Commercial Bid in Commercial bid section. The Bids should be accompanied by a bid security & bid processing fees (non-refundable) as specified in this Bid Document. The Technical & Commercial Bid must be uploaded to <https://gil.nprocure.com> & the Bid Security and bid processing fees must be delivered to the office of Gujarat Informatics Ltd on or before the last date and time of submission of the bid.
- The eligibility section and the Bid Security & bid processing fees section will be opened on the specified date & time in presence of the Bidders or their authorized representative who choose to attend. In the event of the date specified for bid receipt and opening being declared as a holiday for the office of Gujarat Informatics Ltd the due date for submission and opening of bids will be the following working day at the scheduled times.
- In case of any clarifications required, please contact DGM (Tech), GIL in writing 5 days before the Pre-Bid meeting date.

## 1.3 Abbreviations

Abbreviation	Description
ANPR	Automatic Number Plate Recognition
AT	Acceptance Testing
BoQ	Bill of Quantity
CCTV	Closed Circuit TV
CCC	Command and Control Centre
EMD	Earnest Money Deposit
FAT	Final Acceptance Testing
FRS	Functional Requirement Specification
GIL	Gujarat Informatics Limited
GoI	Government of India
GoG	Government of Gujarat
ICT	Information Communication and Technology
IP	Internet Protocol
LoI	Letter of Intent
O&M	Operations and Maintenance
PBG	Performance Bank Guarantee
PoE	Power Over Ethernet
PTZ	Pan, Tilt & Zoom
RLVD	Red Light Violation Detection
RoW	Right of Way
SASGUJ	Safe & Secure Gujarat
SOP	Standard Operating Procedure

SoW	Scope of Work
SRS	Software Requirement Specification
VMS	Video Management System

### DEFINITIONS

In this document, the following terms shall have following respective meanings:

1. "User Acceptance Test (UAT)" means the User Acceptance Testing of the ordered product and services on completion of installation and commissioning as per the requirement.
2. "Acceptance Test Document" means a document, which defines procedures for testing the installed and commissioned product and services against requirements laid down in the Agreement.
3. "Agreement" means the Service Level Agreement to be signed between the successful bidder and the Home Department, Government of Gujarat including all attachments, appendices, all documents incorporated by reference thereto together with any subsequent modifications/changes/corrigendum's, the RFP, the bid offer, the acceptance and all related correspondences, clarifications, presentations.
4. "Authorized Representative/ Agency" shall mean any person/ agency authorized by either of the parties.
5. "TENDERER" here shall mean "Home Department, Government of Gujarat".
6. "Bidder" means any agency who fulfils the requirement laid in the RFP documents and is possess the required expertise and experience as per the RFP document. The word Bidder when used in the pre-award period shall be synonymous with Bidder, and when used after award of the Contract shall mean the successful Bidder with whom TENDERER signs the Service Level Agreement for executing the project.
7. "Center" means Offices of TENDERER
8. "Contract" is used synonymously with Agreement.
9. "Corrupt Practice" means the offering, giving, receiving or soliciting of anything of value or influence the action of a public official in the process of Contract execution.
10. "Default Notice" means the written notice of Default of the Agreement issued by one Party to the other in terms hereof.
11. "Fraudulent Practice" means a misrepresentation of facts in order to influence a procurement process or the execution of a Contract and includes collusive practice among Bidders (prior to or after Bid submission) designed to establish Bid prices at artificial non- competitive levels and to deprive TENDERER of the benefits of free and open competition.
12. "Final Acceptance Test (FAT)" means the acceptance testing of all the commissioned project components at all specified locations.
13. "Go Live Date" means the date on which the FAT of all the project component's as per the Work order has been successfully completed and accepted by the TENDERER.

14. "Good Industry Practice" means the exercise of that degree of skill, diligence and prudence which would reasonably and ordinarily be expected from a reasonably skilled and experienced Operator engaged in the same type of undertaking under the same or similar circumstances.
15. "GIS" shall stand for Geographical Information Systems
16. "Implementation Period" shall mean the period from the date of signing of the Agreement and up to the issuance of Final Acceptance Certificate.
17. "Law" shall mean any act, notification, by-law, rules and regulations, directive, ordinance, order or instruction having the force of law enacted or issued by the Central Government and/ or the Government of Gujarat or any other Government or regulatory authority or political subdivision of government agency.
18. "Lol" means Letter of Intent, which constitutes the intention of the TENDERER to place the Purchase Order with the successful bidder.
19. "Work order" shall mean a formal order issued by TENDERER to the successful bidder covering delivery timelines, SLA and other terms and conditions.
20. "Operator" means the entity/company providing the services / executing the project under the Agreement and is used synonymous with Bidder/Successful Bidder.
21. "O&M Period" means period of 5 years starting with the successful, installation and commissioning and FAT of the project components. The date of start of O&M shall start from the (Go Live) date i.e. from the date of successful FAT of all the equipment at all the site locations as per the work Order.
22. "OEM" Shall stand for Original Equipment manufacturer
23. "PoC" shall stand Proof of Concept.
24. "Period of Agreement" means 5 years' period starting with the commissioning of all Hardware and software ordered as per the Scope of work for the Project.
25. Request for Proposal", means the detailed notification seeking a set of solution(s), services(s), materials and/or any combination of them.
26. "Requirements" shall mean and include schedules, details, description, statement of technical data, performance characteristics, standards (Indian as well as International) as applicable and specified in the Agreement.
27. "Site" means the location(s) for which the Contract will be signed and where the service shall be provided as per agreement.
28. "Service" means provision of Contracted service viz., operation, maintenance and associated services for the Project.
29. "Service Down Time" (SDT) means the time period when specified services/network segments with specified technical and operational requirements as mentioned in this document are not available to TENDERER. The services shall be operational on all days of a year and 24- hours/ day with in the uptime specified in the Service Level Agreement (SLA). The services shall be considered as operational when all

Centers at all tiers/ levels are working, providing all/ specified services as mentioned in full capacity at all locations in the network.

30. "Third Party Agency" means any agency, if/as appointed by TENDERER for monitoring the Project during commissioning and operation.
31. "Termination Notice" means the written notice of termination of the Agreement issued by one Party to the other in terms hereof.
32. "Unplanned downtime" means an instance other than the planned down time in which ordered services are not available to TENDERER.
33. "Uptime" means the time period when specified services with specified technical and service standards as mentioned in Section-6 are available to TENDERER and its user organizations. The uptime will be calculated as follows:  
  
"Total time in a quarter (in minutes) less total Service Down time (in minutes) in the quarter"
34. "% Uptime" means ratio of 'up time' (in minutes) in a quarter to Total time in the quarter (in minutes) multiplied by 100.



***SECTION-II***

***INTRODUCTION***

***&***

***ELIGIBILITY CRITERIA***

## 2.1 Introduction

The Gujarat Informatics Limited (GIL), on behalf of Home Department, Government of Gujarat, is issuing this ***“Request for proposal (RFP) for selection of Implementing Agency for Supply, Installation and Operations & Maintenance of State wide Surveillance and ITMS Project across the State of Gujarat”*** under the flagship program called ***“Safe & Secure, Gujarat-SASGUJ”***

Home Department, Government of Gujarat envisage to implement SASGUJ as a State-wide surveillance project across the state covering approximately 165 Cities spread across the state in a phased manner. Phase-I of the project will cover around 44 major cities and phase-II of the project will cover remaining 120 cities of the state.

### ***Core Objectives of SASGUJ:***

- Surveillance, Security, Law & Order Management
- Traffic Management & Control
- Safeguard public areas
- To minimize losses from natural hazards and human threats
- Provide lead and evidence for investigation
- Integration with Smart City/UDD projects

## 2.2 About the project

Home Department, Government of Gujarat intends to implement the SASGUJ in a phased manner wherein phase-I will consist of creation of Central infrastructure required for entire state as well as end point hardware like camera, videowall etc. at the 44 major cities in the state of Gujarat.

As mentioned above, Home department, GoG intends to procure Video Management System (VMS) and other Video Analytics based software (ANPR System, RLVD System, Speed detection system) for video surveillance and e Integrated Traffic management system for implementation and successfully running of SASGUJ project (Phase I & II) under this contract/RFP.

Further, IT infrastructure (Storage, Router, Switches, Firewall etc.) and End Point devices like CCTV camera, Video wall etc. required at 40 major cities under the phase-I of the project will also be part of the scope of work of this bid.

Bids are thereby invited from reputed and experienced Bidders to participate in competitive bidding process for implementation of SASGUJ project Phase-I in the state of Gujarat.

## 2.3 Eligibility Criteria

The bidder must possess the requisite experience, strength and capabilities in providing services necessary to meet the requirements as described in the RFP document. Keeping in view the complexity and volume of the work involved, following criteria are prescribed as the eligibility criteria for the bidder interested in undertaking the project. The bidder must also possess technical know-how and financial ability that would be required to successfully provide System Integration, Operation and Maintenance services sought by the Home Department, Govt. of

Gujarat for the entire contract duration. The Bids must be complete in all respect and should cover entire scope of work as stipulated in the bid document. This invitation to bid is open to all bidders who qualify the eligibility criteria as given below:

S/N	Specific Requirements	Documents Required
1	Bidder should be a company registered under Companies Act, 1956 and should have been operating for the last five years as on bid issuance date.	Certificates of incorporation & Self-Declaration Certificates
2	Bidder should be an established <b>IT /Telecom System Integrator</b> and should have been engaged in <b>setting-up and Operations &amp; Maintenance Services of Network (Active or Passive) and Data Centres</b> for a period of at least <b>five years</b> as on bid issuance date.	Work Orders / Client Certificates confirming year and area of activity should be enclosed.
3	The bidder must have annual turnover of at least Rs. 500 Crores for each of the last three financial years as on 31 <sup>st</sup> March, 2017.  <i>Average Annual Turnover of the bidder generated solely from supply/service for (active and passive) Networking (setting up or O&amp;M) and Data Centre (setting up or O&amp;M) during the last three financial years, should be at least Rs. 250 crores.</i>  In case Bidder is a wholly owned / 100 % subsidiary, the turnover of Parent company would be considered for eligibility.	Audited and Certified Balance Sheet and Profit/Loss Account of last 3 Financial Years should be enclosed.  Statutory auditors certificate mentioning turnover of the bidder should be enclosed.
5	The bidder must have positive net worth and should be Profit making in each of the last three financial years as on 31 <sup>st</sup> March, 2017	Audited and Certified Balance Sheet and Profit/Loss Account of last 3 Financial Years should be enclosed.  Statutory auditors certificate mentioning net profit of the bidder should be enclosed.
6	Bidder should have demonstrable expertise and experience in executing at least ONE project of Network Integration / Systems Integration/Data Centre (setting up or O&M) anytime during last five years as on bid issuance date, having a <b>minimum value of Rs. 50 crores or TWO projects having a minimum value of Rs. 25 crores each.</b>  <b>Note:</b> In case Bidder is a wholly owned subsidiary, the experience of Parent company would be considered for eligibility	Details of such projects undertaken along with clients' on-going/completion certification/ letter should be enclosed.  Undertaking from the Parent company to support its wholly owned subsidiary.
7	Bidder should have demonstrable expertise and experience of setting up or O&M of integrated control room/city wide control room/emergency response centre with One such Project having minimum 20 seating capacity  Or Data Centre (minimum 400 core computing capacity)/ 2000 Plus WAN Node during last three years as on bid issuance date.	Copies of work order and the client certificates for satisfactory completion of project.  Undertaking from the Parent company to support its wholly

S/N	Specific Requirements	Documents Required
	<p><b>Note:</b> In-house projects for their own corporations executed by the bidder shall not be considered for above purpose.</p> <p><b>Note:</b> <i>In case Bidder is a wholly owned subsidiary, the experience of Parent company would be considered for eligibility</i></p>	owned subsidiary
8	Bidder or OEM should not be blacklisted by any Ministry of Government of India or by Government of any other State in India or by Government of Gujarat or any of the Government PSUs at the time of bidding.	Certificate / affidavit mentioning that the Bidder is not blacklisted by any Ministry of Government of India or by Government of any State in India or by Government of Gujarat or any of the Government PSUs. Self-Declaration Form must be submitted
9	<p>OEMs of proposed equipment/components should have their own registered office in India as per the prevalent/ applicable laws of India and be in operation in India for last five years as on the bid issuance date.</p> <p><b>Registered offices by way of Joint ventures, Franchise, agency, distribution partners will not be considered.</b></p> <p>a.) OEMs for networking devices at aggregation layer and data centre layer should be one of the top five from the GARTNER list of top five companies for data centre networking</p> <p>b.) OEM for other networking equipment's should be in the top Five positions in terms of market share in India as per latest available IDC report or should be present in latest Gartner magic Quadrant.</p> <p>c.) OEM for storage and servers should be from companies featuring in Gartner magic quadrant in leadership position.</p>	Undertaking & copies of supporting documents from the Bidder confirming the compliance along with the OEM authorization.
10	The bidder should have a Permanent Office in Gujarat or should setup in 45 days from the award of Work Order.	Copies of any two of the followings: Property Tax / Electricity / Telephone Bill / VAT/ CST Registration /Lease agreement. Or Undertaking to open Office in Gujarat

**Note:**

- (i) The Bidder must attach valid documents in support to their Technical and Financial capabilities/strength, as mentioned above. Without proper supporting documents, the Bid proposals are liable to be rejected.
- (ii) All the proposed equipment should not be declared End-of-Support by the OEMs for next 7 years and should not be end of production for next one year from the date of bid submission.
- (iii) The MAF is required for Routers, Switches, Firewall, Storage, NMS, Servers etc. being supplied under this project.

***SECTION-III***  
***SCOPE OF WORK***

## SCOPE OF WORK

Gujarat Informatics Limited (GIL) on behalf of Home Department, Government of Gujarat seeks proposal from the interested bidder for the supply, installation, commissioning and Operations and maintenance for 5 years of the Phase-I of SASGUJ project as per the scope of work, functional and technical specification defined in this **“Request for proposal (RFP) for selection of Implementing agency for Supply, Installation and Operations & Maintenance of State wide Surveillance and ITMS project across the State of Gujarat”**.

Home Department, Government of Gujarat envisage to implement as state wide surveillance system called “Safe n Secure-Gujarat” (SASGUJ) covering approximately 165 Cities spread across the state in a phased manner.

- Phase-I of the project will cover around 44 major cities and
- phase-II of the project will cover remaining 120 cities of the state.

### Approach:

At present various surveillance projects are implemented across the states with distributed approach and are working in silos. The foremost objective of the SASGUJ is to create a state level surveillance system wherein gradually each and every system merge with the SASGUJ and central command and control center will be able to view the feeds of the entire state on demand.

Recently, Rajkot Municipal Corporation has floated a tender for city-wide surveillance and ITMS project, however the approach adopted in the Rajkot municipal project compliments the state-wide approach of SASGUJ. In the Rajkot, municipal project application like video management system, video analytics-Automatic Number Plate Recognition, Red light violation detection, speed limit violation, e-Challan etc. procured on yearly subscription basis for 1 Year and on completion it will be integrated with the centralized systems build under the SASGUJ project. Successful bidder of SASGUJ is responsible for integration of the Rajkot CCTV surveillance project with SASGUJ.

As mentioned above entire project is divided in two parts i.e. **Phase-I** will consist of creation of Central infrastructure required for entire state as well as end point hardware like camera, video wall etc. at the 44 major cities in the state of Gujarat

Further, **Phase-II** will cover approx. 120 cities wherein only end point hardware will be procured which will be integrated with the central infrastructure created under the Phase-I.

The sizing for hardware at central side will have to be done for approximately 20,000 cameras at end locations. Sizing for software (Licenses) has to be done for the quantity that is proposed to be procured under this bid.

### **3.1 Scope of work:**

The scope of work under this RFP is broadly divided into three components:

#### **3.1.1 System Integration Component:**

- Software/Application:** Bidder is responsible for Supply, installation, testing, commissioning and O&M of Software/Applications like Video Management System, Video analytics capabilities and City surveillance and Intelligent Traffic Monitoring System such as Red Light Violation Detection (RLVD), Speed Detection, Automatic Number Plate Recognition (ANPR), Vehicle Tracking System, and e- Challan System.
- Hardware/End Points:** Bidder is also responsible for supply, installation, commissioning and O&M of end points like CCTV Cameras, video Walls, Storage, IT Infrastructure, Non-IT Infrastructure (Network Cabling, UPS etc.) to be deployed across multiple cities covered under the Phase-I of SASGUJ Project.

- iii. **Integration of legacy systems:** Cities like Ahmedabad, Surat, Rajkot, Bhavnagar, Gandhinagar, Morbi, Vadodara have set up their own CCTV camera based surveillance projects. Bidder is responsible for integrating their CCTV feeds in to this proposed solution at the central side at respective City/ District location. Bidder shall also be responsible for integration/ Migration of the database's of the above-mentioned Surveillance, ITMS projects, e- challan etc. with the proposed solution under the SASGUJ Project such that there shall be a single Unified system for the entire state. The details of the existing system are provided as per **Annexure B**.
- iv. **Operations & Maintenance Component:** Operation and Maintenance of entire infrastructure (IT and Non-IT) installed as per the scope of work of this RFP for the 5 Years from the date of Go live.

### **3.1.1. System Integration Component:**

The project model will be a Hybrid model i.e. a mix of centralized and distributed architecture wherein the cities will have the deployment of the Cameras, video wall, Storage, IT Infrastructure, etc. at the District/City level and at the central infrastructure at the state Head Quarter hosting all applications running in a client server model.

Bidder is required to consider total sizing of the project (Phase I & II) to the tune of around 20,000 cameras out of which approx. 6500 cameras will be installed under the phase-I of the project.

It is envisaged that all the required software, application will be hosted at state head quarter which will be extended up to the district/city level on API basis. Further, local/city level control room/operation center will perform the required analytics over the video feed for generation of e-Challan and performing other surveillance related activities locally.

As mentioned above, bidder is required to deliver, install valid VMS Licenses (valid and perpetual for life). Further, incremental license (for end devices), if any, can be procured as per the discounting terms mentioned in the price bid section of this RFP.

#### **3.1.1.1 General Obligation under the System Integration**

Selected Bidder is responsible for below mentioned indicative list of activities applicable for all the components/sub-components of the project but not limited to: -

- a) Provide detailed Implementation plan including feasibility study and actual site survey confirming requirement for Poles, Gantry, CCTV Cameras (including Type and QTY), Positioning of junction box, source of power supply, last mile cabling route, kind of coupling/mounting brackets needed to mount cameras.
- b) Design, supply, installation, testing, commissioning of all the hardware (IT & Non-IT) and software inclusive of cables and all applicable accessories required for the successful completion of the entire projects as per the scope of work and technical specification of the RFP at the respective locations.
- c) Setting up and operations of Centralized Command and Control centre and District/ City level Control centres obtaining the required permissions from the authorities/local bodies. However, TENDERER will provide adequate assistance/support as and when required.
- d) Comprehensive Last mile connectivity ( including supply, installation & commissioning of required material/hardware ) between utilities and nearby Junction (connectivity medium like CAT-6/fibre as per the site requirement) including supply of active and passive component within the junction box. Civil Work (Supply, Erection and commissioning) of Non-IT infrastructure like Poles/Gantry/ frames/fixtures/housing etc. with proper electrical earthing (as per IS-3043) wherever required as per the feasibility plan/ report.
- e) Bidder has to ensure that on completion of work, site has to be restored to its original condition as per rules / provisions of respective local bodies/authorities.
- f) All the software application's along with their databases shall be deployed at the district Head Quarter's. i.e. the applications such as Analytics, RLVD, Speed Violation, ANPR etc. shall be hosted at the district/ city location's control centre. the database for the respective client shall be maintained at the district end but the same shall be pulled in real/schedule time, along with CCTV feed and relevant frames at the Centralized CCC. Hardware for management of VMS and CCTV feeds shall be located at central side at Gandhinagar and CCTV cameras and feeds at City / District will act in master client relationship with VMS.

- g) For the client end application support, bidder will provision and supply necessary hardware plus computing power that will be good for camera feeds that will be four times of what is being installed at end points. Storage will be as per the capacity indicated with provision for addition of extra storage disks to take storage capacity to double of what is being asked.
- h) E-Challan payment system including hardware will be centrally hosted. Challan generation activity will be at district/city CCC.
- i) Further the Licenses for all the software applications such as VMS, Video Analytics, RLVD, Speed Detection, ANPR etc. it shall be for cameras/Users/databases for deployment by the TENDERER within the entire state of Gujarat, perpetual for life.
- j) The bidder has to provision all the required hardware/software/services which may be necessary and vital for the successful implementation and running of the entire project.
- k) **The Solution asked under this RFP shall be executed as an EPC based Contract for the bidder to meet the outcome. The bidder may utilize the existing infrastructure such as Poles, Gantry, Lighting pillars, Fixtures etc. where ever available with the prior permission from TENDERER, the bidder in such cases will also have to make sure that such fixtures are not used in a destructive manner or effect the day to day functions of any other work / service. In case no such infrastructure is available for the installation of the end points the bidder will have to erect install and utilize the same for the successful implementation of the project.**
- l) **OEM Support:**
  - i.) The bidder should submit authorization certificate of Original Equipment Manufacturer (OEM) (or multiple OEMs) specific to the bid. The bidder should have a back-to-back support agreement/arrangement for services including supply of spare parts etc. with the OEMs of products like Networking devices, Servers, Storage etc. which includes the post-sales support activities for the entire project period.
  - ii.) **All the proposed equipment should not be declared End-of-Support by the OEMs for next 7 years and should not be end of production for next one year from the date of bid submission.**
  - iii.) **In case if the quoted product/equipment goes out of support or warranty during the implementation period, the successful bidder will have to replace the same with the higher model without any cost limitation to the TENDERER.**
- m) Operation and maintenance of entire project (IT, Non-IT and Software) as per the scope of work for the period of 5 years from the date of Go Live.
- n) The IP Pool for the project will be provided by the TENDERER.
- o) Actual power/electricity required will be provided by TENDERER. However, extension till the last mile/actual utility will be in the scope of successful bidder. Further the Recurring Electricity charges under the project shall be paid by the TENDERER
- p) **The RoW (Right of Way) wherever required for the digging and laying of underground cables for last mile connectivity and foundations has to be obtained by the successful bidder at its own cost, however the TENDERER shall help in obtaining such permissions. The TENDERER will reimburse the RoW charges to the successful bidder on submission of the actual receipts of the such charges paid.**
- q) The bidder under the scope of work will be responsible for integrating the infrastructure that is part of scope of this tender with the existing applications of Govt. of Gujarat such as e-Gujcop, Vahan, Sarathi, and Smart City projects for leveraging the SASGUJ Infrastructure.
- r) The system integrator will also be responsible for data migration from the existing applications/systems such as CSITMS, e- Challan as they exist in Ahmedabad, Gandhinagar, Vadodara and Surat city in the proposed solution.

### 3.1.1.2 CITY SURVEILLANCE SYSTEM

- a) TENDERER plans to build a robust Surveillance Infrastructure under its Safe and Secure Gujarat (SASGUJ) initiative by setting up and providing district/city-wide CCTV surveillance infrastructure. A robust city wide surveillance system will enable the TENDERER and Police Department to keep a watch on sensitive areas of the city through a centrally integrated operations and monitoring on one application layer. Further, this infrastructure will provide advanced level of digital security and surveillance system.
- b) Implementation of surveillance system covering entire city with focus on state of the art security system covering major traffic junctions, vital and sensitive locations of the city , and key gathering places through the Video Camera feeds at the district Control Centre.
- c) Bidder is responsible for Design, supply, installation, testing, commissioning, operations, management and maintenance of entire city surveillance system including of all the components like cameras, video management system etc. as per the technical specification and scope of work of this RFP during the contract duration.



- d) It is envisaged that the City Surveillance System should be an IP based system installed at selected locations for smart traffic management and citizen safety via surveillance.
- e) Detailed list of locations along with the required no. of cameras is mentioned in Annexure-A. However, while doing detailed feasibility study and site survey activity bidder is required to include type and quantities of camera required at each location.
- f) The proposed video surveillance system will involve setting up of IP based outdoor security cameras across various locations in the Cities. The video surveillance data from various cameras deployed will be stored and monitored at control centres at respective district/city and can be viewed at state command and control centre on Pull/Push mechanism.
- g) Bidder is responsible for setting up and O&M of the Central Command and Control Centre and control centre at each district/ city along with end site devices.
- h) To receive collaborative videos from public & private agencies locations (airport, railway stations, roadways, temples, malls, metro stations, fair, festivals etc.) and to display the selected videos on videos on wall and store them, if required.
- i) Technical specification as mentioned in Section 4 of this document is minimum, however the bidder has to ensure the below mentioned outcomes from the surveillance perspective are met at all times:

S/N	Description	DAY		NIGHT	
		Identification of Registration No. of the vehicle	Identification of Face	Identification of No. Plate	Identification of Face
1.	Live Video	Required	Required	Required	Required
2.	Recorded Video (On digital Zoom)	Required	Required	Required	Required
3.	Live video - (Zoom in/out)	Required	Required	Required	Required
4.	Recorded Video Zoom in-Out using Digital Zoom	Required	Required	Required	Required

**j) IP Cameras:**

- (i) Cameras being the core of the entire Surveillance system, it is important that their selection is carefully done to ensure suitability & accuracy of the information captured on the field and is rugged, durable & compact.
- (ii) These cameras need to work on 24 X 7 X 365 basis during all weather conditions and transmit video feeds to the District Control and should be capable to capture the video feeds at a lower FPS during the lean period.
- (iii) Home/Police Department may take the regular review of the requirements for video resolution, FPS and may change these numbers to suit certain specific requirements (for example, there could be a situation when certain cameras are required to be viewed at higher FPS for specific period.
- (iv) The cameras will have the functionality to zoom in and pan out on a specific predefined field in its viewing area, detect and track motion etc.
- (v) The cameras proposed under the project should ensure the use of bit rates and compression techniques such that the bandwidth utilization for the video stream transmission is optimized.
- (vi) Positioning of Cameras should be such that it covers the entire road/lane available at the respective locations.
- (vii) Cameras should be installed on proper pole/Gantry at the locations finalized by the TENDERER. However, there are locations in the city where poles/gantry are already installed/available. It is envisaged that selected bidder should cover the exact availability and requirement of setting up of new poles/gantry in their detailed feasibility status report.
- k) Apart from the above the bidder need to ensure compliance of the project with Government of India IT security guidelines including provisions of:
- The Information Technology Act, 2000” and amendments thereof and Guidelines and advisories for information security published by Cert-In/MeitY (GoI) issued till the date of publishing of tender notice. Periodic changes in these guidelines during project duration need to be complied with.
- l) Proposed solution should include, PTZ, Fixed cameras, server based digital recording system and the centralized VMS software should be from reputed manufacturer which can be integrated to any other manufacturer having ONVIF supported hardware and VMS software.
- m) The Surveillance System should not have any limit on the number of cameras to be connected for Surveillance, Monitoring and recording.

- n) The Surveillance System shall support distributed viewing of any camera in the system using Video walls or big screen displays.
- o) The Surveillance System shall support alarm management. The alarm management shall allow for the continuous monitoring of the operational status and event-triggered alarms from system servers, cameras and other external devices.
- p) It should be possible to integrate the Surveillance System with 3rd-party software, to enable the users to develop customized applications for enhancing the use of video surveillance solution. For e.g., integrating alarm management to initiate SMS, E-Mail, VoIP call etc.
- q) **Signboards for CCTV camera locations:**
  - (i) It is necessary that the CCTV Camera locations should have some standardized signs informing the public of the existence of CCTV cameras in Gujarati language. This will bring about the transparency on installation of CCTV cameras and no one would be able to later complaint for the breach of privacy.
- r) **Video Analytics System:**
  - (i) The TENDERER envisages to implement video analytics system, this analytics layer, being separate from the functionalities sought under city surveillance solution i.e. ANPR/RLVD etc., this will allow rule based alert generation on live feed. It will work on set of rules pre-programmed.
  - (ii) The video analytics software should be capable enough to perform following tasks:
    - Object detection: should be able to detect Un-identified/Abandoned/unattended objects.
    - Attribute based search for Objects and People such as vehicle color, cloth color, size, height etc.
    - Object Origin detection i.e. to detect the unattended object from the time it first appeared on the view of the camera.
  - (iii) The alerts generated by this video analytics system should be automatically registered in the respective control Centres application's list of events and incidents.

### 3.1.1.3 **INTEGRATED TRAFFIC MANAMAGEMENT SYSTEM**

The ITMS shall use the latest available video analytics techniques to regulate the traffic and identify violations at different traffic junctions at each district/city level. Bidder is responsible for supply, installation, commissioning and O&M all the required applications such as RLVD, ANPR, Speed detection etc. with enterprise level licence. Further these applications will be deployed and will process on the video feeds at each of the district control rooms locally. However, all the violation information along with the evidences (Images, Video Clips) shall come to the master databases at the CCC level.

Applications should be integrated with the e- challan system in such a way that Every violation should automatically generate a challan, in the prescribed format along with the image/ video snippets of violations and stored automatically with due indexing. The key objectives of the ITMS system are as follows:

- ⇒ Reduce violation trends
- ⇒ Optimize traffic signal timings for reducing travel time delayed

The Different capabilities required under the ITMS are as below:

- a) **Red Light Violation Detection System**
  - (i) The RLVD system should use the Video/Image processing techniques to identify the red-light violations.
  - (ii) The RLVD system Including ANPR capabilities should be integrated with the various application and Databases like e-GujCop, VAHAN, SARATHI and e-Challan application etc. such that e-Challans can be generated by the system through an automated process.
  - (iii) The RLVD system and related videos as well as the surveillance video feed should go to the central control rooms, wherein the Red-Light violation and its Number plate detection shall take place at the Command and control centre end (server) in real time.
  - (iv) The system should be capable of identifying & capturing of vehicles traveling through a signalized intersection during the 'red' signal phase during 24x7 (both day and Night) and recording a series of violation images that track the whole violation event.
  - (v) The system should be able to capture the image of the violating Vehicle along with the active Red Light & colour, as a proof of the violation.
  - (vi) The system should be able to do simultaneous monitoring of multiple lanes and should be able to identify multiple Red Light Violations simultaneously within the same lane/ Road.
  - (vii) The RLVD system has to be integrated with the Red Light Signalling System controller and should be able to sense the Red-light signal and identify violators based on It.

- (viii) 'Scene' images will be captured the red signal in the direction of vehicle's travel.
- (ix) The System should be able to identify and Log Red Light Violations with minimum accuracy of 90%
- (x) The System should be able to read and identify the Registration plate of the vehicle violating the Red Light through the ANPR system.
- (xi) The system should be able to capture and provide Video Feed from the RLVD application (Server side) for a duration for which the RED Signal is active for that section of the Road.
- (xii) The system should be able to generate various MIS reports like vehicle(s) made rule violations, Vehicle details, violation type along with date and time stamp, week / Month / Year wise reports.

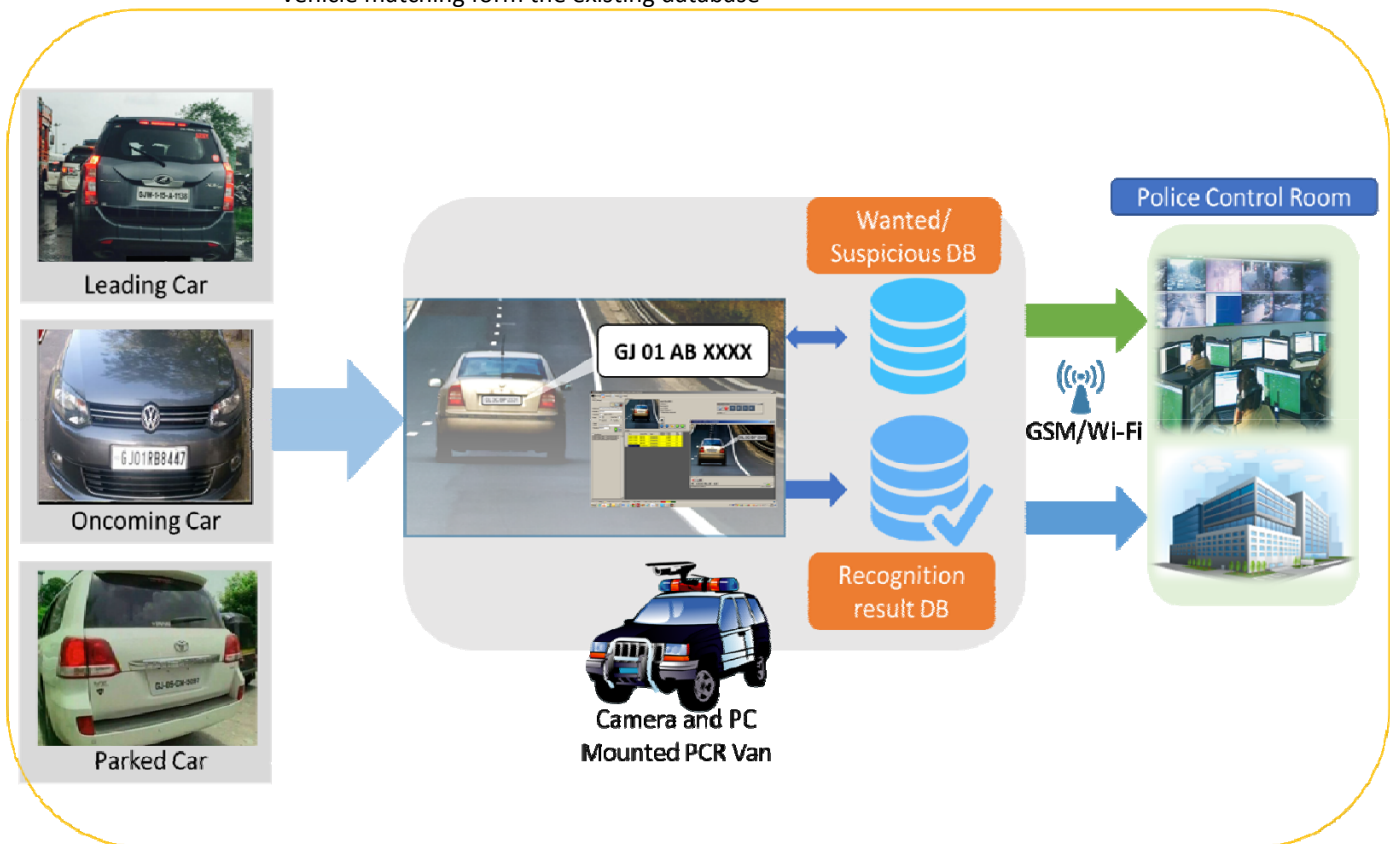
**b) Speed Detection System:**

- (i) This system shall be taken up at multiple cities with cameras installed at identified locations on the freeways/Junctions covering entire road.
- (ii) The Vehicle Speed Detection system should be a camera based Video analytics system wherein the speed of the vehicle is automatically calculated and violations is detected based on the permissible speed limits.
- (iii) The Automatic Speed Detection application (Including ANPR) will have to be integrated with the various application and Databases like e- Gujcop, e- challan, RTO, home/Police department etc. such that e-challans can be generated by the system through an automated process.
- (iv) The Speed Violation system should be capable of measuring speeds up to 120 Km/Hour for both (Two & Four Wheeler's) or higher with minimum accuracy of 90% in detecting speed limit violations both during the day and night time and photographing the incident and reading the vehicle No. plate in various fonts and sizes in English Language.
- (v) The details of limits of speed violations will be shared with the successful bidder by the traffic police department.
- (vi) The system should be able to generate an alarms /alerts based on the vehicles status and category like "Wanted", "Suspicious", "Stolen" etc. as categorized by the database.
- (vii) The system should be capable enough to process the speed violations activity through the raw feed at the district/ city Control Center, and the details of violation like Speed Violation data, alert and videos/photo feed should be stored at the command and control centre.
- (viii) The System should be able to detect the speed of the vehicles with an accuracy of +/- 5 Kmph, the bidder will have to get its system tested and & certified by the competent certifying body for the acceptance as an evidence in the court of law. It is not a pre requisite for the submission of the bid, however, the successful bidder will have to submit such certificate(s) along with its testing Report to the TENDERER on annual basis

**c) Automatic Number Plate Recognition (ANPR) System**

- (i) The proposed ANPR System shall enable monitoring of vehicle flow. The system shall support real-time detection of vehicles, reading of its number plate and conversion of the same into alphanumeric text.
- (ii) The proposed ANPR system has to be integrated with various Applications/ Databases of the e-GujCop application of the Police department, e- challan etc. for verification/checking and fetching the required vehicle information.
- (iii) The proposed system should be able to store the image of vehicle, number plate and also able to create a record of vehicle no., Date & time stamp, locations etc. in DBMS.
- (iv) The proposed ANPR system and related videos as well as the surveillance video feed should go to the command and control centre (servers with ANPR application) for processing and identification of the vehicle Registration plates.
- (v) The proposed System should be able to detect and recognize the English alphanumeric License plate in standard fonts and formats of all the vehicles.
- (vi) The proposed system should be capable to perform OCR (optical character recognition) of number plates (Detect and Read) written in English, language with character in standard or non-standard fonts, unusual characteristics like different size characters, font, colors, special characters etc.
- (vii) The Accuracy of ANPR system should be more than 90% in case of standard English Alphanumeric Font and High Security Registration plates and 75% for non-standard Fonts, the system should be able to capture the Registration Plate of a vehicle moving at a speed of up to 120 Km/hour with the same level of accuracy.
- (viii) The system database should allow to advance search the database with different set of criteria while conducting post incident analysis/investigations.
- (ix) The proposed system should be able to generate various MIS reports like vehicle flow, vehicle category wise reports, Violation wise report, etc.

- (x) **Mobile ANPR:** TENDERER also proposes to have Police Vehicle/PCR Van fitted with ANPR camera(s) to have vigil on the uncovered roads, strategic locations, parking Lots etc. These proposed subsystems should be a standalone ANPR system with the following provisions
- provision of viewing the video feed in the vehicle itself
  - standalone system for capturing, storing and matching the read Vehicle No. Plate against the existing, wanted/suspicious vehicles database.
  - Generating real time alarms in the vehicle as well as at the control centre, in case sightings of any vehicle matching form the existing database



**Figure 2: Vehicle Mounted ANPR & Surveillance System for Illustrative Purpose**

#### **d.) Vehicle Tracking System**

- The vehicle tracking system should be able to identify the vehicle using the ANPR system for the capture of vehicle registration plate.
- The system should be able to plot the camera locations on to the city map (open source digital /Google Map or the Maps provided by TENDERER, bhulekh map etc.) in case of any stolen/suspected/wanted/Hot listed vehicle has been identified by the ANPR system at any or multi camera locations.
- The pictorial view of the data on the map should be along with the date and time stamp of the event, to give meaningful insight to the alert generated and the monitoring of the same can be done in a better way.
- The System should also be able to show the path travelled by the vehicle on the map based on the time difference and the camera sighting location.
- The Application should provide a user interface to search for a particular vehicle based on its registration no. (the last four digit) from the database of the ANPR system between the given date/time frame.
- The System should be able to generate Alert/ Alarm in case a suspicious/Stolen/Hot listed vehicle is sighted by the ANPR cameras at the district control room as well as through SMS to the concerned officer, the alert should also be sent to the local City control centre for relevant and necessary action.

#### **3.1.1.4 STORAGE /RECORDING REQUIREMENT:**

- The bidder will have to deploy the storage at each of the district/City location as well as the central Command and Control/ Data Centre as per the required sizing as provided in Annexure C.
- It is proposed that the storage solution should be modular enough to ensure compliance to the changes in storage/recording policy, to be evolved upon initial deployment of the system.

- c) The video feeds would be kept for 30 days. After 30 days, the video feeds would be overwritten unless it is flagged or marked by the Police/appropriate authority for investigation or any other purpose. The video feeds of all relevant cameras capturing the incident in question would be stored until the Police/appropriate authority deem it good for deletion. Further, incidents that are flagged by the Police or any court order, the video of the relevant portion from all relevant cameras should be stored/archived separately for investigation purposes at the District HQ and the centralized CCC as decided by the TENDERER.
- d) Regardless of the above, the image/video Outputs for RLVD, Speed Detection and ANPR system, along with the timestamp and location of the image/video capture will stored for a period of 3 months.
- e) Full audit trail of reports to be maintained for 90 days.
- f) Every CCTV feeds should be retrievable using IP of camera, based on geo-location. The storage should be configured in such a way that the feeds of CCTV cameras should be able to be pulled in from the Central VMS application from the Centralized CCC. This would require virtualized storage coupling with the centralized CCC infrastructure to be created under the project.
- g) **Retrieval time for any data /Video Feed should be less than 3 seconds. The same should happen through a single click of the mouse button. To realize the same, for the stored CCTV video feed, the bidder will create Geo-tagged, IP enabled web interface, which will be available to users of the state government through user credentials as an interface. By choosing camera either through IP address or through the geo tagged interface, and by choosing the time stamp or other meta data for video clip, the feed should be retrievable.**
- h) **Bidder is also responsible for developing a mobile application which will allow limited set of authorised users to access the video feeds live as well as recorded over the mobile/smart phone. Mobile app developed by the bidder should have minimum functionalities:**
  - (i) **Dashboard: showing various performance/statics reports of the SASGUJ**
  - (ii) **Menu based selection to select and view video feeds on demand/need based**
  - (iii) **Should work on pull based mechanism which will allow user to access the video feeds**
  - (iv) **Should also allow to view video feeds flagged or tagged for the purpose of investigation as a proof and store in an external Hard drive/CD and also at the state centre.**
  - (v) **Mobile application should allow MAC/IMEI No. binding, role based user access over secured VPN client on users mobile/smart phone.**
- i) The Recording Servers / System, once configured, shall run independently of the Video Management system and continue to operate in the event that the Management system is off-line.
- j) The system shall support storage of H.264/H.265, MJPEG or better compression formats for all IP cameras connected to the system.
- k) The system should not limit the amount of storage to be allocated for each connected device.
- l) The on-line storage capability shall be transparent and allow Clients to browse and access recordings without the need to restore the video to a local hard drive for access.

#### 3.1.1.5 **Video Wall**

- a) A state of the art LED video wall facility should be installed at Centralized CCC and the respective district/City locations. The category wise size of the Video Wall is provided in Annexure C. Followings are the functional requirement of video wall: -
- b) The video wall shall use multi-monitor (e.g., different monitor can display different input source) and split screen (e.g., several intersections can be displayed on one monitor) display technology to provide the flexibility to accept audio and video inputs Camera system, TV signal, recorded video, and Laptop computer.
- c) Should have provision for live monitoring and control of various modules of the ITS including dashboard of the surveillance, Traffic management applications.
- d) The system at CCC shall provide the capability for multiple web-based display consoles to configure, manage, display, and control various components of ITS solution for administrative and operations purpose.
- e) All applications that are part of ITMS (Integrated Traffic Management System) should be accessible from the CCC. The Work Stations will be enabled and provide access for appropriate User (Role based, read only/ Read write) and other security controls.
- f) The bidder will also have to make provision for the viewing of the Camera feeds of the citires at its local Police station/ any other location as decided by the Police Department, This will enable quick and prompt response form the local Police Action team as and when required. Such viewing centres shall be provisioned as per the requirement for the Police Department.

#### 3.1.1.6 **VIDEO MANAGEMENT SYSTEM**

- a) Proposed Video management system should have the following features:
  - (vi) Video recording from multiple Camera Sources
  - (vii) Live Monitoring Functionality
  - (viii) Video viewing and playback in desired matrix formats and playback controls
  - (ix) Web Browser Viewing on Portable Devices
  - (x) PTZ Control through multiple Pre-sets
  - (xi) Import & Export of Video and databases in various file formats
  - (xii) Collaborative monitoring
  - (xiii) Mapping of the end devices on the City's Map
  - (xiv) Dashboard for Viewing KPI and other performance measures
- b) The proposed Video Management System shall provide a complete end-to-end solution for security surveillance application. The control centre shall allow an operator to view live / recorded video from any camera on the IP Network.
- c) The VMS should support viewing of multiple cameras in one screen or viewing of one camera feed on one screen based on user selection. Multiple camera views will support 2\*2, 3\*3, 4\*4, 5\*5, 6\*6, or alternatively 3\*2, 4\*3, 5\*4, 6\*5, 7\*6, 8\*6 camera feeds on the same screen. On a video wall, it would be possible to show up to 400 cameras feeds on to the wall at the same time, auto sequencing to bring all feeds and then to pan in and zoom on one or more cameras simultaneously on the video wall.
- d) The above-mentioned requirements are only functional and the detailed module wise specification is given under Section 4 technical Specification.

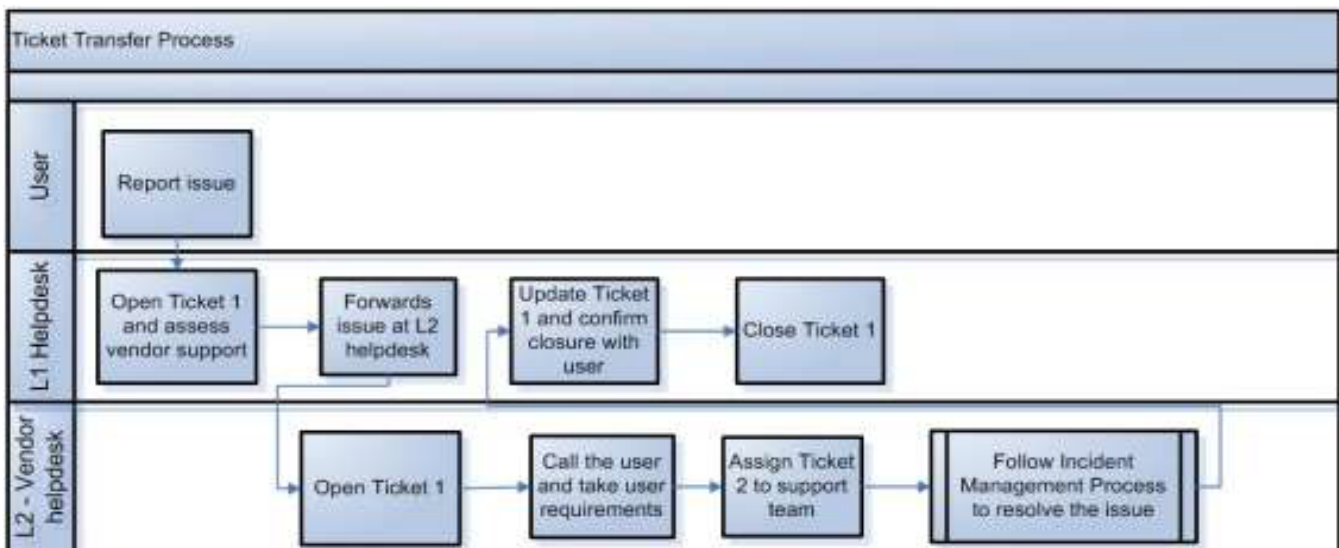
#### 3.1.1.7 **e-Challan System**

- a.) The successful bidder is required to develop a “e- Challan system/solution” based on the laws/rules of Motor Vehicle Act of central/state government.
- b.) Successful bidder is responsible for end-to-end designing, planning, supply, implementation, testing, commissioning and maintenance of entire e-Challan system.
- c.) It is envisaged that successful bidder will have to submit a detailed Functional Requirement document and software requirement specification covering each and every aspect of the system required to successfully run the system.
- d.) e-Challan system should be able to automatically generate e-challan's based on the laws/rules of Motor Vehicle Act of central/state government for the violations detected by the surveillance system. It should also have a provision/interface for manual e- challan generation for violations captured through manual level investigation of video feeds and field level. Should the government make's changes in laws pertaining to traffic management during the O&M period of the contract, the bidder will have to carry out such changes without any additional cost.
- e.) The management module of the e- Challan system shall be hosted at the central CCC whereas the actual challan generation and printing shall take place at the district/ city Control room. The E- challan system proposed under this RFP shall be a single system, that shall be deployed at multiple locations within the state of Gujarat, the Bidder will have to consider the sizing of the application accordingly.
- f.) It should be integrated with the all the required databases/systems for auto generation of e-Challan like RTO system, VMS system, ITMS system and other required resources.
- g.) The successful bidder is required to submit the SoPs, documents, FAQ along with all the patches and upgrades of the system.
- h.) Application development must be documented in detail and the code/script should be properly annotated with comments etc.
- i.) The successful bidder is also required to develop a “web based e-Challan payment” module integrated with a Payment Gateway (to be provided by the TENDERER) for the online payment of the challans by the citizens through multiple mode i.e. Debit/Credit Card/Internet Banking/wallet etc.
- j.) The system should also have the provision for integration of the e-challan system with an SMS gateway for intimating the offenders/violators at the various steps such as at the time of generation of challan, Payment due, payment made etc.
- k.) The system should be able to generate MIS reports based on the type/ Date /time/Location of offences, as may be required for the day to day activity.

- I.) The successful bidder shall integrate solution with applications such as eGujcop, Sarathi, Vahan, CCTNS etc. Bidder shall also publish API of challan information generated to be integrated by such other applications in to their data bases.

### 3.1.1.8 Centralized Helpdesk: -

- a.) The bidder under the scope of the project will have to set up a centralized helpdesk at the Command and Control Centre
- b.) It is envisaged that the centralized helpdesk, functioning as proposed below, would be managed by a separate agency (operators will come from separate agency) however. The solution, including the infrastructure, shall serve following objectives:
- Act as the Point of Contact for the users of Surveillance System
  - Own an Incident throughout its Lifecycle
  - Communicate effectively with Police / Home Dept. Officers and IT support teams.
  - Maintain high user satisfaction levels
  - Maintain the SLA statistics & submit quarterly report to Police / Home Department
- c.) A general process flow for the helpdesk management is depicted in the flow-chart given as follows bidder shall have to prepare and submit a detailed Helpdesk Policy in consultation with all the stakeholders prior to the Go Live.



### 3.1.1.9 IT & Non-IT Infrastructure for State Wide Surveillance

- a) State wide IT infrastructure shall be the core backbone of this project. Looking at the volume and size and span of the project the TENDERER envisages to implement the state-wide IT Infrastructure in a distributed model.
- b) The successful bidder will be responsible for design, supply, installation, configure, testing, commissioning, integrate (wherever required) and operation & maintenance for 5 years of all the systems (Hardware-active & passive; Software, database's) as per the scope of work and technical specification of the RFP.
- c) Carry out installation of active and passive components and accessories supplied as per standards for successful integration and implementation of the systems at each site connected under this RFP.
- d) Configuring and fine-tuning of subsystems to achieve overall optimal network performance and highest security.
- e) The Successful Bidder should propose a comprehensive solution for state wide IT infrastructure. However, below are indicative/minimum (but not limited to) list of components bidder is required provide as a part of entire solution:
- (i) Network equipment (like Routers, Switches)
  - (ii) Servers including recording and Application servers
  - (iii) Erection of mast/poles/Gantry
  - (iv) Video surveillance systems (VMS- License Bank including VMS based Analytics)
  - (v) Video Analytics Bank (Face identification, ANPR, RLVD, Speed Detection etc.)
  - (vi) Video management Controller
  - (vii) Storage hardware at specified locations
  - (viii) Computer hardware and Accessories at specified locations
  - (ix) All system and application software

- f) The bidder shall depute minimum required skilled resources as defined in this RFP document. However, to ensure that the implementation and commissioning activities are carried out on schedule and as per the scope of work bidder may increase the required nos. of resources without any additional cost to the tenderer.
- g) The bidder shall submit a detailed test plan and test cases for each solution, that will be used to carry out the UAT (user acceptance test) and FAT (final acceptance test)
- h) As part of the project completion documentation, the bidder shall submit the documentation, which should at least contain:
  - (i) As-implemented configurations
  - (ii) As-implemented architecture and topology diagrams
  - (iii) Standard operating procedures for administration of the installed devices.
- i) Bidder needs to design network architecture as per the client requirement using industry best practices.
- j) Bidder should ensure availability of all the patches and updates released by OEM of the product during the contract durations.
- k) The bidder will have to make an assessment of the deployment of the end points switches based on the no. of end points devices such as camera's, to be deployed at the site locations.
- l) Electrical cabling from the input source and up to the equipment to be kept at each location, Junction rack etc. as the case may be, shall be the responsibility of bidder.

### **3.1.2. Operations and Maintenance (O&M) of the project**

- 3.1.2.1 The bidder shall be responsible for the overall operations & maintenance, management of the IT and Non-IT Infrastructure and enabling infrastructure maintenance services / facility management services at all Site locations for ensuring adherence of SLAs. Bidder shall provide the Operations and Maintenance Services for a period of 5 years following the Go Live date.
- 3.1.2.2 Tenderer will issue a separate RFP for the requirement of connectivity at all the locations. However, Network management system supplied, installed, configure and commissioned by this successful bidder should allow to discover, manage and monitor the connectivity links provided by the successful bidder of connectivity RFP. Further the successful bidder of this RFP is only responsible for discovery, monitoring, logging of service request (in case of link is down) etc.
- 3.1.2.3 The bidder shall be responsible for performing various day to day activities like discovery of network devices, monitoring of network health, generation of various MIS reports, pertaining to the network management through NMS tools supplied him under this RFP. Bidder is also responsible for adhering to the Service level agreements and maintaining entire system with the minimum required uptime defined in this RFP document.
- 3.1.2.4 The bidder is also responsible for performing/carrying out preventive maintenance activity at least once in a quarter which includes configuration backup and software up gradation/updation. Up gradation/Updation will be part of the back to back warranty support from the OEM.
- 3.1.2.5 The Bidder is required to submit preventive maintenance schedule of all equipment to TENDERER. After performing preventive maintenance activities, successful bidder is required to submit the detailed report of the same. All such activities should be done preferably during non-working hours or on non-working days/holidays.
- 3.1.2.6 As part of the Operations and Maintenance services, the bidder shall provide support for the software, hardware, and other infrastructure provided as part of this RFP. The bidder shall also provide services comprising of but not limiting to the following:
  - a) Operations and maintenance services for the IT and Non-IT Infrastructure supplied or commissioned by the bidder at the designated locations as defined in this RFP document during the contract period.
  - b) The scope of work under O&M is not limited to the IT and Non-IT Infrastructure components deployed by the successful bidder but it also includes O&M for any additional equipment/devices/hardware/software related to the project supposed to be procured during the contract period of 5 years by the TENDERER.
  - c) O&M charges for any such additional work shall be paid at 2% per annum of the cost of such additional equipment/devices/hardware/ software component to be deployed at the central site and the rate of 10% per annum for the end point devices. Further successful bidder is required to comply with the overall SLA requirement of contract for any such additional SoW.
- 3.1.2.7 **Warranty Support:** - As part of the warranty services bidder shall provide:
  - a) Bidder shall provide a comprehensive on-site warranty support for 5 years from the date of successful completion of FAT for all the equipment supplied under the project.
  - b) Bidder shall provide the comprehensive manufacturer's warranty and support in respect of proper design, quality and workmanship of all hardware, equipment, accessories etc. covered by the RFP. Bidder must



- warrant all hardware, equipment, accessories, spare parts etc. procured and implemented as per this RFP against any manufacturing defects during the warranty period.
- c) Bidder shall provide the performance warranty in respect of performance of the installed hardware and software to meet the performance requirements and service levels in the RFP.
  - d) Bidder is responsible for sizing and procuring the necessary hardware and software licenses as per the performance requirements provided in the RFP. During the warranty period bidder, shall replace or augment or procure higher-level new equipment or additional licenses at no additional cost in case the procured hardware or software is not adequate to meet the service levels.
  - e) Mean Time between Failures (MTBF): If during contract period, any equipment has a hardware failure on four or more occasions in a period of less than three months, it shall be replaced by equivalent or higher-level new equipment by the bidder at no cost. For any delay in making available the replacement and repaired equipment for inspection, delivery of equipment or for commissioning of the systems or for acceptance tests / checks on per site basis, the TENDERER reserves the right to charge a penalty.
  - f) The bidder will also cover the failure of the end point equipment's due to earthing or power fluctuations under this warranty/AMC. It is the responsibility of the bidder to undertake preventive maintenance of the supplied UPS and proper earthing to avoid this risk
  - g) During the warranty period bidder, shall maintain the systems and repair / replace at the installed site, at no charge, all defective components that are brought to the bidder's notice.
  - h) The bidder shall as far as possible repair/ replace the equipment at site.
  - i) Warranty should not become void, if the TENDERER buys, any other supplemental hardware from a third party and installs it within these machines under intimation to the bidder. However, the warranty will not apply to such supplemental hardware items installed.
  - j) The bidder shall carry out Preventive Maintenance (PM), including cleaning of interior and exterior, of all hardware and testing for virus, if any, and should maintain proper records at each site for such PM. Failure to carry out such PM will be a breach of warranty and the warranty period will be extended by the period of delay in PM.
  - k) Bidder shall monitor warranties to check adherence to preventive and repair maintenance terms and conditions.
  - l) Bidder shall ensure that the warranty complies with the agreed Technical Standards, Security Requirements, Operating Procedures, and Recovery Procedures.
  - m) For Cameras, the bidder will have to maintain minimum 5 % of the quantity deployed as spare at each of the district HQ's for quick and prompt replacement.
  - n) Bidder shall have to stock and provide adequate onsite and offsite spare parts and spare component to ensure that the uptime commitment as per SLA is met.
  - o) Bidder shall develop and maintain an inventory database to include the registered hardware warranties

#### 3.1.2.8 Network operations, Services and Maintenance

- a) **Network management system shall be deployed centrally at the state centre. However, proposed NMS shall allow creation of Groups/multiple users with role based access. Further, District/local level user should be able to monitor network component like device & links coming under the respective District boundaries.**
- b) The services as per the scope of the contract shall include maintaining the network equipment; ensuring running of the services (As laid down in the Scope of Work) with availability in line with the SLA and Round-the-clock Network monitoring. This shall include:
  - (i) Equipment Configuration Management
  - (ii) Upgrading IOS
  - (iii) Maintaining access control list for the various Control centres
  - (iv) Complete IP Management of the entire Network
  - (v) Regular review of Network and its components, end point devices and nodes
  - (vi) Regular reports as required by the Home/Police Department and authorized agency
  - (vii) Regular backup of NMS server and router configurations
  - (viii) Upgrading Patches on all equipment's including NMS-Servers, network & Security Devices and hardening of network & security devices
- c) The Successful bidder is required to maintain uptime of the network between the different network nodes, camera end points and different control centres to meet the SLA. In case the network uptime is not maintained due to non-availability of link/Bandwidth by Service provider, bidder is required to produce

documentary proof (Service Desk Complaints/Incidents or Vendor assigned Tickets) in terms of certificate of downtime of network link/b/w from the service providers. In case bidder fails to provide such documentary proof the same shall be treated as non-performance of SLA and would be liable for penalty.

- d) The Successful bidder will be responsible for setting up the QoS parameters (Quality of Service) for the entire Surveillance network for the various data types i.e. Voice, Video, Data, prioritize and manage them as per the requirement of the project from time to time.
- e) Successful bidder will have to do operational liasoning with stake holders (link providers, state government, local bodies, third party agencies / consultants appointed/identified by the TENDERER or its user departments) to keep the link up & running.
- f) In case the TENDERER decides to migrate the network to IPv6, the successful bidder shall prepare the migration plan and execute the same as per the timeline mutually agreed between the TENDERER and successful bidder.
- g) Bidder has to provide UPS & Battery Health Reports in every quarter after completing proactive maintenance every quarter.
- h) Under the scope of this RFP, the successful bidder has to setup control centre(s) to control and monitor the project operations from a central location at Gandhinagar as well as from the various district and city locations and the same has to be operated and maintained, as prescribed:
  - (i) LAN Cabling with proper tagging as per cabling standards with network diagrams need to be maintained for every Data Center and control Centers created under this project.
- i) **NMS for SLA and Performance Reporting**
  - (i) The Successful bidder shall operate and maintain a Network Management System (NMS) and SLA and Performance Monitoring System for the complete Network backbone both at the city level as well as the central CCC level.
  - (ii) The NMS system shall be configured to automatically discover all manageable elements through IP/SNMP at regular intervals in order to determine their status and working
  - (iii) All network components shall be configured to alert the centralized/City level NMS server(s) in case of any events, so as to reflect real status of all network components and links across the network
- j) **Functional Requirement of the NMS**
  - (i) **Alarms**
    - The NMS should be able to generate alarms at various event of failure, non-performance, SLA breach etc.
    - The system should allow alarm Filtering through flexible filtering rules for NOC staff to filter the alarms by category, severity, elements, duration, by user, by views, by geography or by end utility.
    - Ability to apply severity to alarms according to predefined rules and to add description to the alarms.
    - The system should be able to clearly identify configuration changes as root cause of network problems
    - It should be possible to convert Critical Alarms into Incidents for auto ticket generation.
  - (ii) **Network Fault and Performance Management**
    - The Network Management function must monitor performance across heterogeneous networks from one end of the enterprise to the other.
    - The Network Management function should have a graphical topological display of all discovered network devices in real time.
    - The proposed Network Fault Management solution must also provide network asset inventory reports
    - The proposed Network Fault Management solution must support extensive discovery mechanisms and must easily discover new devices using mechanisms such as SNMP Trap based discovery. It must also allow for inclusion and exclusion list of IP address or devices from such discovery mechanisms
    - The proposed solution must provide sufficient reports that identify unused ports in the managed network
    - It should show live interface connections between discovered network devices and must be able to do mapping of LAN and WAN connectivity with granular visibility up to individual port levels.
    - It should be able to automatically generate a notification in the event of a link failure to ensure proper handling of link related issues.

- The proposed solution must scale to large networks while supporting a single web interface for access to reports.

(iii) **Service level Management**

- Solution should support comprehensive SLA management platform
- Manage service levels for delivery and support of business services
- Must allow creating and applying various operational level parameters to Incidents, Requests, Changes, and Release management modules.
- Real-time visualization of service level targets, agreement compliance data, penalties and rewards.
- The SLM module should integrate with incident and problem management to automate escalation, and notification activities based on response and resolution targets
- It should also integrate with change management to provide access to service level agreement details, implementation windows, change blackout periods, and availability requirements
- The application should have a predefined/customizable field to indicate & track the progress/status of the lifecycle of ticket(s). It should contain predefined status codes and allow defining new status codes.
- The tool should provide an audit trail, tracking & monitoring for record information and updates from opening through fulfilment to closure for example: IDs of individuals or groups opening, updating & closing records; dates / times of status & activities updates, etc.

(iv) **System generated Reports by NMS:**

- NMS reports including Bandwidth utilization report & Link up-time report & network equipment health check report on a monthly basis.
- Network Device Performance Report for each zone, junction and end device and other priority offices on Weekly, Monthly basis.
- New Location Connectivity –Weekly, Monthly
- Asset Report Location wise – Monthly
- Vendor SLA Violation Report – Weekly, Monthly
- Audit Report – Quarterly
- Network Utilization Report – Monthly
- Network performance after Integration (with other network) Reports – every 6 month.
- Device level incidence report- Weekly, Monthly
- Preventive Maintenance Report – Quarterly
- Bidder should also provide on-line Dash board where; the TENDERER or its user departments can get summary view of the entire project and its components and Connectivity and Health Status.
- Successful bidder would generate and provide Reports as stated above periodically. Bidder shall also be under obligation to provide any other reports as asked by the TENDERER or its user departments.

**3.1.2.9 Implementation, Operations and Services & Maintenance of New Junctions and End Points**

- a) In case the TENDERER desires to set up the new Junction points or end points with cameras for the deployment of any of the end point utilities, the charges shall be paid to successful bidder as per the unit price quoted in the price bid. The Complete setup including supply of additional hardware, software installation, commissioning will have to be done by the successful bidder during the contract period. After implementation of the said location, Operation, Services and maintenance of new Junctions/utilities will be applicable at the quoted unit rate of operation, service and maintenance as per the rate as defined in this bid.
- b) Any such new Junctions locations will have to include into the main system and discovered in the NMS, and treated as an existing node and the O&M will also form part of this project.
- c) Thereafter any such locations shall be treated as part of the project and will be monitored under the same SLA's as defined for this project.

**3.1.2.10 License Management**

- a) All the software licenses should be in the name of the TENDERER
- b) Successful bidder shall keep the record of all the software licenses and track software usage throughout the IT setup so as to effectively manage the risk of effective usage of software's.
- c) The successful bidder shall avoid the unauthorized usage of Licensed Software. In the event of any claim asserted by Third Party of Infringement of Copyright, Patent or Trademark arising from the use of IT

components or software, the successful bidder shall be entirely responsible to extinguish such a claim. If the successful bidder fails to comply and the TENDERER is required to pay the compensation to the Third Party resulting from such infringement, the O&M agency shall be responsible for the compensation including all expenses, court costs and lawyer fees.

#### 3.1.2.11 MIS Reports

- a) The successful bidder shall submit the reports on a regular basis (the reports may be soft copy / hard copy or both, as required by the TENDERER from time to time) in a mutually decided format. The following is only an indicative list of MIS reports that may be submitted to the TENDERER or its user departments:
- (i) City Wise Bandwidth Utilization, total traffic, peak Traffic etc.
  - (ii) Overall Network Bandwidth Utilization.
  - (iii) Summary of resolved, unresolved and escalated issues / complaints
  - (iv) Component wise Report (Server, Network, Security devices, other utility hardware, Backup, Website Updation, etc.)
  - (v) SLA Reports
  - (vi) Log of preventive / scheduled maintenance undertaken
  - (vii) Any other report as may be required from time to time

#### 3.1.2.12 O&M of Physical Infrastructure:

- a) All the devices installed as part of the physical infrastructure should be monitored and managed on a 24x7x365 basis. The physical infrastructure management and maintenance services shall include, but not limited to the following:
- (i) Operation and management and proactive monitoring of the entire Physical infrastructure installed at both levels i.e. city level, District level control centres as well as the central CCC.
  - (ii) Management of Physical Access to the premises as per the policies set by the TENDERER or its User departments.
  - (iii) Monitoring, recording and reporting usual and unusual movements in and around the premises.
  - (iv) Material inward/ outward control as per policies set by the TENDERER or its User departments.
  - (v) Monitoring and managing safety and surveillance equipment like CCTV, Access Control, Fire detection and Suppression etc. at the city Control Centre(s) and the CCC.
  - (vi) Issuing access control as per approval from the TENDERER or its User departments.
  - (vii) Reporting incidents to the TENDERER and its User departments.
  - (viii) Co-ordinate with respective trusted personnel and communicate with authorized maintenance personnel for various utilities at the city Control Centre(s) and the CCC as required.
  - (ix) Vendor Co-ordination for various physical Infrastructure components
  - (x) Component that is reported to be down on a given date should be either fully repaired or replaced by temporary substitute (of equivalent or higher configuration) within the time frame indicated in the Service Level Agreement (SLA). In case the selected bidder fails to meet the above standards of maintenance, there will be a penalty as specified in the SLA.
  - (xi) The selected bidder shall also maintain records of all maintenance of the system and shall maintain a logbook on-site that may be inspected by the TENDERER or authorized authority.
  - (xii) CCTV footage is to be kept to meet legal, regulatory, ISO Policies compliance requirements. The record retention period shall be as per policies of the TENDERER.
  - (xiii) Ensure availability of the physical Infrastructure including Power, Cooling, CCTV, Access Control, Fire detection and suppression systems, and other components included as part of physical Infrastructure related services for the Control Centres and the CCC.
  - (xiv) For the Physical infrastructure installed at site locations such as Junction boxes, Poles, Towers, casings etc. the Successful bidder will have to keep a check of such items and maintain the same from weather conditions, rodents etc. for the entire duration of the contract.
  - (xv) Proactive and reactive maintenance, repair or replacement of defective components (IT and Non-IT/ Hardware and Software) related to Physical Infrastructure systems and sub-systems. The cost of repair and replacement shall be borne by the selected bidder.
  - (xvi) The selected bidder shall have back-to-back arrangement with the OEMs and shall provide a copy of the service level agreement signed with respective OEMs.
  - (xvii) The Bidder shall maintain documentation for installation, testing, commissioning of any system/sub-systems that is installed or upgraded.
  - (xviii) Acceptance test shall be carried out for any system that is installed and/or upgraded.

- (xix) The bidder shall carry out comprehensive fire drills as per Policy/Guidelines specified by the TENDERER and submit drill reports to the TENDERER on regular intervals.
- (xx) The Bidder shall record all the incidents/issues related to physical infrastructure services, security, systems and Sub-systems.
- (xxi) The bidder shall carry out Risk assessment of the Physical Infrastructure as per Policy/Guidelines specified by the TENDERER and provide a Risk Assessment report including recommendations.
- (xxii) The bidder shall provide training to resources deployed at periodically.
- (xxiii) Full compliance to all the policies, procedures, processes, guidelines, Government- Acts, Rules & Regulations, etc. The bidder shall provide full compliance/adherence of all activities performed by them, to the aforementioned statutes, without any additional cost to the TENDERER.
- (xxiv) The successful bidder will be responsible for the integration of the Cameras with the recording servers and ensure that at least 15 days on primary and 30 days on the secondary storage units.

### 3.1.2.13 Manpower Requirement

- a) The minimum requirement of manpower resources, their qualification and responsibility of each resource is given below. The bidder has to ensure that appropriate qualified manpower with requisite skill sets is deputed for the project.
- b) The bidder shall depute the resources as per the requirements for carrying out the O&M Activity and maintaining the SLA. This is minimum indicative list of resources and based on actual requirements, the bidder may deploy any number of resources to meet the SLA. The TENDERER shall not pay any cost for additional resources required to operate, maintain, monitor & manage the project as per the SLA.
- c) In case deputed employee/staff is not available or is on leave, the bidder is required to provide the alternative personnel with same or higher technical capabilities of the non-available personnel.
- d) The manpower deployment for the project should only be done after a proper written approval/permission from the TENDERER or its User department. The bidder will have to replace any person, if not found suitable for the job.
- e) The manpower to be deployed under this project should be without any criminal background / record. The TENDERER or its User department reserves the right to carry out background check of the personnel proposed on the Project for verification of criminal record, at the beginning of deployment or during deployment.
- f) All the manpower shall have to undergo training from the successful bidder for at least 15 working days on the working, understanding and Operations of project components. Training should also cover dos & don'ts and will have few sessions from the TENDERER and its User department officers on right approaches for monitoring the feeds.

S/N	Designation	Qty.	Roles & Responsibilities	Desired Qualification
<b>A. State Centre</b>				
1	Nodal officer/ Project Manager- Operations	1	<ul style="list-style-type: none"> <li>• Overall in-charge of Project Implementation, O&amp;M of the complete project infrastructure.</li> <li>• Coordinating with third party agencies, bandwidth operators and software/equipment's vendors.</li> <li>• Should be the single point contact (SPOC) for managerial responsibilities and direct interface with the TENDERER.</li> <li>• Responsible for ensuring timely delivery of deliverables for each of the project components.</li> </ul>	<ul style="list-style-type: none"> <li>• BE /B. Tech (CS or IT) with M. Tech /MBA/ PMP</li> <li>• 10+ Years of Post Qualification Experience in large scale ICT infrastructure projects.</li> <li>• <b>Relevant Exp.:</b> 5+ Years of experience as a project manager of large scale ICT infrastructure or WAN/MAN Projects.</li> </ul>

S/N	Designation	Qty.	Roles & Responsibilities	Desired Qualification
2	Technical Manager cum Network Expert	2	<ul style="list-style-type: none"> <li>Responsible for overall management of the IT Infrastructure of the project</li> <li>Should be responsible for effective Technical Resource management, System &amp; Resource planning, based on business forecast</li> <li>Responsible for overall deployment, Integration, upkeep and maintenance of all the IT components including hardware, software, Databases etc.</li> </ul>	<ul style="list-style-type: none"> <li>BE /B. Tech (EC) with CCNP or higher certification</li> <li>7+ Years of Post Qualification Experience in large scale ICT infrastructure projects.</li> <li>Relevant Exp.: 3+ Years of experience as a network manager of large scale ICT infrastructure WAN/MAN Projects.</li> </ul>
3	Manager Operations- CCC (state Center)	1	<ul style="list-style-type: none"> <li>Managing day-to-day activity and operations of CCC</li> <li>Technical expertise in managing the daily operational needs and requirements of the CCC including trouble shooting and problem resolution.</li> </ul>	<ul style="list-style-type: none"> <li>BE /B. Tech (EC/IT)</li> <li>5+ Years of Post Qualification Experience in ICT infrastructure projects.</li> <li>Should have working experience of proposed or similar OEM technology of CCC system</li> </ul>
4	VMS software Expert	4	<ul style="list-style-type: none"> <li>Responsible for managing the end to end Video Management software and services.</li> <li>Expert in generation of various MIS reports on regular basis or on demand.</li> <li>Should act as a technical software expert handholding employees working on software and perform required trouble shooting activities</li> <li>Need to configure/re-configure smart utilities on the software and dashboard</li> </ul>	<ul style="list-style-type: none"> <li>BE /B. Tech (EC/CS/IT)</li> <li>5+ Years of Post Qualification Experience in surveillance projects.</li> <li>Should have working experience of proposed or similar VMS Software</li> </ul>
5	CCC & Video analytics software expert	4	<ul style="list-style-type: none"> <li>Responsible for working on different modules of smart surveillance system i.e. RLVD, ANPR, , Speed Detection etc.</li> <li>Need to work pro-actively and generate various MIS report on demand or regularly</li> </ul>	<ul style="list-style-type: none"> <li>BE /B. Tech (EC/CS/IT)</li> <li>3+ Years of Post Qualification Experience in surveillance projects.</li> <li>Should have working experience of proposed or similar system/software</li> </ul>
6	Network cum security Administrator	2	<ul style="list-style-type: none"> <li>The resource should be able to administrate and manage the NMS Tools</li> <li>Managing and monitoring Network operations</li> <li>Responsible for monitoring of adherence to defined SLA by vendors by making effective utilization of deployed NMS tools</li> </ul>	<ul style="list-style-type: none"> <li>BE /B. Tech (EC) with CCNP or higher certification</li> <li>4+ Years of Post Qualification Experience in large scale ICT infrastructure projects.</li> <li>Relevant Exp.: 2+ Years of experience of working of NMS Tool</li> </ul>

S/N	Designation	Qty.	Roles & Responsibilities	Desired Qualification
7	Storage and Backup Engineer	2	<ul style="list-style-type: none"> <li>• Backup of operating system, database and application as per stipulated policies.</li> <li>• Monitoring and enhancement of the performance of scheduled backups, schedule regular testing of backups and ensure adherence to related retention policies.</li> <li>• Ensuring prompt execution of on-demand backups of volumes, files and database applications whenever required.</li> <li>• Real-time monitoring, log maintenance and reporting of backup status on a regular basis. Prompt problem resolution in case of failures in the backup processes.</li> <li>• Media management including, but not limited to, tagging, cross-referencing, storing, Retrieving, archival logging, testing, and vaulting in fire proof cabinets.</li> </ul>	<ul style="list-style-type: none"> <li>• BE/B.Tech/MCA in computer science/ IT</li> <li>• 5+ years of Post Qualification experience</li> <li>• 3+ years of experience in NAS/ SAN or TMS backup environment</li> </ul>
8	Engineer Server Management	2	<ul style="list-style-type: none"> <li>• Managing server infrastructure installed under the project</li> <li>• Responsible for system configuration, scalability, performance, load balancing, OS administration / management, troubleshooting &amp; Debugging and monitoring of servers.</li> <li>• Implement the back-up plan for storing and retrieving of data, maintain servers, machines and also responsible in resolving the real time (RT) requests as per SLA.</li> </ul>	<ul style="list-style-type: none"> <li>• BE /B. Tech (IT/CS)</li> <li>• 2+ years of similar type post qualification experience</li> </ul>
9	Database Administrator	2	<ul style="list-style-type: none"> <li>• Responsible for database administration, and application change management procedure.</li> <li>• Responsible for management of database repository, creation, deletion, modification, backup and restore of databases and their tables.</li> </ul>	<ul style="list-style-type: none"> <li>• BE /B. Tech (IT/CS)</li> <li>• 2+ years of similar type post qualification experience</li> </ul>
10	Application level support	6	<ul style="list-style-type: none"> <li>• Troubleshooting, monitoring and maintenance, resolution of queries during the O&amp;M</li> <li>• Application development during the O&amp;M phase of the solution, for additional functionalities, variation in existing functionalities</li> </ul>	<ul style="list-style-type: none"> <li>• Minimum 6 years of experience as developer in the programming language used for the applications</li> </ul>
<b>B. District/Local Site</b>				
1	Control centre Supervisor (1@ each Location)	39	<ul style="list-style-type: none"> <li>• Overall In-charge Operation and Maintenance of the Control Centres</li> <li>• Co-ordination with various stakeholders / agencies for resolution of issues/problems etc.</li> <li>• Responsible for end to end functioning and uptime of CCC and its related infrastructures</li> </ul>	<ul style="list-style-type: none"> <li>• BE /B. Tech (EC/IT) with MBA</li> <li>• 5+ Years of Post Qualification Experience in large scale ICT infrastructure projects.</li> <li>• Relevant Exp.: Must have an experience of managing command and control center</li> </ul>

S/N	Designation	Qty.	Roles & Responsibilities	Desired Qualification
2	Network Engineers Cum Security Expert (1 @ each DC)	33	<ul style="list-style-type: none"> <li>• Installation, commissioning, Troubleshooting, of all the network equipment available in the area of a zonal office</li> <li>• Maintenance, Monitor &amp; Support for network equipment of zonal, ward, Junctions/locations offices.</li> <li>• Regular update of software patches, antivirus etc.</li> <li>• Any other activities as and when required.</li> </ul>	<ul style="list-style-type: none"> <li>• BE /B. Tech with CCNA or higher certification</li> <li>• 2+ years of similar type post qualification experience</li> </ul>

Note:

These are the minimum indicative list of type and quality of resources required. However, bidder is free to put additional manpower wherever required for the necessary Operations, maintenance and support to comply with the required service levels as per the RFP/contract agreement with no extra cost to the TENDERER.

### 3.2 Implementation Timelines

S/N	Deliverables	Timeline
1.	a. Signing of contract agreement b. Submission of performance Bank Guarantee	Within 15 calendar Days from date of issuance of LOI/ Work order
2.	Implementation Roadmap, plan and execution strategy document (Include feasibility study, site survey, fixtures, Edge devices, coupling, clamp, pole, Gantry etc.)	Within 30 calendar days of issuance of LOI/Work order
3.	Delivery of the IT and Non-IT Equipment of central Infrastructure as defined in BoQ (hardware and software) at a central location/Vendors Warehouse	Within 45 calendar days from the date of Approval of the PoC
4.	Delivery of <b>Edge Location Infrastructure</b> like Cameras, Switches, Junction Boxes, UPS etc. at central location /Vendors Warehouse of respective City/Locations	1 <sup>st</sup> Lot: 25% of the Work order – within 45 calendar days 2 <sup>nd</sup> Lot: 50% of the Work order -within 60 calendar days** Final Lot: Remaining 25% of the work order- within 90 calendar days** <b>**from the date of approval of PoC</b>
5.	Proof of concept for 50 CCTV cameras, with VMS detection and challan generation for speed limit violation and RLVD, ANPR (Instead of central side solution for the application, cloud based solution allowed for the POC, will have to use CCTV camera from 3 different OEMs)	<b>30 days from Lol/Work order</b>
6.	Development/Customization and testing of the proposed software / Mobile Application(s) (central side infrastructure)	Within 90 calendar days from the date of approval of PoC
7.	Installation and Commissioning and FAT of hardware/software at end point Locations	Within 150 calendar days from the date of approval of PoC

**Note:**



- 1.) FAT evaluation will be done within 15 days of reporting by the TENDERER
- 2.) Rectification of faults, if any, reported during the FAT and go live of solution - one month from the providing of feedback by the TENDERER on FAT

**Proof of Concept (PoC):**

- 1.) Successful bidder has to successfully demonstrate the proposed solution within the 30 days from the date of LoI (letter of Intent). The TENDERER will not be liable to pay/reimburse any type of cost incurred by the successful bidder pertaining to the PoC.
- 2.) During the PoC, successful bidder is required to deploy at least 50 CCTV cameras with all systems (ANPR, RLVD, Speed Violation,) at the locations specified by the TENDERER.
- 3.) The Bidder is free to choose make and model (3 different OEM's) for the PoC of the CCTV. However out of these 3 OEMs one make and model must be the same which is proposed/quoted in the Technical and price bid by the bidder.
- 4.) The POC shall be done to showcase the requirements of the said system(s) as specified under the scope of work and in compliance to the technical specification as laid down in this RFP
- 5.) The bidder will have to successfully qualify the POC based on the parameters defined below. In case if the successful bidder fails to achieve the required benchmark as mentioned, then in such a case, the successful bidder will have to re-demonstrate the PoC (all component's or part of the system/component) within 7 days, and will have to successfully qualify the same.
- 6.) Please note that if the successful bidder fails to complete Proof of concept or perform as per the requirement of the TENDERER even after the second attempt, then his EMD will be forfeited, contract terminated, and the work will be assigned to L2 bidder, subjected to his acceptance, at cost to the successful bidder.
- 7.) The proof of Concept will be evaluated based on the below mentioned criteria: on the components given below:

Sr. No	Component	Functionality to be Demonstrated	Benchmark Achieved
1.	CCTV Cameras	CCTV feeds of 50 cameras (3 different OEM's) are all discoverable in VMS and can be seen simultaneously on monitors (TV/PC monitor)	Yes/ No
2.	RLVD/ANPR System	Reporting of the event of violations by the RLVD/ANPR solutions along with the contextual screen shots with sufficient accuracy (as demanded in this RFP) for recognition of number plates	Yes/ No
3.	CCTV Camera	In few cameras with auto zoom, auto focus, (2 or 3 cameras may be shown) whether it is possible to zoom from remote location (depicting a control room) from lowest to highest focal length with auto focus	Yes/ No
4.	CCTV Camera	Does the camera work as per the required wide dynamic range. This will be tested during night time by positioning a car with head lamp focusing in the camera and minimum 60% of viewing area of camera will contain lateral space (Horizontally) outside the car to see if the details of headlamp, car frame, and an object located 15 feet away from car when the car and objects are placed 50 feet away from the camera, are clearly discernible. And	Yes/ No

Sr. No	Component	Functionality to be Demonstrated	Benchmark Achieved
		object being visible clearly.	
5.	Quality of Video Feed for Surveillance cameras (Fixed, PTZ)	Video Quality as acceptable to the TENDERER under different Light Conditions	Yes/ No

### 3.3 Roles and Responsibilities

S/N	Stakeholders	Roles and Responsibilities
1	<b>Successful Bidder</b>	<ul style="list-style-type: none"> <li>• Detailed Implementation Plan including site survey/feasibility study</li> <li>• Supply, Installation, Commissioning and operations &amp; maintenance of the ordered Items and Infrastructures for the period of 5years</li> <li>• Development of test cases for UAT &amp; FAT</li> <li>• Integration with the various existing systems</li> <li>• Provide necessary and qualified manpower for the entire Project duration</li> <li>• Obtain required clearances/ approvals from appropriate authorities</li> <li>• Adherence to the regulatory requirements</li> <li>• SLA compliance</li> </ul>
2	<b>TENDERER</b>	<ul style="list-style-type: none"> <li>• Providing required physical infrastructure at the operation centres of SHQ/DHQ/City with complete Civil and electrical Infrastructure such as Power, seating space, Air Conditioning, Furniture's, Flooring, DG Set etc.</li> <li>• Payment to successful bidder</li> <li>• To provide necessary space for edge equipment erection/installation.</li> <li>• IP schema/ Pool for the network and IP equipment</li> <li>• RAW power/electricity. However, extension till the last mile/actual utility will be in the scope of successful bidder.</li> <li>• To help and assist Successful Bidder for obtaining necessary clearances/approvals from appropriate authorities</li> </ul>

***SECTION-IV***  
***TECHNICAL SPECIFICATIONS***

# Technical Specifications

## 4.1 Video Management System

S/N	Specification
<b>1.) General Features</b>	
a.)	The Video Management System (VMS) should provide the software infrastructure and tools for the management of video surveillance systems, including the recording, transmission, viewing, analytics and event management of video, audio and other data.
b.)	The VMS should seamlessly support audio and video inputs from all types of video recorders: Networked Video Recorders (NVR), Smart Video Recorders (SVR) or Intelligent Video Recorders (IVR) and combinations of the above.
c.)	The VMS should provide a seamless integration between all recorders types under the same user interface and management system.
d.)	The VMS should have a central database (AMS) for consistent configuration of site equipment and user data. The centralized management shall be available from remote locations over the network.
e.)	The VMS should provide virtual matrix (VMX) features and capabilities allowing full switching and control of the VMS inputs via a GUI and/or CCTV keyboard.
f.)	The VMS should provide viewing capabilities by web browsing, supporting laptops, smart phones and tablets for remote viewing without any installation on the viewing device.
g.)	The VMS should have seamless redundancy solution for its main components: the central database, Central Video Storage Servers, and the distributed video recorders and database
h.)	The VMS should have seamless redundancy solution for its main components: the central database, Central Video Storage Servers, and the distributed video recorders and database
i.)	The VMS should support remote independent sites that are connected to a central site, allowing to have a hierarchy of independent VMS systems.
<b>2.) Operational Capabilities</b>	
a.)	The VMS application suite should include applications for viewing and investigation of video, user policy setup, site setup and configurations, and an application for monitoring and providing alarms of failure or errors of any of the VMS components.
b.)	The VMS should support various architectures, centralized and/or distributed.
c.)	The VMS should be suitable for 'pure-IP' installations using the components (recorders, management application etc.).
d.)	The VMS should be fully scalable both in terms of number of cameras that can be added (simply obtain additional licenses to support thousands of cameras as well by the ability to enjoy advanced features that can be also enabled by license update.
e.)	The VMS operator application should allow authorized users to monitor and playback video from cameras connected to the VMS, on local workstation and/or external monitors.
f.)	The VMS operator application should allow authorized users to monitor, record and playback audio from audio sources connected to the VMS.
g.)	The VMS should support multi-monitors scheme, enabling floating viewing windows which can be allocated to additional monitors connected to the same workstation. User shall be able to set the following: <ul style="list-style-type: none"> <li>a) Video Layout</li> <li>b) Map Display</li> <li>c) Visual navigation of Events/alarms or user customized screen display</li> </ul>
h.)	User shall be able to present several types of sensors per viewing window, and several pages can be created as tabs, allowing multi functionality viewing window
i.)	The VMS operator application should graphically display camera states on the hierarchical list, the states shown shall include indication of:

	<ul style="list-style-type: none"> <li>a.) Loss of the video signal or some other failure</li> <li>b.) Alarm, triggered by a sensor, a rule or manually,</li> <li>c.) Disconnected, indicated that the recorder for that camera is disconnected</li> <li>d.) State change acknowledged</li> <li>e.) Armed mode – Processes alarms and failure alarms for selected sensors/cameras or all sensors/cameras in a group</li> <li>a.) Disarmed mode – Disables any rules or automatic actions for selected sensors/cameras or all sensors/cameras in the group but still processes alarms and failure alarms</li> <li>b.) Bypass mode – Ignores all activity (sensor/camera is still armed but does not go into alarm or trigger actions upon activity).</li> <li>c.) Association with audio channel.</li> <li>d.) Recording status (recording or not recording).</li> <li>e.) Indication of camera type (PTZ or fixed cameras).</li> </ul>
j.)	The VMS operator application should allow the user to monitor and playback video on a full screen or a camera layout page displaying 1, 4, 7, 8, 9, 10, 13, 16 or 25 cameras. In case multi monitor is used, there is no limit to the number of monitors
k.)	<p>The VMS should support digital zoom on the workstation or external monitors (analog or digital). The user shall be able to perform digital zoom magnification up to 20 times, digitally zooming in up to 672% of the original size.</p> <ul style="list-style-type: none"> <li>a.) The zoom feature shall be available on monitor and playback modes.</li> <li>b.) The zoom feature shall provide Digital PTZ functionality, allowing the user to Pan and Tilt within the zoomed image</li> </ul>
l.)	The VMS should allow the user the ability to define a homepage to be displayed in the local workstation. The homepage shall include a specific layout of video panes and pre-selected cameras either in live or playback modes, as well as other security sensors and maps
<b>3.) Video Playback</b>	
a.)	The VMS should allow the user to perform any of the following actions on played back video: Start and Stop, Pause and Resume, Fast Forward/Fast Reverse, Slow Forward/Slow Reverse, Frame by frame advance or rewind and Loop Replay.
b.)	<p>Instant Playback control:</p> <ul style="list-style-type: none"> <li>a.) User should have the ability to change from a real time live monitoring to a playback and the playback time by dragging the video player timeline.</li> <li>b.) User should have the ability to resume real time monitoring at any with one click of a button.</li> </ul>
c.)	<p>Continuous Playback:</p> <ul style="list-style-type: none"> <li>a.) Playback should never stop as long as there's available recorded video</li> <li>b.) User should have the ability to play recorded video in loop based on a time segment that the user shall be able to mark on the player timeline.</li> </ul>
d.)	<p>Synchronized Playback:</p> <ul style="list-style-type: none"> <li>a.) The VMS should allow the user to play up to 16 synchronized video channels or up to 15 video channels and one audio channel synchronized.</li> <li>b.) The channels that are part of a synchronized playback session shall stay in a session even when changing from playback to live video and back to playback.</li> <li>c.) The VMS should allow adding video channels to, and removing from a synchronized playback session by clicking a button on playing video channels.</li> <li>d.) The VMS should allow video channels to be automatically added to a synchronized</li> </ul>

	<p>playback session when added to the video page.</p> <p>e.) Playback synchronization should support advanced playback operations including fast/slow forward/reverse playback, pause and frame by frame.</p>
<b>4.) Live Monitoring Function</b>	
a.)	The VMS should enable live monitoring, reconstructing the live monitoring view post a failure (network, recorder, etc.) and as a reaction to other conditions including a sensor's state change or an event, as well as based on scheduling
b.)	The VMS should support audio from edge device, enabling both recording and live monitoring of the audio from the remote capture edge device the guard control station.
<b>5.) Viewing Capabilities on Web Browser &amp; Portable Devices</b>	
a.)	The VMS should provide viewing capabilities through web browsing, laptops, smart phones and tablets for remote viewing without any installation on the viewing device.
b.)	The VMS web interface should use the built-in browser and player on the viewing device without any installation.
c.)	The VMS web interface should allow authorized users to monitor and play back video from input channels.
d.)	The VMS web interface should present the VMS channels of the media sources that the user is authorized to view. The media sources should be grouped and organized.
e.)	User should be able to search for a media source name or shortcut alias from the VMS web interface.
f.)	The VMS web interface should all VMS video media sources by providing transcoding services and load balancing between the transcoder services
g.)	VMS video sources should be viewable directly from the web interface without transcoding
h.)	The VMS should be able to minimize the use of transcoding service as much as possible. If there are two or more requests with the same parameters for live viewing, the VMS should not transcode twice, but use the same stream.
i.)	The VMS web interface should be able to control PTZ cameras from the active output or from the PTZ control panel and allow moving a PTZ camera to a preset.
j.)	The VMS web interface should support English language
k.)	The VMS web interface should support Single Sign On (SSO) Facility.
l.)	Upon user re-login, the VMS interface should be able to restore video streaming from the time when it was stopped.
m.)	The VMS web interface should support media export to AVI, MPEG or to any proprietary VMS file format (i.e. w/o transcoding).
n.)	The VMS web interface user should be able to forward video by e-mail to another web interface user. The e-mail shall include the URL to reconstruct the display layout.
o.)	The VMS should provide LoS support in MPEG4, H.264 or H.265 for monitoring of streaming devices. Therefore, it shall automatically select the most appropriate stream from the edge device in accordance with the workstations/decoder performance and network bandwidth
p.)	<p>The VMS viewing application should provide the capability to manage CPU resources and bandwidth utilization on the user's network. The following options shall be independently configured for each workstation:</p> <ol style="list-style-type: none"> <li>(1) Best Available – Provides the user with the highest resolution, bit-rate and frame-rate possible based on the available network bandwidth.</li> <li>(2) Pre-defined Bandwidth Limits – Provides the user with pre-defined bandwidth limits presets</li> <li>(3) User-defined Bandwidth Limits – Allows the user to manually set the maximum bandwidth the Control Application can use</li> </ol>
<b>6.) PTZ Control</b>	
a.)	The VMS viewing application workstation shall provide support for PTZ Keyboards to allow authorized users of the control room of district/city level as well as the CCC level administrator to control PTZ cameras

b.)	<p>VMS PTZ Presets</p> <p>(1) The VMS viewing application should allow authorized users to create new PTZ presets.</p> <p>(2) The VMS viewing application should allow authorized users to call up PTZ presets (via GUI and/or CCTV keyboard).</p> <p>(3) The VMS should allow authorized users to predefine a home-preset to each camera and a predefined timeout after which a PTZ camera, if was not handled by any user, will return to the home preset.</p> <p>(4) The VMS should present the PTZ preset name on OSD when moving to a PTZ preset</p>
c.)	<p>VMS VA presets:</p> <p>i.) User should be able to associate for each VA application a PTZ preset.</p> <p>ii.) When the PTZ camera reaches the preset, the VA application shall be activated, When the PTZ camera leaves the preset the VA application shall be deactivated.</p>
d.)	The VMS should be able to enable independent PTZ camera speed for each Pan, Tilt and Zoom axes, iris control and focus and should also support all supported speeds of the PTZ camera
e.)	<p>The VMS viewing application shall support PTZ control from:</p> <p>i.) The video viewing window by referencing mouse location on the video window</p> <p>ii.) Graphical joystick with speed control</p> <p>iii.) support PTZ zoom control via the mouse wheel</p>

### 7.) Media File Export

a.)	VMS should allow the user to export a clip to a file
b.)	It should be able to export\burn a number of clips at the same time. Along with size and format details
c.)	It should be able to export H.264/ H.265 compressed video to a standard MKV file format without transcoding
d.)	Executing an export job should run in the background and not lock the user from continuing to operate the VMS client application
e.)	Upon completion of the export job the VMS should display a notification message with a link to the target folder of that export.
f.)	User shall be able to mark a time segment on a playback's timeline and add that segment to the export jobs window.

### 8.) Map Interface

a.)	The VMS should allow the user to open a page layout that includes maps as well as other video windows
b.)	The VMS should be able to display a list of maps allowing easy navigation through all available maps.
c.)	The VMS should allow the user to perform operations on cameras or any other end device that are places on a map.
d.)	The VMS should allow the user to click on an indicator on the map and drill down to additional linked maps
e.)	The VMS should allow the user to zoom into the map and select a "fit to screen" option which will stretch the current map onto the available map space on the current layout.
f.)	The VMS should allow the user to "drag & drop" a camera from the map area to a video window or to click on a camera to start viewing it in a pop-up window.
g.)	The VMS should provide the user with an indication of alarm or change in state, when a camera is "Triggered" or has lost signal connectivity due to various reasons such as power, connectivity etc. ,the user will see the alarm on the map and support – icon change, icon resize, icon border color change, hide/show icon, overlay icon.
h.)	The VMS should allow administrator users to place the following components on maps: cameras (including indication of their angle) as well as linked maps and pages, and links to preprogrammed automatic actions.
i.)	The VMS should allow calibrating maps to geographical coordinates
j.)	The VMS should allow the user to search for an entity on the map using a free-text search field.
k.)	Each user should be able to view part\all the maps, based on privileges associated with the user role

### 9.) Tour Support Feature

a.)	The VMS viewing application should support “Tour feature” allowing the user to monitor several video input channels, in a single window in a cyclic succession.
b.)	User should have the ability to configure from one to any channel in which to display a sequence of touring cameras.
c.)	The VMS viewing application should have a tab containing all preconfigured-tours and should be capable to group tours into a hierarchy tree for easy access.
d.)	User should have the ability to progress to the next camera in the tour or go to previous camera in the tour, regardless of the predefined dwell time
<b>10.) Paging Feature</b>	
a.)	The VMS should support a page feature allowing the user to save any of the available video layouts while assigning specific cameras and/or other sensors and/or tours and/or maps to each tile in the layout. The user can later, from the VMS viewing application, call up the page manually or upon alarm.
b.)	The VMS should have tab per saved page and should be able to group pages into a hierarchy tree for easy access.
c.)	A page can be edited and saved with changes made to its name, shortcut and content.
<b>11.) Video Wall / External monitor management</b>	
a.)	Authorized user should have the access to call up cameras/tours on external monitors connected to the VMS decoders
b.)	Authorized users should be able to switch to an external monitor view mode by selecting a specific control room/ monitor layout GUI.
c.)	The VMS should allow the user to assign a shortcut to each external monitor
d.)	User should be able to control playback session, playing on the wall, even if it was started by another user.
<b>12.) Alarm Management</b>	
a.)	The VMS should support management of alarms based on VMD, AVMD, Video Analytics Application, 3 <sup>rd</sup> party input via API, TTL, and edge device events
b.)	Actions Associated with Alarms. (1) The VMS should allow associating a system action to an alarm. (2) Each alarm should change the icon of the alarmed sensor indicating its alarmed state. (3) Each alarm should have the capability to be assigned to individual users or to user groups (roles). (4) User should have the ability to set or filter cameras and any other sensor in the cameras /tree according to the alarm state or that sensor.
c.)	Alarm Notification (1) The VMS should support the following methods of notifying users that a video alarm has occurred: i.) Indicate the alarm of a camera in the main cameras list. ii.) Alarm video pop-up on local or external monitors. iii.) Audio notification may be sounded when the event occurs. iv.) API – Notifies a third-party security system that a video alarm has occurred. v.) TTL/Relay – Activates a TTL/Relay to drive an external alarm device. vi.) Integrated sensor – send a command to a sensor of an integrated 3 <sup>rd</sup> party system. (2) The VMS should support standard SNMP for notifying that a maintenance alarm has occurred.
d.)	Alarm Display on Local Workstation (Pages) i.) User should have the ability to associate each video alarm with a pre-defined alarm page which contains a video pane layout and pre-configured cameras in live or playback mode. ii.) User should have the ability to configure a different alarm page for each alarm in the system. iii.) User shall be able to associate alarms with a pre-defined page to be automatically displayed on one or more external monitors upon an alarm.
e.)	Automatic Actions upon Alarm (1) User should have the ability to define rules to automatically execute actions upon an alarm condition. (2) Automatic actions upon an alarm condition shall include the following actions: Send command to



	camera, Play page locally, Play page on external monitor, Display live video, Display playback video, Close video, Move camera to PTZ preset, Start/Stop Virtual Tour, Start/Stop recording, Play a predefined sound, Send an HTTP request, Execute an external application locally on the operator workstation.
f.)	<p>Alarm/Incident Workflow</p> <p>(1) User should have the ability to define a workflow for each event.</p> <p>i.) User should have the ability to define a procedure containing a list of tasks instructing the operator what actions to take when an alarm occurs. Other users shall be able to see the status of each task for a specific event on the respective workstation.</p> <p>ii.) The workflow should be adaptive to the user's selections and change the remaining tasks in the workflow based on conditional tasks that present multiple options to proceed.</p> <p>iii.) The workflow should support simple tasks that can be managed (e.g. completed) manually, as well as automatic tasks that execute an automatic action that performs a system command and/or a sensor command.</p> <p>iv.) Automatic actions executed as automatic tasks in a workflow procedure shall support creating, closing and changing incidents.</p> <p>v.) User should have the ability to change the state of each task to: Suspend, In Progress, Complete, Cancel and Fail.</p> <p>(2) User should have the ability to acknowledge, reject or reset each alarm – after the alarm has been acknowledged all authorized users shall see the alarm status change on their respective workstations.</p> <p>(3) The system administrator should have the ability to audit user alarm actions (acknowledge /reject/reset).</p> <p>(4) The system administrator should have the ability to simulate a change in a sensor's state by enforcing a synthetic change of the sensor's state.</p>
g.)	<p>Alarm/Incident Escalation</p> <p>i.) User should have the ability to define escalation profiles to incidents.</p> <p>ii.) Alarm/Incident which was not handled by its originally assigned user will be escalated to other user profiles after predefined time.</p> <p>iii.) The system administrator should be able to configure automatic actions that can be performed upon escalation of an alarm/incident or when an escalation ends.</p>
h.)	<p>PTZ Alarm Presets</p> <p>i.) User should have the ability to define a set of presets for each PTZ camera.</p> <p>ii.) Each of these presets may be associated with an alarm.</p> <p>iii.) Upon an alarm the associated PTZ camera(s) will automatically move to the specified preset</p>
i.)	<p>Maintenance Alarms</p> <p>(1) A standard 3<sup>rd</sup> party technical supervisory application should be available to the system technical supervisor, providing indications on the system's components viability.</p> <p>(2) Each of the supervised units shall be listed with the following:</p> <p>(a) Indication that the supervised unit is working properly.</p> <p>(b) Number of alarms.</p> <p>(c) Date and time of latest alarm.</p> <p>(3) Maintenance alarms may initiate the transmission email and/or SNMP Trap using a standard 3<sup>rd</sup> party technical supervisory application.</p>
<b>13.) Incident Management</b>	
a.)	The VMS should allow the user to manage events as incidents that are associated with specific context, including custom pages of video cameras, recorded video playback, maps, as well as textual description
b.)	Incident should include associated predefined operational workflow procedures to provide the operator structured guidance as well as assistive information for successfully managing an incident.
c.)	Incident should allow collaboration by involving other system users as stakeholder that can have access to the incident and contribute to the incident's management by completing tasks and adding information to it.

d.)	The VMS should allow users to create a new incident that includes the relevant context in the form of the relevant entities (e.g. map, cameras, video playback) when created from an option within the entity's representation in the GUI.
e.)	The VMS should allow users to drag an indicator and drop it on a map to create a new incident at that point where the indicator was dropped, making the incident associated with that position.
f.)	The incident management should allow communication between its stakeholders through a textual message board.
g.)	The VMS should have a dedicated Incident screen intuitively providing situation decision guidance support.
h.)	The VMS should have the following Incident creation options: automatically as a result of pre-configured rules, on demand by operators or from scheduled triggers
i.)	The VMS should support various methods of incident assignments: claiming by acknowledge, automatic assignment according to various or assigning to a supervisor, who dispatches incidents to operators according to his/her considerations
j.)	Open incidents on the list should be automatically sorted according to the following criteria: first by severity and then by time (more recently opened incidents first)
k.)	The VMS should have the capability to record defined procedural actions taken when managing the incident.
l.)	The VMS should have the capability to record operator screens when managing the incident for the purpose of future debriefing.
m.)	The VMS should have the ability to update and escalate incidents that were either open beyond a predefined period of time or not managed within a predefined time.
n.)	The VMS should "pop-up" notifications when incidents are created and when they are escalated
o.)	The VMS should allow to capture comments upon incident closure. Comments can be predefined quick comments and/or custom text
<b>14.) Audit Reports</b>	
a.)	The VMS should provide detailed Audit Reports on need and time basis
b.)	User should have the ability to generate, view and export the Audit information, including Event ID, Source, Type, Time, User, Computer IP and specific parameters according to the source type.
c.)	User should have the ability to filter audit records based on selected users, record types, computer IP, timeframe and level (Information, Warning, Error and Critical)
<b>15.) Video Dashboard</b>	
a.)	User should be able to generate a site report of the recorders, storage and edge devices configuration connected to the VMS and present it as a dashboard table.
b.)	The VMS should be able to present a view of all the site channels information including retention days, oldest recording time, edge device model and vendor, compression, resolution, etc.
c.)	The VMS should be able to present a view of all the site recorders with maintenance information such as IP address, number of channels, version, OS, Physical memory, CPU type, storage capacity, throughput, etc.
d.)	User should be able to export and import the report to a CSV file format
e.)	User should be able to generate a recorder report grouping video channels according to their configured retention. <ul style="list-style-type: none"> <li>i.) Each retention group with a unique color</li> <li>ii.) Pie chart with channels count and required storage according to the configuration</li> </ul>
f.)	User should be able to view VMS recorder storage capacity estimation according to its video channels configuration <ul style="list-style-type: none"> <li>i.) Storage allocation</li> <li>ii.) Exceeding storage allocation due to configuration (bit-rate, retention, etc.)</li> </ul>
<b>16.) SDK for 3<sup>rd</sup> Party Integration</b>	
a.)	The VMS should be provided with extensive SDK, allowing the integration of its different video surveillance components into 3rd party management systems and applications

b.)	The VMS SDK should enable integration of live and playback video to the 3rd party system.
<b>17.) User Authentication and Authorization</b>	
a.)	The VMS should enable the system administrator to define user profiles with different user privileges to ensure secured access to the VMS System, the VMS user management application shall be used by the VMS System Administrator to centrally set-up and maintain user profiles. A user may be associated with multiple user profiles
b.)	Integration Microsoft Active Directory groups
<b>18.) Video Authentication</b>	
a.)	The VMS should provide video authentication for recorded video streams input from edge devices
b.)	The video authentication should be provided for H.265, H.264 and MPEG-4 compressions
c.)	The VMS recorders shall utilize SHA-1 secure hash algorithm to authenticate the recorded video.
d.)	The VMS authentication scheme should be able to detect an altered video stream, a removal of a video frame etc.
<b>19.) Edge recording</b>	
a.)	The VMS recorder should support catch-up of video and/or audio recording from edge device local storage
b.)	The VMS recorder should support catch-up of recording gaps origin from network disconnection between the recorder and the edge device
c.)	The VMS recorder configured for event recording should support catch-up of pre-alarm video from the edge device local storage with the following conditions. <ul style="list-style-type: none"> <li>i.) The edge device is local recording</li> <li>ii.) There should be no live streaming of video from edge device to the VMS recorder for recording of pre-alarm.</li> <li>iii.) Once the edge device initiates an event, the VMS recorder shall request a live stream from the edge device for the event recording.</li> <li>iv.) The VMS recorder shall catch-up the pre-alarm from the edge device local storage. The catch-up may be in parallel to live streaming from the edge device.</li> </ul>
<b>20.) Security</b>	
a.)	The VMS recorders should be able to connect via a secure connection using authentication and encryption <ul style="list-style-type: none"> <li>i.) Authentication - user and password credentials</li> <li>ii.) Encryption – TLS with AES256 cipher</li> </ul>
b.)	The VMS recorder should be able to connect via a secure HTTPS connection to its associated edge devices (IP cameras & encoders)
c.)	The VMS management database connection shall be encrypted using AES256 cipher
d.)	The VMS should encrypt with AES256 cipher the exported proprietary VMS file format when using password protection
<b>21.) Virtualization</b>	
a.)	Redundancy solution should be used to perform VMS recorder redundancy and shall be supported on the virtual infrastructure using industry standard Virtualization solutions.
<b>22.) Camera Tampering Alert</b>	
a.)	The VMS should provide a centralized camera tampering detection solution in real-time by automatically identifying tampering to ensure video image capture and integrity. The solution sends an alert when the following potential tampering is detected: <ul style="list-style-type: none"> <li>• Scene too bright — e.g. flash light, direct sun, laser pointer that is pointed at the camera, causing it to become over saturated.</li> <li>• Scene too dark — not enough light to see a clear image, if camera is covered.</li> <li>• Camera is covered or blocked — if something is blocking or partially blocking most of the camera's field of view.</li> <li>• Camera redirection detection — if camera is redirected from its' initial position of field of view</li> </ul>

(FOV).

- Unfocused or blurred view — if the camera was sprayed with rain or its focus changed.

The System should be able to detect tampering on any IP camera that has been discovered in the VMS and send alerts through SMS, Email for any tampering detected to the concerned officers as well as the control room.

## 4.2 Automatic No. Plate Recognition (ANPR) System

S/N	Specification
1.	Vehicle Detection and Video Capture Module: - The System should automatically detect a vehicle in the camera view using video detection/Still Image and activate license plate recognition
2.	The System should be able to automatically detect the license plate in the captured video feed/Still Image of all passing vehicles irrespective of traffic violation and non-violation
3.	The system shall perform OCR (optical character recognition) of the license plate characters (English alpha-numeric characters in standard and non-standard fonts). The system shall be robust to variation in License Plates in terms of font, size, contrast and color and should work with good accuracy for all type of vehicles i.e. cars, HGV, LGV , PSV and two wheelers
4.	The System shall store JPEG image of vehicle and license plate and store it in a database along with date and time stamp along with site location details.
5.	The System shall be able to capture license plate in day and night operation.
6.	The System should be able to capture license plates for vehicle moving up to the speed of 120 Km/Hours at: <ul style="list-style-type: none"><li>• 90% accuracy for Standard English alpha-numeric fonts and HSRP for both day and night</li><li>• 75% accuracy for non-standard fonts for both day and night</li></ul>
7.	The system should have option to take input of registration numbers according to the hot listed categories like "Wanted", "Suspicious", "Stolen" etc. by authorized personnel.
8.	On successful recognition of the number plate, system should be able generate instantaneous and automatic alarm to alert the control room for vehicles which have been marked as "Wanted", "Suspicious", "Stolen", "Expired". (System should have provision/expansion option to add more categories for future need).
9.	The system shall enable easy and quick retrieval of snapshots, video and other data for post incident analysis and investigations. For example, a database could be searched using criteria like date, time, location and vehicle number
10.	The system should be able to generate suitable MIS reports that will provide meaningful data to concerned authorities and facilitate optimum utilization of resources. These reports shall include. <ul style="list-style-type: none"><li>▪ Report of vehicle flow at each of the installed locations for Last Day, Last Week and Last Month.</li><li>▪ Report of vehicles in the detected categories at each of the installed locations for Last Day, Last Week and Last Month.</li></ul>
11.	The system should be able to store license plates numbers of at least 10,000 suspected vehicles at a time and should generate an Alert in form of Video popup at the Monitor and/or SMS on Cell phones in case such vehicle has been captured by the ANPR system.
12.	The system shall have Search option to tune the reports based on license plate number, date and time, site location as per the need of the authorities.
13.	The system shall have option to save custom reports for subsequent use. The system shall have option to export report being viewed to common format for use outside of the ANPR or exporting into other systems.
14.	The system should provide advanced and smart searching facility of License plates from the database. There should be an option of searching number plates almost matching with the specific

	number entered (up to 1 and 2-character distance).
15.	Should be able to integrate with the Video Management Software to be proposed under this RFP
16.	Should be able to store the details captured in Storage system as per the guidelines received from Home/Police Department

### 4.3 Red Light Violation Detection (RLVD) System

S/N	Specification
1.	The RLVD should use the Video/Image processing techniques to identify the red-light violator
2.	The system should be able to identify red signal light either through the Camera or through the Traffic Controller to know signal status.
3.	The solution should synchronize the record of Red Light violation, Number plate of vehicle and 3 snaps clearly showing the vehicle is crossing the stop line while signal is RED which can be used as evidence where required.
4.	The system should generate Alarms at control room software if any signal is found not turning RED within a specific duration of time.
5.	The system should provide facility to search for the cases of violations occurred during any specific span of time, and provide a statistical analysis of the number of such incidences occurring during various days of the month, various months of the year in graphical forms. A report of all such incidences should be available and transferable in hard copy during any selected span of time.
6.	The accuracy of the RLVD system should be identify Red Light Violations with an accuracy of at least 90% both during day and Night time
7.	The system should be able to show Live video in multiple Matrix (full view, lane view, No. Plate view etc.) layout for all the cameras in the system at real time.
8.	Should be able to integrate with the Video Management Software to be proposed under this RFP
9.	Should be able to store the details captured in Storage system as per the guidelines received from Home/Police Department

### 4.4 Speed Violation Detection (SVD) System

S/N	Specification
1.	The Vehicle Speed Detection system should be a camera based Video analytics system where in the speed of the vehicle is automatically calculated and violations is detected based on the permissible speed limits.
2.	The Automatic Speed Detection application will have to be integrated with the ANPR and e- challan application (to be developed under the scope of this RFP) for the Home Department and the Central Database of the Transport Department (VAHAN Database managed by NIC), such that e challans can be generated by the system through an automated process.
3.	The Camera system shall be capable of measuring speeds with an accuracy of 90% in detecting speed limit violations and photographing the incident.
4.	The system should be capable to detect Speed of the violating vehicle even at very high speed up to 120 Km/ Hour
5.	Both day and night time violations should be captured with the same level of accuracy
6.	The system should be able to generate alarms /alerts based on the vehicles status and category like "Wanted", "Suspicious", "Stolen" etc. as categorized by the e-Gujcop database.
7.	The Speed Violation details and alert and E-challan related videos/ photo feed should go to the central control room, whereas the processing and recording of the video footage of speed violation
8.	Should be able to integrate with the Video Management Software to be proposed under this RFP

9.	Should be able to store the details captured in Storage system as per the guidelines received from Home/Police Department
----	---

#### **4.5 Video Analytics Application**

S/N	Specification
1.	The software/ system should be capable to identify Unattended Objects, Baggage's, Persons, vehicles etc. through video analytics Techniques/Algorithms
2.	The System should support the Object Origin feature
3.	Should generate an Alarm/Alert in case of detection of an Unidentified Object/Baggage
4.	The System Should be capable to do the analytics on Live Video Cameras as well as Stored Video records from such cameras
5.	The applications should also be able to do People search based on a given description/attributed/Sketch/Full length photograph
6.	Should have an interface to Create sketches, Composite (Human like Figure) of the suspect based on description. There Shall be different options available for describing hair color and style, Facial Attributes, shirts, trousers, patterns, etc.
7.	The applications should be able to integrate with the VMS of the Command and Control Center/Control Center
8.	It should support commercial-off-the-shelf computing hardware without the need of any proprietary hardware
9.	Able to produce reliable analytics at lower resolutions like 4CIF resolution in order to save the computation
10.	It should get video from camera or VMS and send alarms to VMS to be viewed in VMS client
11.	It should support multiple regions of analytics on single video feed

#### **4.6 Online UPS for Control Centre (s) and CCC & DC**

S/N	Parameter	Minimum Specification
1.	Output Power Capacity	Adequate capacity to cover all above IT Components at respective location
2.	Technology	True On-line High-Frequency Design UPS with Double Conversion technology
		Rectifier & Inverter both to be IGBT based PWM
3.	Certifications	ISO 9001:2000 and 14001 Certified OEM (certificate to be submitted)
		UPS should meet CE /BIS and ROHS standards (Compliance to be submitted)
4.	Input Voltage Range	160-280 VAC @ 100% load, Three Phase
5.	Input Freq. Range	50Hz +/- 3 (auto sensing)
6.	Input Power Factor	0.99 (100% Load)
7.	Input Protection	Thermal Circuit Breaker
8.	Output Voltage	220/230/240 VAC +/- 1%, 380/400/415 VAC +/- 1%
9.	Output Frequency	50Hz ± 0.5Hz
10.	Output Waveform	Pure Sinewave
11.	O/P Voltage Distortion	<3% for Linear, <6% for Non-Linear Load
12.	Output Connections	Output Connections: (1) Hard Wire 3-wire (H N + G),

13.	Efficiency (Overall)	> 85%
14.	Efficiency (Inverter)	> 90%
15.	Battery Type	SMF-VRLA (Sealed maintenance free valve regulated lead acid)
16.	Battery Make	Exide, Quanta, Panasonic, CSB, Yuasa, Relicell or equivalent
17.	Battery Backup	60 min backup on Full Load
18.	Communication	Full-Functional SNMP Card should be present; RS 232 & USB port with software for UPS status monitoring
19.	Protection	Inherent protection should be provided for Output Short-circuit and Overload, Input Fault, Cold Start, Low battery, Battery Over and Under charge, Battery Disconnect, Battery self-test feature, Over Temperature, OVCD, External Transient Voltage Surge Suppressor, etc.
20.	LCD Display	Input Voltage, Input Frequency, Output voltage, Output Current, Output Frequency, Battery Voltage, UPS Status, Load Level, Battery Level, Discharge Timer, Battery Disconnect and Fault Conditions
21.	By Pass	Manual and Automatic (Built-in) Bypass switch should be provided
22.	Environment	Noise Level – less than 60 dB at a distance of 1 meter
23.	Programmable Outlets	UPS should have programmable outlets for control of load segment
24.	Operating Temperature	0-45° C
25.	Relative Humidity	20-90%RH @0-40° C (Non-condensing)
26.	Miscellaneous	ECO Mode Operation with Enable/Disable function
		Cooling: Forces Air Cooling
		Emergency Power Off (EPO)
		BYPASS Mode Operation with Enable/Disable function
		Cables: With all necessary cables and plug and Battery links
		Rack: Suitable Metallic Rack for housing of SMF Batteries to be provided
27.	Battery Replacement	The successful bidder has to replace the UPS battery every 2 years for uninterrupted and smooth operations. OEM should confirm battery replacement in UPS at the end of 2nd year and 4th year respectively.

#### **4.7 Junction Box, with adjustable mounting frames**

S/N	Parameter	Specification
1.	Built	The Outdoor Utility Cabinet will be constructed with a front sheet steel door with 3-point Locking system to ensure the security of the cabinet. Side and Wall Panels shall be thick wall constructed, with fixing bolts internal to the cabinet. The Cabinet should have the required frames to mount the required components like, network device, power, UPS, LIU, battery, etc.
2.	Utility & IP rating	Should be Made for 24/7/365 Outdoor Applications; The Utility Cabinet shall be IP 55 rated (Regulatory Standard Compliance) for ingress protection.
3.	Size	The cabinet has to be provided of size suitable for the mounting of the associated network devices, power, UPS and Battery components securely and safely within the cabinet.
4.	Power Slot	Minimum 3 x 5 way Indian Standard PDU's has to be provided to support the site equipment. PDU type should be as per actual requirement.

5.	Installation	Each Cabinet will be mounted on a raised height Plinth, 600 - 1000 mm high, as per site requirements. FAN Cooling unit shall be inherent in the design.
6.	Cable	Proper cable management should be provided
7.	Management	Cable Routing: Power connection cable shall be provided from the nearest access point provided by Power utility company to the Outdoor Utility Cabinet through Power meter enclosure.

#### 4.8 Voltage Stabilizers at Junctions

S/N	Parameter	Minimum Specification
1.	Device capacity	3 KVA
2.	Voltage Correction	Automatic, IC Controlled
3.	Input Voltage Range	130 V to 280 V
4.	Frequency Range	50 Hz +/- 5 %
5.	Output Voltage Range	200 V to 230 V, +/-5 %
6.	Efficiency	> 95%
7.	Protection/Cut off	Over Voltage and over Current Protection, Thermal and Electronic Overload
8.	Device Construction	Compact and modular construction for easy handling and servicing
9.	Power Outlets	4 Nos. Indian Standard Power Outlets
10.	Operating Temperature	Ambient Temperature range. The bidder has to take into consideration of the internal temperature adjustment of the junction box

#### 4.9 Surge Protection Power Strips

S/N	Parameter	Minimum Specification
1.	Clamping Voltage	240 V
2.	Response time	<10 ns
3.	Energy Dissipation	Min 500 joules
4.	Max voltage Spike protection	Up to 400 Volts
5.	Max current Spike Protection	5000 Amps
6.	Cable	Heavy duty Cable of standard Length
7.	Power Outlet	Min. 4 Nos. 5 Amp Indian Standard Power Outlets
8.	Operating Temperature	Ambient Temperature range. The bidder has to take into consideration of the internal temperature adjustment of the junction box

#### 4.10 Poles including mounting/installation

S/N	Parameter	Minimum Required Specifications
1.	Pole type	Galvanized pole as per IS:2629 and Fabrication as per IS:2713
2.	Height	6 meter above ground surface Bottom section : 1.4 meter Middle Section : 1.4 meter Top Section : 3.2 meter
3.	Foundation	Minimum 1 meter so as to ensure that video feed quality is not impacted due to winds



		in different climatic conditions and from vibration caused due to heavy vehicles on road
4.	Pole Diameter (Outer side)	Bottom section : 97.9mm Middle Section : 76.2mm Top Section : 65.2mm
5.	Bottom Base Plate	300mm x 300mm x 6mm
6.	Protection	Lightening arrestor and Earthing
7.	Cantilevers	The pole should support 3 number of cantilever of varying length from 0.5 to 2.0 meters. The cantilever should be fitted such that the can be rotated to change the direction or adjust the angle, if at all required. The Cantilever should be strong enough so as to mount at least 2 CCTV camera's, if required.
8.	Mounting Facility	CCTV camera on pole or cantilever, Junction Box

#### 4.11 Video Wall Solution-

S/N	Parameter	Minimum Required Specifications
1.	Configuration	Full HD IPS LED/DLP Display, Direct LED Backlight, Display suitable for use in video wall with bezel to bezel distance not more than 3 mm
2.	Screen Size	55" or higher
3.	Resolution	Full High definition (1920 X 1080) 16:9 Widescreen
4.	Contrast Ratio	1200:1 or better
5.	Brightness	500 Cd/m2 or better
6.	Refresh Rate	60 Hz or better
7.	Response Time	8 to 12 ms
8.	Viewing Angle	160 degrees or better
<b>Interface</b>		
9.	Standard Inputs	1x Digital DVI-I ; 1x Digital DVI-D, or Higher
10.	Standard Outputs	1x Digital DVI-D / 1x DP 1.2
11.	Control	RS-232/RS-422/IR
<b>Power</b>		
12.	Consumption	Not more than 4000 Watt
13.	Power Supply	AC 100 -240 V~ (+/-10 %), 50/60 Hz
<b>General</b>		
14.	Operating Temperature	0°C - 40°C
15.	Humidity	20% - 90%, non-condensing
<b>Accessories</b>		
16.	Cables	Dual Link DVI-D cable, power cable for daisy chain, AC cable, Remote Controller
17.	Display Controller	Video Distributor, Display controller to control Video wall in a matrix as per requirement with necessary software:

Processor specs: Quad core 64-bit, 3.4 GHz CPU or latest  
RAM: 8 GB DDR3/4 minimum  
HDD: Min 500 GB Hard Disk (Hard disk Capacity should be upgradable)  
Network support: Gigabit Ethernet Controller inbuilt, Support for Add on Network adapters.  
Videowall Display: Display multiple source windows in any size, anywhere on the wall  
Accessories: DVD-R,DVD+RW, Keyboard, mouse  
OS Support: 64-bit Operating Systems Windows / Linux or equivalent industry standard

**Video Wall Management Software**

18.	Display & Scaling	Display multiple sources anywhere on display up to any size
19.	Input Management	All input sources can be displayed on the video wall in freely resizable and movable windows
20.	Scenarios Management	Save and Load desktop layouts from Local or remote machines
21.	Layout Management	Support all Layout from Input Sources, Internet Explorer, Desktop and Remote Desktop Application
22.	Multi View Option	Multiple view of portions or regions of Desktop, Multiple Application Can view from single desktop
23.	Other features	<ul style="list-style-type: none"> <li>• SMTP support</li> <li>• Remote Control over LAN</li> <li>• Alarm management</li> <li>• Remote management</li> <li>• Multiple concurrent client</li> <li>• KVM support</li> </ul>
24.	Cube Management	<ul style="list-style-type: none"> <li>• Cube Health Monitoring</li> <li>• Pop-Up Alert Service</li> <li>• Graphical User Interface</li> </ul>

**4.12 Workstations**

S/N	Parameter	Minimum Required Specifications
1.	Processor	Latest Quad Core i7 with min 3 GHz or higher
2.	Motherboard & Chipset	OEM Motherboard & Compatible 64 bit Chipset
3.	Video	Integrated Graphic controller with minimum 2 GB video memory (non-shared), NVIDIA GeForce/AMD Radeon/Intel, it should support 3 monitors simultaneously without degrading the quality of the HD video Quality
4.	System Memory	Minimum 8 GB DDR4 or higher expandable up to 32 GB or more
5.	Ports	6 Nos. or Higher USB (min 2 USB3.0), 1XHDMI / 1 VGA Port.
6.	Storage	1 TB, SATA HDD 7200 RPM. Provision for installing more drives
7.	Monitor	27 Inches or higher x 3 Nos., Wide LED Touch Screen, Resolution- 1920x1080, Aspect Ratio-16:9 , refresh rate 5ms or better
8.	Keyboard	104 Keys or Higher Mechanical Keyboard
9.	Mouse	USB/wireless Optical Scroll Mouse
10.	OS Support	Pre-Loaded Windows 10 with recovery disc
11.	Certification	RoHS, ENERGY STAR/BEE
12.	Warranty Support	Minimum from 5 years from the date of Commissioning

#### 4.13 Desktop PC

S/N	Parameter	Minimum Required Specifications
1.	Processor	Intel Core i5 with min 2.8 GHz with 4MB cache or higher AMD A10 with min 3.2 GHz, 4MB cache or higher
2.	Motherboard & Chipset	OEM Motherboard & Compatible 64 bit Chipset
3.	Video	Integrated Graphic controller with minimum 2 GB video memory (non-shared), NVIDIA GeForce/AMD Radeon/Intel
4.	System Memory	Minimum 4 GB DDR3/DDR4 or higher expandable up to 16 GB or more
5.	Ports	4 Nos. or Higher USB (min 1 USB 3.0), 1XHDMI / 1 VGA Port.
6.	Storage	1 TB , SATA HDD 7200 RPM
7.	Monitor	19.5 Inches or Higher, Wide LED Screen , Resolution- 1920x1080, Aspect Ratio-16:9
8.	Keyboard	104 Keys or Higher Mechanical Keyboard
9.	Mouse	USB/Wireless Optical Scroll Mouse
10.	OS Support	Windows 10
11.	Certification	RoHS, ENERGY STAR/BEE
12.	Warranty Support	Minimum from 5 years from the date of Commissioning

#### 4.14 Indoor Fixed Dome Cameras with PoE

S/N	Specification
1.	Image sensor : 1/3" Progressive Scan CMOS 2 MP or better
2.	Lens : 3 to 9 mm or better, DC-iris, motorized
3.	Field of View : 35-38°~100-104°(horizontal), 20-22° ~ 55-72° (vertical), 42°~112° (diagonal)
4.	Day and Night : Automatic/manual/scheduled
5.	Min. Illumination / Light Sensitivity : Color mode: F1.2 @ 0.5 lux Black and white mode: F1.2@ 0.05 lux
6.	Light sensor: Senses the level of ambient light to determine when to switch day/night mode.
7.	Video Compression: H.264 and Motion JPEG
8.	Audio Compression: G.711 A-Law, G.711 U-Law, G.726
9.	Resolutions and frame rates : 30 fps at 1920x1080 (1080p)
10.	Protocol Support: IPv4, IPv6, TCP/IP, HTTP, DHCP, UDP, DNS, SMTP, RTP, RTSP, SNMP protocols/Should meet all functional requirement of the project
11.	PoE : 802.3af compliant
12.	Environmental Certification and Housing: IP66 and IK10 rated
13.	Camera Should remote Zoom and Auto focus
14.	Camera should supplied with 32GB Micro SD/SDHC for recording
15.	Should be ONVIF profile S & G compliant
16.	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

#### 4.15 Camera Type A (Box Cameras for ANPR, RLVD, Speed Detection)

S/N	Parameter	Minimum Specification
-----	-----------	-----------------------

S/N	Parameter	Minimum Specification
1.	Image sensor and Effective Pixels (Resolution)	1/ 2.8" or better, CMOS Progressive Scan & Minimum 2 MP (for ANPR & Speed Detection) and 8 MP (for RLVD) or better
2.	Electronic Shutter	1 to 1 / 10,000 s or better
3.	Focus	Automatic and Manual both
4.	Automatic Gain Control	Automatic / Manual
5.	S/N Ratio	>50 dB
6.	Frame Rate	50/60 FPS for ANPR & Speed Detections Camera and 20 FPS for RLVD Camera at Full Resolution
7.	Codec	H.264/H.265, MJPEG or better, Audio Compression: G.711
8.	Multi Focal Lens	≤6 mm to ≤50 mm Lens or better, For RLVD Camera "Lower End of Focal length less than 4.1 mm (3, 3.5 etc. allowed), Higher End of Focal Length more than 9 mm (10, 11, 20 etc. Allowed)
9.	Minimum Illumination	0.1 Lux@30 (IRE) f1.2 (Colour) & 0.001 Lux @ 30 (IRE) f1.2(B/W)
<b>Video</b>		
10.	Day and Night functionality	Automatic, Color, Mono
11.	IR illuminator	External Illuminator with visibility should be at least 50m, Power requirement & connectivity should be part of the solution. Illumination (Colour & b/w) should be sufficient to capture Objects/Faces at night time when there is not sufficient illumination at site.
12.	WDR	True WDR 100 dB or better
13.	Video Streams	Individually configurable 03 video streams (H.264/ H.265, MJPEG), Unicast/ Multicast
14.	Intelligent Video	Motion detection, Tampering Alert
<b>Network &amp; Interface</b>		
15.	Interface	RJ-45 for 10/100 base-T Ethernet
16.	Network Protocols support	IPv4, IPv6, TCP/IP, HTTP, DHCP, UDP, DNS, SMTP, RTP, RTSP, SNMP protocols/Should meet all functional requirement of the project
17.	Alarm Event (Non-working, tampering,)	Events / alerts send via FTP, HTTP, email, Pre-Post alarm video buffering.
18.	Compliance	ONVIF Profile S & G compliant
<b>Security</b>		
19.	General	Password Protection, HTTPS encryption, IEEE 802.1X
<b>General Camera Features</b>		
20.	Operational Temperature °C	0°C to 55 °C
21.	Outer Casing	Vandal Proof IK10 or above rated, NEMA 4X/ IP66 rated Housing
22.	Power	PoE (802.3 af) OR AC 24V/ DC12V, 100- 230VAC
23.	Certifications	CE, FCC, EN/UL
24.	Local Storage (memory card of Min 32 GB to be included)	In the event of failure of connectivity to the central server the camera shall record video internally or on the SD card automatically.

#### **4.16 Camera Type B (Box Camera for Surveillance)**

S/N	Parameter	Minimum Specification
1.	Image sensor and Effective Pixels (Resolution)	1/ 3" or better, CMOS Progressive Scan & Minimum 2 MP or better
2.	Electronic Shutter	1 to 1 / 10,000 s or better
3.	Focus	Automatic and Manual both
4.	Automatic Gain Control	Automatic / Manual
5.	S/N Ratio	> 50 dB
6.	Frame Rate	25/30 FPS for 1920 x 1080
7.	Codec	H.264/H.265, MJPEG or better Audio Compression: G.711
8.	Multi Focal Lens	≤6 mm to ≥50 mm lens or better
9.	Minimum Illumination	0.1 Lux (30 IRE)@f1.2 (Colour) & 0.001 Lux (30 IRE) @ f1.2(B/w)
<b>Video</b>		
10.	Day and Night functionality	Automatic, Color, Mono
11.	IR illuminator	External Illuminator with visibility should be at least 50m. Illumination (Color & b/w) should be sufficient to capture Objects/Faces at night time when there is not sufficient illumination at site.
12.	Video Resolution	Minimum 2 MP (1920 x 1080) or Better
13.	WDR	True WDR 100 dB or better
14.	Video Streams	Individually configurable 02 video streams (H.265/ H.264, MJPEG), Unicast/ Multicast
15.	Intelligent Video	Motion detection, Tampering Alert
<b>Network &amp; Interface</b>		
16.	Interface	RJ-45 for 10/100 base-T Ethernet
17.	Network Protocols support	IPv4, IPv6, TCP/IP, HTTP, DHCP, UDP, DNS, SMTP, RTP, RTSP, SNMP protocols/Should meet all functional requirement of the project
18.	Alarm Event	Events / alerts send via FTP, HTTP, email, Pre-Post alarm video buffering.
19.	Compliance	ONVIF Profile S & G compliant
<b>Security</b>		
20.	General	Password Protection, HTTPS encryption, IEEE 802.1X
<b>General Camera Features</b>		
21.	Operational Temperature °C	0°C to 55 °C
22.	Outer Casing	Vandal Proof IK10 or above rated, NEMA 4X /IP66 rated Housing
23.	Power	PoE (802.3 af) OR AC24V/ DC12V, 100- 230VAC
24.	Certifications	CE, FCC, EN/UL
25.	Local Storage (memory card of Min 32 GB to be included)	In the event of failure of connectivity to the central server the camera shall record video internally or on the SD card automatically.

#### 4.17 Camera Type C: PTZ


S/N	Parameter	Specification
1.	Sensor	1/3" CMOS & Minimum 2 MP
2.	Min. Illumination	Color: 0.5 lux 0.01 lux with IR or better
3.	Scanning System	Progressive
4.	S / N Ratio	>55dB
5.	IR Distance	Internal/ External with min 100 meters coverage
6.	IR Intensity	Automatically Adjust
7.	IR on/Off Control	Auto
8.	WDR	True WDR 100 db or better
<b>Lens</b>		
9.	Optical Zoom	20X or better
10.	Focal Length	5.2 to 104mm
11.	Focus Control	Auto/Manual
<b>Pan Tilt Zoom</b>		
12.	Pan/Tilt Range	Pan: 0° ~ 360° endless; Tilt: -15° ~ 90°, auto flip 180°
13.	Manual Control Speed	Pan: 0.1° ~160° /s; Tilt: 0.1° ~120° /s
14.	Preset Speed	Pan: 240° /s; Tilt: 200° /s
15.	Presets	Minimum 50 Preset Points
<b>Video</b>		
16.	Compression	H.265/H.264 / MJPEG
17.	Streaming Capability	2 Streams
18.	Resolution	1080 P or Better
19.	Frame Rate	1080P (1 ~ 25/30fps)
20.	Day and Night	Automatic, Color, Mono
21.	White Balance	Auto / Manual /ATW/Indoor/Outdoor/Daylight lamp/Sodium lamp
22.	Noise Reduction	Ultra DNR (2D/3D)
23.	Motion Detection	Required
24.	Region of Interest	Required
25.	Digital Zoom	12X or better
<b>Network</b>		
26.	Ethernet	RJ-45 (10/100Base-T)
27.	Protocols	IPv4/IPv6, HTTP, HTTPS, 802.1X, QoS, FTP, SMTP, UPnP, SNMP, DNS, DDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, ICMP, DHCP,
28.	Interoperability	ONVIF Profile S & G compliant
29.	Streaming Method	Unicast / Multicast
30.	Local Storage (memory card of Min 32 GB to be included)	In the event of failure of connectivity to the central server the camera shall record video locally on the SD card automatically.
31.	Certification	CE, FCC, EN/UL
32.	Power	PoE /+(802.3 af/at) OR AC 24V/ DC12V, 100- 230VAC
<b>General</b>		
33.	Working Temperature /	0°C to 55 °C, 80% RH non-condensing within enclosure

S/N	Parameter	Specification
	Humidity	
34.	Security	Password Protection, HTTPS encryption, IEEE 802.1X
35.	IP Rating	Vandal Proof IK10 or above rated, NEMA 4X /IP66 rated Housing
36.	Mounting Accessories	For pole and surface mount with L/C Brackets

#### 4.18 PTZ Joystick

S/N	Parameter	Minimum Required Specifications
1.	General	PTZ speed dome control for IP cameras
2.		Minimum 10 programmable buttons
3.		Multi-camera operations
4.		Compatible with all the camera models offered in the solution
5.		Compatible with VMS /Monitoring software offered

#### 4.19 CCTV Sign boards

S/N	Parameter	Minimum Specification
1	Size	Board Width = 12" / 12"
2	Plate Material	Corrosion resistant Aluminum Alloy as per IRC 67:2001 (Code of Practice for Road signs)
3	Plate Thickness	Minimum 1.5 mm
4	Retro-Reflective sheeting for sign-plate	Weather-resistant, having color fastness
5	Other Specifications	As per IRC 67:2001 (Code of Practice for Road signs)
6	Mounting	Can be mounted on wall or pole (appropriate mounting brackets to be provided)
7	Design	<p><b>As per following signage diagrams: The Text on the board should be in Gujarati Language only</b></p> 

#### 4.20 IR Illuminator

S/N	Parameter	Specification
1.	Range	Min 50 meter at 60-degree angle
2.	Minimum illumination	Hight Sensitivity @0 Lux
3.	Angle of Mounting	Adjustable
4.	Power	PoE, Auto on/off
5.	Casing	IP 66 and IK10 Rated
6.	Operational Temperature	0°C to 55 °C

7.	Certification	CE, FCC, EN/UL
----	---------------	----------------

#### 4.21 Internet Router

S. No	Minimum Required Specifications
1.	Router should support capacity of minimum 5 Gbps.
2.	Router should support Redundant Power Supply and should also support On line insertion and removal of the same from day one.
3.	Router should have IPV4 and IPV6, IGMP V1/V2/V3, MLD, PIM(V1,V2), 6PE and 6VPE mode for IPV6 transport over IPV4, IPV4 Multicast, VPN V4 multicast ECMP, LDP, BGP Prefix independent control (EDGE and Core) for IPV4 and IPV6, BGP,MBGP, IS-IS, OSPF v2 and v3,NAT, MPLS (L2 & L3), RSVP,VRRP, Loop free alternate FRR and traffic engineering
4.	Router should have high availability for all BFD, BGP, OSPF and IS-IS and no packet loss during controller switch over.
5.	Router shall support HQOS/QoS on all kind of interface in both ingress and egress direction. Similar QoS shall be supported for all type of interface including Bundled interfaces.
6.	The Router Support Ingress classification, marking and policing on physical Interfaces and logical Interfaces using source/destination IP subnet, protocol types (IP/TCP/UDP), source/destination ports, IP Precedence, MPLS EXP, DSCP, 802.1p.
7.	The router should be supplied with the following: - 4x1G Interfaces and should be scalable to additional 4x1G ports in future.
8.	Router should have redundant data and control plane for non-stop forwarding and routing
9.	The Router should be NDPP or EAL3 certified at the time of Bidding
10.	The router should support the aggregation of the interfaces to form one single logical interface for data transfer.
11.	The Router should be Rack mountable.
12.	The Router should be supplied with Indian Standard power cables.
13.	The Router should be supplied with all necessary SFP's, interfaces, connectors, patch cords (if any) must be delivered along with the applicable Licenses from day one.

#### 4.22 Router

S/N	Specification
1.	In case of failure of any single route processor, none of the line card traffic should be impacted.
2.	Router capacity and Port Details : As per Annexure C
3.	Router should support 4000 MAC addresses or more.
4.	Router should support Redundant Power Supply and should also support On line insertion and removal of the same from day one.
5.	Router must support TCP/IP, PPP, Frame Relay, HDLC
6.	Router should support the aggregation of the interfaces to form one single logical interface for data transfer.
7.	Router should support IPv4 and IPv6 from day one



8.	Router should support all standard routing protocols like BGP, MBGP, OSPF v2/v3, IS-IS, RIP/RIPv2, static routes, MPLS (L2 & L3), PIM(v1, v2), IGMP(v1, v2, v3), , Ipv6 tunneling, NAT, NTP, etc.
9.	Router should support High Availability (VRRP, or other proprietary protocol, etc.)
10.	Router should support QoS (DSCP, CoS), marking, classification and Policing
11.	Router should support Traffic Engineering & MPLS-TE with FRR
12.	Router should have a dedicated OOB Management port using CLI(SSH), WebUI(SSL), SNMP (v1, v2, v3), TFTP, etc.
13.	Router should support AAA features using TACACS+, Radius, LDAP, etc.
14.	Router should be NDPP or EAL3 certified at the time of bidding
15.	The device should support the aggregation of the interfaces to form one single logical interface for data transfer.
16.	Router should have redundant, hot-swappable power supply support for a fully loaded chassis
17.	The Router should be supplied with Indian Standard power cables.
18.	Router should have redundant data and control plane for non stop forwarding and routing
19.	The Router should be supplied with all necessary SFP's, interfaces, connectors, patch cords (if any) must be delivered along with the applicable Licenses from day one.

#### 4.23 Managed L3 Switch

S/N	Specification
1.	Port Details (Duplex: Full, Half) and minimum switching capacity : As per Annexure C
2.	All the interfaces ports should be wire speed and non-blocking
3.	Should be IPv4 and IPv6 ready from day one
4.	Should support minimum 8000 MAC address entries
5.	Should support protocols like MSTP, STP, RSTP, dot1q VLAN-tagging, LACP, NTP
6.	Should have features like port-security, auto-negotiate, flow control, MAC filtering
7.	Should support dynamic routing protocols like static route, OSPF, RIP, BGP, Multicast, PIM(v1, v2), IGMP(v1, v2, v3) from day one for both IPv4 and IPv6.
8.	Should have a dedicated OOB Management port using CLI(SSH), WebUI(SSL), SNMP (V1, V2, V3), TFTP, etc.
9.	Should support AAA features using TACACS+, Radius, LDAP, etc.
10.	Should be NDPP or EAL3 certified at the time of Bidding
11.	All necessary SFP's, interfaces, connectors, patch cords (if any) & licenses must be delivered along with the switch from day one.
12.	The device should support the aggregation of the interfaces to form one single logical interface for data transfer.
13.	Should have redundant power supply and FAN in N+1 formation
14.	The Switch should be Rack mountable & the switch should be supplied with Indian standard AC power cord.

#### 4.24 Managed L2 Switch

S/N	Specification
1.	Port Details (Duplex: Full, Half) and minimum switching capacity : As per Annexure C

2.	All the interfaces ports should be wire speed and non-blocking
3.	Should be IPv4 and IPv6 ready from day one
4.	Should support minimum 4000 MAC address entries
5.	Should support protocols like MSTP, STP, RSTP, dot1q VLAN-tagging, LACP, NTP
6.	Should have features like port-security, auto-negotiate, flow control, MAC filtering
7.	Should have a dedicated OOB Management port using CLI(SSH), WebUI (SSL), SNMP (V1, V2, V3), TFTP, etc.
8.	The device should support the aggregation of the interfaces to form one single logical interface for data transfer.
9.	Switch should support AAA features using TACACS+, Radius, LDAP, etc.
10.	Should be NDPP or EAL3 certified at the time of Bidding
11.	All necessary SFP's, interfaces, connectors, patch cords (if any) & licenses must be delivered along with the switch from day one.
12.	The device should support the aggregation of the interfaces to form one single logical interface for data transfer.
13.	The Switch should be Rack mountable & the switch should be supplied with Indian standard AC power cord.

#### **4.25 Managed Outdoor L2 Switch, PoE with Fibre Port-**

S/N	Specification
1.	Minimum 8 No's of 10/100/1000 Base-Tx PoE ports (Duplex, Full, Half) and 2 x 1G SFP Uplink port.
2.	All ports should have features of auto- negotiate, flow control (802.3x), port based network access control (802.1x), port security, MAC filtering etc.
3.	Minimum Switching capacity of 8 Gbps or more
4.	Should be IPv4 and IPv6 ready from day one
5.	Should have IGMP snooping v1,2 & 3 supporting min 100 multicast groups
6.	Features of DHCP (including option 82), DHCP Relay NTP or equivalent, SNMPv1, v2 & v3, TELNET/ SSH
7.	Should have console port for administration & management, CLI and web based GUI for easy management
8.	Support for IEEE 802.3ad Link Aggregation Control Protocol (LACP)
9.	Port Security to secure the access to a port based on the MAC address of a user's device. The aging feature to remove the MAC address from the switch after a specific time to allow another device to connect to the same port.
10.	Multilevel security on console access to prevent unauthorized users from altering the switch configuration.
11.	Port-based and 802.1Q tag-based VLANs, MAC-based VLAN, Guest VLAN, Private VLAN, also known as protected ports, with multiple uplinks

12.	Web/SSL, Telnet server/SSH, ping, traceroute, Simple Network Time Protocol (SNTP), Trivial File Transfer Protocol (TFTP), SNMP, RADIUS, syslog, DNS client, protocol-based VLANs
13.	Duplicate address detection (DAD)
14.	Temperature: Ambient temperature range of 0 ° C to 55 ° C. The bidder has to take into consideration of the internal temperature adjustment of the junction box
15.	10 % to 90 % RH, non condensing

#### **4.26 Managed Outdoor L2 Switch with PoE - 8-port**

S/N	Specification
16.	Minimum 8 No's of 10/100/1000 Base-Tx PoE ports (Duplex, Full, Half) and 2 x 1GE Uplink port.
17.	All ports should have features of auto- negotiate, flow control (802.3x), port based network access control (802.1x), port security, MAC filtering etc.
18.	Minimum Switching capacity of 8 Gbps or more
19.	Should be IPv4 and IPv6 ready from day one
20.	Should have IGMP snooping v1,2 & 3 supporting min 100 multicast groups
21.	Features of DHCP (including option 82), DHCP Relay NTP or equivalent, SNMPv1, v2 & v3, TELNET/ SSH
22.	Should have console port for administration & management, CLI and web based GUI for easy management
23.	Support for IEEE 802.3ad Link Aggregation Control Protocol (LACP)
24.	Port Security to secure the access to a port based on the MAC address of a user's device. The aging feature to remove the MAC address from the switch after a specific time to allow another device to connect to the same port.
25.	Multilevel security on console access to prevent unauthorized users from altering the switch configuration.
26.	Port-based and 802.1Q tag-based VLANs, MAC-based VLAN, Guest VLAN, Private VLAN, also known as protected ports, with multiple uplinks
27.	Web/SSL, Telnet server/SSH, ping, traceroute, Simple Network Time Protocol (SNTP), Trivial File Transfer Protocol (TFTP), SNMP, RADIUS, syslog, DNS client, protocol-based VLANs
28.	Duplicate address detection (DAD)
29.	Temperature: Ambient temperature range of 0 ° C to 55 ° C. The bidder has to take into consideration of the internal temperature adjustment of the junction box
30.	10 % to 90 % RH, non condensing

#### 4.27 Server

S/N	Parameter	Specification
1.	Processor	Latest series/ generation x86 processor(s) with ten or higher cores Processor speed should be minimum 2.2 GHz Minimum 2 processors per each physical server
2.	RAM	Minimum 256 GB Memory per physical server
3.	Internal Storage	2 x 900 GB SAS (10k rpm) hot swap disk
4.	Network interface	2 X 10Gbps ports for providing Ethernet connectivity 2 X Dual-port 10Gbps FC/FCoE/HBA for providing FC connectivity
5.	Power supply	Dual Redundant Power Supply
6.	RAID support	As per requirement/solution
7.	Operating System	Licensed latest version of Linux/ /Microsoft Windows based Operating system
8.	Form Factor	Blade server
9.	<b>Virtualization</b>	Shall support Industry standard virtualization hypervisor like Hyper-V, VMWARE, Citrix. etc.

#### 4.28 Network Rack- 19U

S/N	Specification
1.	19 U: 750 x 1070 x 1185 mm
2.	Door Steel Ful Prf 750W x 19U
3.	Castor with ft break (2+2)
4.	Sliding Tray
5.	Should have sufficient perforation for ventilation of air
6.	IPDU : As per the requirements of the IT equipment's to be loaded

#### 4.29 Server Rack- 42U

S/N	Specification
1.	42 U : 600 x 1070 x 1991 mm
2.	Door Steel Ful Prf 600W x 42U
3.	Castor with ft break (2+2)
4.	Sliding Tray
5.	Should have sufficient perforation for ventilation of air
6.	IPDU : As per the requirements of the IT equipment's to be loaded

#### 4.30 Network Rack- 42U

S/N	Specification
1.	42 U : 750 x 1070 x 1991 mm
2.	Door Steel Ful Prf 7500W x 42U
3.	Castor with ft break (2+2)
4.	Sliding Tray

5.	Should have sufficient perforation for ventilation of air
6.	IPDU : As per the requirements of the IT equipment's to be loaded

#### 4.31 Firewall for District Control Centres

S/N	Minimum Required Specifications
1.	Proposed device should also perform activities like Intrusion prevention, IP Reputation, Antivirus & Anti-BOT control from day one with required perpetual Licenses and 24*7 support for 5 years
2.	<b>Minimum firewall throughput and port details : As per Annexure C</b>
3.	Device should support IPv4 & IPv6 dual stack functionality
4.	Firewall should support both routed & transparent mode
5.	Firewall should support static NAT, PAT, dynamic NAT, PAT
6.	Firewall should support Nat66 (IPv6-to-IPv6) and Nat46 (IPv4-to-IPv6) functionality, NAT66
7.	Firewall should support static, dynamic and multicast routing protocol
8.	Firewall should support creating access polices on the basis of IPv4, IPv6 objects, protocols, ports, applications, URL, user etc.
9.	Firewall should support user authentication via captive portal & should be integrate with LDAP, RADIUS, AD for SSO
10.	Solution should support troubleshooting tools like Ping, Traceroute, Packet Tracer/capture, etc.
11.	The device should be manageable using standard protocols HTTP, HTTPS, SSL, telnet, SSH, SNMP etc.
12.	The device should be able to fully managed by centralized management solution and should be managed from the CCC. It should be able to send the Logs to centralized logging server
13.	The device should be supplied with Indian Standard power cables.

#### 4.32 Firewall for CCC

S/N	Minimum Required Specifications
1.	Proposed device should also perform activities like Intrusion prevention, IP Reputation, Anti Malware, Web filtering & Anti-BOT control from day one with required perpetual Licenses and 24*7 support for 5 years
2.	Device must have support for IPSec, VPN & SSL VPN with 500 user support from day 1 in any kind of mode (office/routed/tunnel/web, etc.) & must have capacity to expand up to 1000 users in same unit
3.	Device should have <b>Minimum firewall throughput of 20 Gbps</b>
4.	Device should have Minimum VPN throughput of 2 Gbps
5.	The device should support at least <b>4x10 G and 4x 1 G ports</b> from day one and should be scalable to additional 2x10 G and 2X1 G ports
6.	Device should support IPv4 & IPv6 dual stack functionality
7.	Firewall should support both routed & transparent mode
8.	Firewall should support static NAT, PAT, dynamic NAT, PAT
9.	Firewall should support Nat66 (IPv6-to-IPv6) and Nat46 (IPv4-to-IPv6) functionality, NAT66
10.	Firewall should support static, dynamic and multicast routing protocol

11.	Firewall should support creating access polices on the basis of IPv4, IPv6 objects, protocols, ports, applications, URL, user etc.
12.	VPN Client must be available to download for IOS/Android/Windows platform, there should be a provision for integration of such VPN client with the mobile application for creating a secure VPN Connection
13.	Firewall should support user authentication via captive portal & should be integrate with LDAP, RADIUS, AD for SSO
14.	Solution should support troubleshooting tools like Ping, Traceroute, Packet Tracer/capture, etc.
15.	The device should be manageable using standard protocols HTTP, HTTPS, SSL, telnet, SSH, SNMP etc.
16.	Device must support High availability with stateful failover of hardware.
17.	The device should be able to fully managed by centralized management solution and should be managed from the CCC. It should be able to send the Logs to centralized logging server
18.	The device should support the aggregation of the interfaces to form one single logical interface for data transfer.
19.	The device should be supplied with Indian Standard power cables.
<b>Centralize Reporting &amp; Management Tool</b>	
20.	Device must support atleast 50 Firewalls from the day 1
21.	It should support detail logging & reporting feature inbuilt/external for atleast 50 remote firewall's
22.	It Should be supplied with additional Hard disk of suitable storage capacity for storing the daily Logs

### 4.33 Web Application Firewall (WAF) for CCC

S/N	Minimum Required Specifications
1.	WAF Should protect against application-level attacks targeted at web applications.
2.	Should provide bi-directional protection against sophisticated threats like SQL injection and cross-site scripting
3.	Should provide controls to prevent identity theft, financial fraud and corporate espionage.
4.	should have unlimited application licenses.
5.	Should support Automatic signature update and install
6.	Should monitor and enforce government regulations, industry best practices, and internal policies.
<b>Performance Requirement</b>	
7.	Should support atleast 20000 HTTP transactions per second
8.	Should deliver minimum throughput of 250 Mbps
9.	Should have Sub Millisecond Latency
<b>Interface and connectivity requirements</b>	
10.	Should support 4 no's of GE RJ45 Interfaces with bypass option (2ports) & 2x 1G SFP port
11.	Should be supplied with atleast 200 GB of Storage space
<b>Application Features</b>	
12.	Should be able to perform in multiple modes such as Active mode, passive mode, Transparent mode, proxy mode
13.	Should continuously track the availability of the Server(s) being protected.
14.	Should have a Web Vulnerability Scanner to detect existing vulnerabilities in the protected web applications.

15.	Should have Data Leak Prevention module to analyze all outbound traffic alerting/blocking any financial Information leakage and information disclosure
16.	Provide controls to meet PCI compliance requirements for web application servers.
17.	Should support automatic signature updates to protect against known and potential application security threats.
18.	Should have built in policies and support custom signatures
19.	Provide ability to allow/deny URL access
20.	Support IPv4 and IPv6 and allow IPv4 to IPv6 communication
21.	Device should able to control BOT traffic and It should able to block known bad bots and fake search engine requests
22.	Should have the capability to Auto-Learn Security Profiles required to protect the Infrastructure.
23.	Should detect and have controls against Brute force attacks
24.	Should be able to protect Cookie Poisoning and Cookie Tampering
25.	Should support multiple HTTP versions such as HTTP/0.9, HTTP/1.0, HTTP1.1
26.	Should be in High Availability in active mode and load-balancing engine
27.	Should have in built capability for Web Application Vulnerability Scanning
28.	Should support Secure Administrative Access using HTTPS and SSH
29.	Should support Role Based Access Control for Management

#### 4.34 Enterprise Management System

S/N	Specification
1.	<p>The System should deliver following functionalities:</p> <ol style="list-style-type: none"> <li>1. Network &amp; Server Fault Monitoring &amp; Performance for IP/SNMP enabled devices like router, switches, CCTV devices, etc.</li> <li>2. Application Performance Management</li> <li>3. IT Helpdesk – ITIL v3 Aligned</li> <li>4. Business Services Dashboard</li> <li>5. Service Level Management</li> <li>6. Capacity Management</li> <li>7. IT Asset Inventory Management &amp; License Management</li> <li>8. Configuration Automation.</li> </ol>
2.	The Centralized EMS solution needs to have a standalone system and has to be technology / vendor agnostic that shall enable to introduce any additional technology / vendor in the network. Such a network as and when introduced should seamlessly integrate with the solution proposed and continue to provide the services right since the day one of its introduction.
3.	The EMS should also support single pane visibility across multiple areas of Monitoring
4.	The system must allow for push or pull methods to send/collect or receive the information to and from various 3rd party systems/devices/servers.
5.	The system should have the ability to provide performance/service data to external systems.
6.	The system shall be able to interface with fault management system via standard protocol.
7.	The solution should be able to monitor the performance, availability, utilization, memory, etc. of all the devices in the network.

8.	It should have a WEB Based user Interface through which Administrator can access all administrative tasks and operational status monitoring for Network Devices, Servers, Sensors, etc.
9.	It should produce a WEB based interface to the users also for accessing the SLA reports
10.	Should be able integrate with Helpdesk System for automated incidents reporting with option for manual reporting followed by viewing, updating, tracking and closing.
11.	The Enterprise Management tools must have Service Level Management function to allow building various service levels and track the performance of Infrastructure and operational service levels in real time.
12.	The EMS tool should allow creation of groups/multiple users with role and geography based access to the Network management capabilities
13.	The solution should have perpetual licenses to manage all the devices in the network and any other devices that may be added in future

#### 4.35 Access Control System

S/N	Specification	
<b>Biometric Finger Scan Reader</b>		
1.	Transmission Frequency: 13.56 MHz	
2.	iClass/Mifare Technology	
3.	The data flow between card & Reader should be encrypted using 64 bit authentication keys.	
4.	Should be configured as a Reader – Enroller, Enroller Only & Reader Only (All three are mandatory)	
5.	Optical Finger print sensor with resolution of atleast 500dpi	
6.	Finger print should be captured in less than 2 seconds and verified in less than 5 seconds.	
7.	Should have fingerprint enrollment software	
8.	Operating temperature: 0° to 45°C	
9.	Operating humidity: 10% to 90% relative humidity (Non-Condensing)	
<b>Smart card Reader</b>		
10.	Transmission Frequency: 13.56 MHz	
<b>Controller</b>		
11.	Inputs	Reader Inputs: 2 Nos., Universal Inputs: 2 Nos., Tamper Input: 1Nos., Digital Lock Input: 2 Nos.
12.	Processor	Min 50 MHz with 32 MB RAM
13.	Processor For Reader Inputs	Yes (Combined/Dedicated Processor)
14.	Communication	10/100 Ethernet Port
15.	Memory	Minimum 500 personnel Records
16.	Area Lockdown Support	Yes
17.	Real Time Clock	Yes
18.	Encryption	64 bit
19.	Visual Indicator	Yes
20.	Mounting	Wall / Ceiling Mount
21.	Battery Backup	5 hours or more
22.	Technology Compatibility	Wiegand



S/N	Specification	
23.	Card Reader Power	5V DC
24.	Wiring Distance	150 meters (Wiegand)
25.	Indicator LED	Yes
26.	Push Button Switches	Yes (For clearing the memory & Resetting the IP Address)
27.	Enclosure	Yes
28.	Certifications	CE/UL Certified
29.	Operating Temperature	0° to 45°C
30.	Operating Humidity	10% to 80% relative humidity (Non-Condensing)
<b>Access Control Software</b>		
31.	Compatibility with any Windows Operating System	
32.	Compatibility with MYSQL / SQL / ORACLE	
33.	Support for TCP/IP Communication	
34.	Provision for Alarm Monitoring for Battery, Mains Supply, Door Opened too Long, Door Forced Opened, Unauthorized Swipe & Controller Tampering	
35.	Support for unlimited number of Card Database & Transactions	
36.	Specify Card Activation & Expiry Date	
37.	Support for Biometric, Pin & Smart Card Applications	
38.	Management of Dual Access Levels to a single Card	
39.	Remote Locking & Unlocking of Doors	
40.	Remote management of Controllers	
41.	Customization of Door User time for every card Holder	
42.	One Client License	
43.	Two Stages of Alarm Management (Acknowledgement on Receipt & Closure on Investigation)	
44.	Access Privileges on the basis of Time & Date	
45.	Creation of holiday schedules to cover maintenance & Vacations / Holidays	
46.	Permission to activate any control output for a specific event such as alarm	
47.	Programmable Shunt time to control the door opening time	
48.	Area Control by using Hard Anti Pass back, Soft Anti Pass back, Timed Anti Pass back, Occupancy Limit, Multi man principle, Area Lock down, Threat level conditioning.	
49.	Alarm Management	
50.	Automatic User Log off	
51.	Cardholder Management & Enrollment	
52.	Creation & Maintenance of User Database	
53.	Assignment of Access Privileges	

#### 4.36 Centralized Antivirus Solution

Sr. No.	Specification
1.	Should be able to protect all computing resources such as servers, desktops, workstations and other end point devices from centralized Antivirus solution

2.	Shall be able to scan through several types of compression formats.
3.	Must update itself over internet for virus definitions, program updates etc. (periodically as well as in push-updates in case of outbreaks)
4.	Able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)
5.	Shall be able to scan only those file types which are potential virus carriers (based on true file type)
6.	Shall be able to scan for HTML, VBScript Viruses, malicious applets and ActiveX controls
7.	Shall provide Real-time product Performance Monitor and Built-in Debug and Diagnostic tools, and context- sensitive help.
8.	The solution must support multiple remote installations
9.	Shall provide for virus notification options for Virus Outbreak Alert and other configurable Conditional Notification.
10.	Should be capable of providing multiple layers of defense
11.	Shall have facility to clean, delete and quarantine the virus affected files.
12.	Should support in-memory scanning so as to minimize Disk IO.
13.	Should support heuristic scanning to allow rule-based detection of unknown viruses
14.	Updates to the scan engines should be automated and should not require manual intervention
15.	All binaries from the vendor that are downloaded and distributed must be signed and the signature verified during runtime for enhanced security
16.	Updates should be capable of being rolled back in case required
17.	Should support various types of reporting formats such as CSV, HTML and text files
18.	Shall be able to automatically push any updates, patches, fixes to all client machines to ensure up-to-date antivirus protection for all IT devices and systems.
19.	In case of virus outbreak and compromised endpoints (Servers, Workstations, Desktop etc.) the OEM should provide cure solution within specified SLA (at no extra cost), to remove the virus and clean the system(s) to restore the environment.

#### **4.37 Server Load Balancer for Central CCC**

<b>S/N</b>	<b>Minimum Required Specifications</b>
1.	Device should support load balancing of both TCP and UDP based traffic using algorithms like round robin, weighted round-robin, least connections, persistent connects, etc.
2.	Device should provide minimum throughput of 10 Gbps
3.	Device should provide 4x10G ports scalable to additional 4x10G ports
4.	Should support Client availability (Heartbeat) monitoring
5.	Should be support High Availability in Active-Active, Active-Passive mode.
6.	Should be Manageable using CLI(SSH), WebUI(SSL), SNMP (V1, V2, V3), etc.
7.	The management option should allow configuration, operation, firmware upgrade, traffic reporting, error logs, status logs
8.	Should support IPv6 from day one
9.	Should support static and dynamic routing
10.	Should support Global Server Load balancing, URL based Load balancing, HTTP, HTTP redirection, HTTP Layer 7 redirection, DNS redirection, DNS Fallback redirection,
11.	Should be Rack mountable & should be supplied with Indian standard AC power cord.
12.	Should support multiple instances having dedicated CPU, memory, SSL & I/O for guaranteed performance.

#### 4.38 Server Load Balancer for District/City Control Centre

S/N	Minimum Required Specifications
13.	Device should support load balancing of both TCP and UDP based traffic using algorithms like round robin, weighted round-robin, least connections, persistent connects, etc.
14.	Device should provide minimum throughput of 10 Gbps
15.	Device should provide 4x1G ports scalable to additional 4x1G ports
16.	Should support Client availability (Heartbeat) monitoring
17.	Should be support High Availability in Active-Active, Active-Passive mode.
18.	Should be Manageable using CLI(SSH), WebUI (SSL), SNMP (V1, V2, V3), etc.
19.	The management option should allow configuration, operation, firmware upgrade, traffic reporting, error logs, status logs
20.	Should support IPv6 from day one
21.	Should support static and dynamic routing
22.	Should support Global Server Load balancing, URL based Load balancing, HTTP, HTTP redirection, HTTP Layer 7 redirection, DNS redirection, DNS Fallback redirection,
23.	Should be Rack mountable & should be supplied with Indian standard AC power cord.
24.	Should support multiple instances having dedicated CPU, memory, SSL & I/O for guaranteed performance.

#### 4.39 Storage (For Applications)

S/N	Parameter	Specification
1.	Storage	<ul style="list-style-type: none"> <li>• Solution should be IP Based/iSCSI/FC/FCOE/NFS/CIFS</li> <li>• Storage Capacity :5 TB Useable for each District HQ and 10 TB for CCC</li> <li>• Disks should be minimum of 1 TB SAS drives</li> <li>• Storage solution should comprise of Active-Active Load Balancing Storage Controllers with 64GB Cache from day one and the storage solution should be scalable up to 128GB Cache without replacing existing Controllers</li> <li>• Front End: Minimum 8 x 10Gbps FC/FCoE ports for host connectivity scalable to 16 ports</li> <li>• Should be able to store all types of data (Data, Application, Voice, Images, Video, etc.)</li> <li>• Storage should support all industry standard RAID type</li> <li>• The proposed Storage should have 6 Gbps Drives (it should support SSD, SAS &amp; NL-SAS types) or higher.</li> <li>• Modular design to support controllers and disk drives expansion</li> <li>• Should be Rack Mountable</li> <li>• The controllers / Storage nodes should be upgradable without any disruptions / downtime</li> <li>• Licenses for the storage management software should include disc capacity/count of the complete solution and any additional disks to be plugged in in the future, up to max capacity of the existing controller/units.</li> <li>• A single command console for entire storage system.</li> </ul>

		<ul style="list-style-type: none"> <li>• Should have the functionality of performance, utilization monitoring of storage, disk drives and management software</li> <li>• The storage array must have complete cache protection mechanism either by de-staging data to disk or providing complete cache data protection with battery backup for minimum 4 hours</li> <li>• Controllers shall be active-active so that a single logical unit can be shared across all offered controllers, while supporting all the major functionalities like Thin Provisioning, Data tiering.</li> <li>• the storage should have no single point of failure on components like controllers, disks, cache memory, I/O Ports, Power supply, Fan, etc.</li> </ul>
2.	SAN Switch	<ul style="list-style-type: none"> <li>• May be proposed as per the solution requirement Compatible with the Storage</li> </ul>

#### 4.40 Storage (for Video's)

S/N	Parameter	Specification
1.	Storage	<ul style="list-style-type: none"> <li>• Storage period of 30 days <ul style="list-style-type: none"> <li>○ Storage Capacity: As per Annexure C</li> <li>○ The Storage capacity mentioned is the Usable capacity. The proposed storage solution should be scalable as per requirement.</li> </ul> </li> <li>• Disks should be minimum of 6 TB</li> <li>• Storage solution should comprise of Active-Active Load Balancing Storage Controllers with 64GB Cache from day one and the storage solution should be scalable up to 128GB Cache without replacing existing Controllers</li> <li>• Should be able to store all types of data (Data, Voice, Images, Video, etc.)</li> <li>• Storage should support all industry standard RAID type</li> <li>• The proposed Storage should have 6 Gbps Drives ( it should support SSD, SAS &amp; NL-SAS types) or higher.</li> <li>• Modular design to support controllers and disk drives expansion</li> <li>• Should be Rack Mountable</li> <li>• The controllers / Storage nodes should be upgradable without any disruptions / downtime</li> <li>• Licenses for the storage management software should include disc capacity/count of the complete solution and any additional disks to be plugged in the future, up to max capacity of the existing controller/units.</li> <li>• A single command console for entire storage system.</li> <li>• Should have the functionality of performance, utilization monitoring of storage, disk drives and management software</li> <li>• The storage array must have complete cache protection</li> </ul>

S/N	Parameter	Specification
		<p>mechanism either by de-staging data to disk or providing complete cache data protection with battery backup for minimum 4 hours</p> <ul style="list-style-type: none"> <li>• The storage should have no single point of failure on components like controllers, disks, cache memory, I/O Ports, Power supply, Fan, etc.</li> <li>• The Storage should be based on IP address and the time stamp of the feed for video data, images received from camera.</li> <li>• The solution should allow to transfer and store the data, on need basis, to any other storage irrespective of Make/Model across LAN/WAN within the state.</li> </ul>

**Note:**

1.) The above-mentioned specification are the minimum required specifications, the bidder is free to quote a product with better or higher specifications to meet the outcome of each service asked under the project.

2.) **Better or Higher Specification would mean:**

a.) In case of a camera, higher pixel resolution, lower focal length on lower end of zoom and higher focal length on higher end of zoom, more frame rates than sought, bigger sensor size (number on denominator being smaller when sensor size presented as 1/x" size), better pan/tilt angles, better zoom (bigger than ## \* times specified)

b.) In case of networking devices, better through put, more number of ports for ethernet or fibre as specified, PoE Rating

***SECTION-V***  
***INSTRUCTION TO BIDDERS***

## **5.1 GENERAL INSTRUCTION TO BIDDERS**

All information supplied by Bidders may be treated as contractually binding on the Bidders on successful award of the assignment by the TENDERER on the basis of this RFP. No commitment of any kind, contractual or otherwise shall exist unless and until a formal written contract has been executed by or on behalf of the TENDERER. Any notification of preferred bidder status by the TENDERER shall not give rise to any enforceable rights by the Bidder. The TENDERER may cancel this public procurement at any time prior to a formal written contract being executed by or on behalf of the TENDERER.

This RFP supersedes and replaces any previous public documentation, communications, and Bidders should place no reliance on such communications. The TENDERER may terminate the RFP process at any time and without assigning any reason. The TENDERER make no commitments, express or implied, that this process will result in a business transaction with anyone.

## **5.2 COST OF BIDDING**

**5.2.1** The Bidder shall bear all costs associated with the preparation and submission of the Bid. The TENDERER will in no case be responsible for those costs, regardless of the conduct or outcome of the bidding process.

**5.2.2** Bidder is requested to pay **Rs. 15,000/-** as a bid processing fee (Non-refundable) in the form of demand draft in favour of "Gujarat Informatics Ltd." payable at Ahmedabad/Gandhinagar along with the EMD cover. In case of non-receipt of bid processing fees & EMD the bid will be rejected by GIL/Home Department as non-responsive.

## **5.3 BIDDING DOCUMENT**

Bidder can download the bid document and further amendment if any freely available on <https://www.gil.gujarat.gov.in> and <https://www.gil.nprocure.com> and upload the same on <https://www.gil.nprocure.com> on or before due date of the tender. Bidder is expected to examine all instructions, forms, terms, and specifications in the bidding documents. Failure to furnish all information required by the bidding documents or submits a Bid not substantially responsive to the bidding documents in every respect may result in the rejection of the Bid. Under no circumstances physical bid will be accepted.

## **5.4 CLARIFICATION ON BIDDING DOCUMENT**

Bidders can seek written clarifications on or before pre-Bid to DGM (Tech), Gujarat Informatics Ltd., 8th Floor, and Block No. 1, Udyog Bhavan Gandhinagar 382017. GIL/Home Department will clarify & issue amendments if any to all the bidders in the pre-bid meeting. No further clarification what so ever will be entertained after the pre- bid meeting date.

## **5.5 AMENDMENT OF BIDDING DOCUMENTS**

At any time prior to the deadline for submission of bids, the TENDERER, for any reason, whether at its own initiative or in response to the clarifications requested by prospective bidders may modify the bidding documents by amendment & put on our websites.

All prospective bidders are requested to browse our website & any amendments/ corrigendum/ modification will be notified on our website and such modification will be binding on them.

In order to allow prospective bidders a reasonable time to take the amendment into account in preparing their bids, the TENDERER, at its discretion, may extend the deadline for the submission of bids.

## **5.6 LANGUAGE OF BID**

The Bid prepared by the Bidder, as well as all correspondence and documents relating to the Bid exchanged by the Bidder and the TENDERER shall be in English. Supporting documents and printed literature furnished by the bidder may be in another language provided they are accompanied by an accurate translation of the relevant pages in English. For purposes of interpretation of the bid, the translation shall govern.

## **5.7 BID SECURITY/ EARNEST MONEY DEPOSIT (EMD)**

- 5.7.1** Bidders shall submit, along with their Bids, EMD of Rs. 4,00,00,000/-, in the form of a Demand Draft OR Bank Guarantee (in the format specified in Format IV) issued by any nationalized/ Scheduled bank in favour of "Gujarat Informatics Ltd." payable at Ahmedabad/Gandhinagar, and should be valid for minimum 180 Days from the due date of the tender / RFP.
- 5.7.2** EMD of all unsuccessful bidders would be refunded by GIL within 60 Days on selection of successful bidder.
- 5.7.3** **The EMD of the successful bidder would be returned upon successful submission of Performance Bank Guarantee as per the format provided in Format V.**
- 5.7.4** EMD amount is interest free and will be refundable to the unsuccessful bidders without any accrued interest on it.
- 5.7.5** The bid / proposal submitted without EMD and Bid Processing fee, mentioned above, will be summarily rejected.
- 5.7.6** The EMD may be forfeited, In case of a Bidder if:
  - 5.7.6.1** The bidder withdraws its bid during the period of bid validity.
  - 5.7.6.2** The Bidder does not respond to requests for clarification of their Bid.
  - 5.7.6.3** The Bidder fails to co-operate in the Bid evaluation process.
  - 5.7.6.4** In case of successful bidder, the said bidder fails:
    - 5.7.6.4.1** Fails to sign the agreement in time
    - 5.7.6.4.2** Fails to submit performance bank guarantee

## **5.8 LANGUAGE OF THE BID**

- 5.8.1** The Bid prepared by the Bidder, as well as all correspondence and documents relating to the Bid exchanged by the Bidder and the TENDERER shall be in English. Supporting documents and printed literature furnished by the bidder may be in another language provided they are accompanied by an accurate translation of the relevant pages in English. For purposes of interpretation of the bid, the translation shall govern.

## **5.9 LATE BIDS**

- 5.9.1** Bids received after the due date and the specified time (including the extended period if any) for any reason whatsoever, shall not be entertained and shall be REJECTED.
- 5.9.2** The bids submitted by telex/telegram/ fax/e-mail etc. shall not be considered. No correspondence will be entertained on this matter.

## **5.10 SECTION COMPRISING THE BIDS**

- 5.10.1** The quotation should be scan-able and distinct without any option stated in.
- 5.10.2** All forms / Tables, duly filled-in with necessary proofs, as required and stated in the bid document & supporting documents for eligibility criteria should be uploaded. The bid uploaded shall have the following documents:
  - 5.10.2.1** **BID SECURITY SECTION:** The bid security & bid processing fee (non-refundable) to be furnished to GIL office in the form of demand draft in favour of "Gujarat Informatics Ltd." payable at Ahmedabad/Gandhinagar before the last date and time of the bid submission.
  - 5.10.2.2** **ELIGIBILITY & TECHNICAL SECTION**
    - 1.) Financial Capabilities. (In the Prescribed Format Only: Format VI)
    - 2.) Bidder's Experience. (In the Prescribed Format Only: ANNEXURE VII)
    - 3.) Compliance Statement. (In the Prescribed Format Only: ANNEXURE VII)



- 4.) Proposed Technical Solution as per the Scope of Work with details of each component/Module
- 5.) Proposed Technical Architecture for the project, with details of each project component
- 6.) Detailed Write-up on the Approach & Methodology for implementing and maintenance of the project.

**5.10.2.3 PRICE BID SECTION: Priced bid** (in the prescribed format only in Section VI)

- 5.10.3** Price shall be inclusive of all freight, forwarding, transit insurance and installation charges. Prices shall be inclusive of Excise Duties. The prices shall strictly be submitted in the given format. Quoted prices shall be without VAT. The tax (VAT) components as applicable shall be mentioned separately in the respective columns. Successful Bidder will have to supply/provide goods with an Invoice from a place located within State of Gujarat.
- 5.10.4** Prices shall be written in both words and figures. In the event of difference, the price in words shall be valid and binding. Arithmetical errors will be rectified on the following basis.
- 5.10.5** The bidder should provide calculations (Bill of Material with installation and setup charges, exclusive of taxes) for the quoted items, without which the bid is liable for rejection. Any arithmetical errors in these calculations will be on bidders account.
- 5.10.6**
- 5.10.7** Offered price should be exclusive of all applicable taxes such as VAT/CST/Service Tax, FOR destination (anywhere in Gujarat state).

## **5.11 BID OPENING**

- 5.11.1** Bids will be opened in the presence of Bidder's representatives, who choose to attend. The Bidder's representatives who are present shall sign a register evidencing their attendance.
- 5.11.2** In the event of the specified date of Bid opening being declared a holiday for the GIL, the Bids shall be opened at the appointed time and location on the next working day.
- 5.11.3** The Bidder's names, bid modifications or withdrawals, discounts and the presence or absence of relevant Bid security and such other details as the TENDERER officer at his/her discretion, may consider appropriate, will be announced at the opening.
- 5.11.4** Immediately after the closing time, the TENDERER contact person shall open the Un-Priced Bids and list them for further evaluation.
- 5.11.5** Bids that are not opened at bid opening shall not be considered further for evaluation.

## **5.12 BID VALIDITY**

- 5.12.1** Bids shall remain valid for 180 days after the date of Bid opening prescribed by the TENDERER. A Bid valid for a shorter period shall be rejected as non-responsive.
- 5.12.2** In exceptional circumstances, the TENDERER may solicit Bidder's consent to an extension of the period of validity. The request and the responses thereto shall be made in writing. The Bid security shall also be suitably extended. A Bidder's request to modify the Bid will not be permitted.

## **5.13 CONTACTING THE TENDERER**

- 5.13.1** Bidder shall not approach the TENDERER officers outside of office hours and/ or outside the TENDERER office premises, from the time of the Bid opening to the time the Contract is awarded.
- 5.13.2** Any effort by a bidder to influence the TENDERER officers in the decisions on Bid evaluation, bid comparison or contract award may result in rejection of the Bidder's offer. If the Bidder wishes to bring additional information to the notice of the TENDERER, it should do so in writing.

## **5.14 REJECTION OF BIDS**

The TENDERER reserves the right to reject any Bid, and to annul the bidding process and reject all bids at any time prior to award of Contract, without thereby incurring any liability to the affected Bidder(s) or any obligation to inform the affected Bidder(s) of the grounds for such decision.

## 5.15 BID EVALUATION PROCESS

**5.15.1** The TENDERER will form a Committee which will evaluate the proposals submitted by the bidders for a detailed scrutiny. During evaluation of proposals, the TENDERER, may, at its discretion, ask the bidders for clarification of their Proposals.

### 5.15.2 Pre-Qualification evaluation:

**5.15.2.1** Bidders who have submitted the valid EMD and non-refundable bid processing fee shall be considered for further evaluation. If bidders fail to submit the bid security and non-refundable bid processing fee as per this RFP document, the Bid shall be out rightly rejected.

### 5.15.3 Financial Bid Evaluation

The Financial Bids of qualified bidders only would be opened and evaluated to determine the L1 (lowest) bidder. All other Commercial bids will be returned un-opened. In case of conditional bid or major deviations from the RFP requirements, the TENDERER may at its discretion reject the respective bid and will not be considered for further evaluation process.

## 5.16 AWARD OF CONTRACT

**5.16.1** Award Criteria: The Criteria for selection will be the lowest cost to the TENDERER for the qualified bid. The TENDERER may negotiate the prices with L1 Bidder, under each item/head offered by Bidder.

**5.16.2** The TENDERER right to vary requirements at time of award: The TENDERER reserves the right at the time of award to increase or decrease quantity for the requirements originally specified in the document without any change in Bid rate or other terms and conditions.

**5.16.3** In case, the lowest bidder does not accept the award of contract or found to be involved in corrupt and/or fraudulent practices, the next lowest bidder will be awarded the contract. In such scenario, the next lowest bidder has to match the Lowest Bidder's Price and execute the project at the L1 Price for the entire contract duration.

## 5.17 NOTIFICATION OF AWARD & SIGNING OF CONTRACT

**5.17.1** Prior to expiration of the period of Bid validity, the TENDERER will notify the successful Bidders and issue Lol.

**5.17.2** Within Seven (7) calendar days of receipt of the Contract Form, the successful Bidder shall sign and date the Contract and return it to the TENDERER. The contract Performance guarantee has to be submitted within 15 calendar days of receipt of final work order. The Performance Bank guarantee shall be equal to 10% of the contract value valid for duration of 180 days beyond the expiry of contract.

## 5.18 FORCE MAJEURE

**5.18.1** Force Majeure shall mean any event or circumstances or combination of events or circumstances that materially and adversely affects, prevents or delays any Party in performance of its obligation in accordance with the terms of the Agreement, but only if and to the extent that such events and circumstances are not within the affected party's reasonable control, directly or indirectly, and effects of which could have prevented through

Good Industry Practice or, in the case of construction activities through reasonable skill and care, including through the expenditure of reasonable sums of money. Any events or circumstances meeting the description of the Force Majeure which have same effect upon the performance of any contractor shall constitute Force Majeure with respect to the TPA.

**5.18.2** The Parties shall ensure compliance of the terms of the Agreement unless affected by the Force Majeure Events. The TPA shall not be liable for forfeiture of its implementation / Performance guarantee, levy of Penalties, or termination for default if and to the extent that it's delay in performance or other failure to perform its obligations under the Agreement is the result of Force Majeure.

**5.18.3** Force Majeure Events: The Force Majeure circumstances and events shall include the following events to the extent that such events or their consequences (it being understood that if a causing event is within the reasonable control of the affected party, the direct consequences shall also be deemed to be within such party's reasonable control) satisfy the definition as stated above. Without limitation to the generality of the foregoing, Force Majeure Event shall include following events and circumstances and their effects to the extent that they, or their effects, satisfy the above requirements:

**5.18.4** Natural events ("Natural Events") to the extent they satisfy the foregoing requirements including:

**5.18.4.1** Any material effect on the natural elements, including lightning, fire, earthquake, cyclone, flood, storm, tornado, or typhoon;

**5.18.4.2** Explosion or chemical contamination (other than resulting from an act of war);

**5.18.4.3** Epidemic such as plague;

**5.18.4.4** Any event or circumstance of a nature analogous to any of the foregoing.

**5.18.5 Other Events** ("Political Events") to the extent that they satisfy the foregoing requirements including:

**5.18.5.1** Political Events which occur inside or Outside the State of Gujarat or involve directly the State Government and the Central Government ("Direct Political Event"), including:

- Act of war (whether declared or undeclared), invasion, armed conflict or act of foreign enemy, blockade, embargo, revolution, riot, insurrection, civil commotion, act of terrorism or sabotage;
- Strikes, work to rules, go-slows which are either widespread, nation- wide, or state-wide or are of political nature;
- Any event or circumstance of a nature analogous to any of the foregoing.

**5.18.6 FORCE MAJEURE EXCLUSIONS:** Force Majeure shall not include the following event(s) and/or circumstances, except to the extent that they are consequences of an event of Force Majeure:

**5.18.6.1** Unavailability, late delivery

**5.18.6.2** Delay in the performance of any contractor, sub-contractors or their agents;

**5.18.7 PROCEDURE FOR CALLING FORCE MAJEURE:** The Affected Party shall notify to the other Party in writing of the occurrence of the Force Majeure as soon as reasonably practicable, and in any event within 5 (five) days after the Affected Party came to know or ought reasonably to have

known, of its occurrence and that the Force Majeure would be likely to have a material impact on the performance of its obligations under the Agreement.

## **5.19 CONTRACT OBLIGATIONS:**

Once a contract is confirmed and signed, the terms and conditions contained therein shall take precedence over the Bidder's bid and all previous correspondence.

## **5.20 AMENDMENT TO THE AGREEMENT**

Amendments to the Agreement may be made by mutual agreement by both the Parties. No variation in or modification in the terms of the Agreement shall be made except by written amendment Signed by both the parties. All alterations and changes in the Agreement will take into account prevailing rules, regulations and laws applicable in the state of Gujarat.

## **5.21 REPRESENTATIONS AND WARRANTIES**

### **5.21.1 Representations and Warranties by the Selected Agency:**

- 5.21.1.1** It is a company/ organization under any statute of India duly organized and validly existing under the laws of India and has all requisite legal power and authority and corporate authorizations to execute the Agreement and carry out the terms, conditions and provisions hereof;
- 5.21.1.2** It has in full force and effect all requisite clearances, approvals and permits necessary to enter into the Agreement and perform its obligations hereof;
- 5.21.1.3** It will have the legally valid and enforceable title to all Equipment as may be necessary for proper functioning and it will be free from all encumbrances, liens, charges, any security interest and adverse claims of any description;
- 5.21.1.4** The Agreement and the transactions and obligations hereof do not contravene its constitutional documents or any law, regulation or government directive and will not contravene any provisions of, or constitute a default under, any other Agreement or instrument to which it is a party or by which it or its property may be bound or any of its obligations or undertakings by which it or any of its assets are bound or cause a limitation on its powers or cause it to exceed its authorized powers;
- 5.21.1.5** There is no pending or threatened actions, suits or proceedings affecting the selected agency or its affiliates or any of their respective assets before a court, governmental agency, commission or arbitrator or administrative tribunal which affects the selected agency's ability to perform its obligations under the Agreement; and neither selected agency nor any of its affiliates have immunity from the jurisdiction of a court or from legal process (whether through service of notice, attachment prior to judgment, attachment in aid of execution or otherwise);
- 5.21.1.6** The selected agency confirms that all representations and warranties of the selected agency set forth in the Agreement are true, complete and correct in all respects;
- 5.21.1.7** No information given by the selected agency in relation to the Agreement, project documents or any document comprising security contains any material misstatement of fact or omits to state as fact which would be materially averse to the enforcement of the rights and remedies of the TENDERER or which would be

necessary to make any statement, representation or warranty contained herein or therein true and correct;

**5.21.1.8** All equipment including material to be installed by the selected agency shall be new. All equipment shall conform to the codes, standards and regulations applicable to networking facilities and benefit from the usual manufacturer's guarantees.

**5.21.2 Representations and Warranties by the TENDERER**

**5.21.2.1** It has full legal right; power and authority to execute the said project and to enter into and perform its obligations under the Agreement and there are no proceedings pending.

**5.21.2.2** The Agreement has been duly authorized, executed and delivered by the TENDERER and constitutes valid, legal and binding obligation of TENDERER.

**5.21.2.3** The execution and delivery of the Agreement with the selected agency does not violate any statutory judgment, order, decree, regulation, right, obligation or rule of any court, government authority or arbitrator of competent jurisdiction applicable in relation to the TENDERER, its assets or its administration.

**5.22 RESOLUTION OF DISPUTES**

**5.22.1** If any dispute arises between the Parties hereto during the subsistence or thereafter, in connection with the validity, interpretation, implementation or alleged material breach of any provision of the Agreement or regarding a question, including the questions as to whether the termination of the Contract Agreement by one Party hereto has been legitimate, both Parties hereto shall endeavour to settle such dispute amicably. The attempt to bring about an amicable settlement is considered to have failed as soon as one of the Parties hereto, after reasonable attempts [which attempt shall continue for not less than 30 (thirty) days], give 15 days' notice thereof to the other Party in writing.

**5.22.2** In the case of such failure the dispute shall be referred to a sole arbitrator or in case of disagreement as to the appointment of the sole arbitrator to three arbitrators, two of whom will be appointed by each Party and the third appointed by the two arbitrators.

**5.22.3** The place of the arbitration shall be Gandhinagar, Gujarat.

**5.22.4** The Arbitration proceeding shall be governed by the Arbitration and Conciliation Act of 1996 as amended.

**5.22.5** The proceedings of arbitration shall be in English language.

**5.22.6** The arbitrator's award shall be substantiated in writing. The arbitration tribunal shall also decide on the costs of the arbitration procedure.

**5.22.7** The Parties hereto shall submit to the arbitrator's award and the award shall be enforceable in any competent court of law

**5.23 BOOKS & RECORDS**

The selected agency shall maintain adequate Documents Related to project's physical materials & equipment's for inspection and audit by the TENDERER during the terms of Contract until expiry of the performance guarantee.

**5.24 WARRANTY TERMS**

In the event that the materials supplied do not meet the specifications and / or are not in accordance with the Scope of work set out in this order, and rectification is required at all specified locations, The TENDERER shall notify the Successful bidder giving full details of difference. The Successful bidder shall attend to such materials (at specified locations) within seven days of receipt of such notice to meet and agree with representatives of GIL/Home Department, the action required to correct the deficiency. Should the Successful bidder fail to attend meeting at locations within the time specified above, the TENDERER shall be at liberty to rectify the work/materials and Successful bidder shall reimburse the TENDERER all costs and expenses incurred in connection with such trouble or defect.

## **5.25 PERFORMANCE GUARANTEE**

- 5.25.1** The Selected agency shall furnish Performance Guarantee as provided in the bid document to the TENDERER for an amount equal to 10% of the value of Order.
- 5.25.2** The performance guarantee will be in the form of bank guarantee for the amount equal to 10% of the value of the Order / LOI towards faithful performance of the contract obligation, and performance of the equipment during Warranty period. In case of poor and unsatisfactory field services, the TENDERER shall invoke the PBG.
- 5.25.3** The Performance Guarantee shall be valid for a period of 180 days beyond Contract period and shall be denominated in Indian Rupees and shall be in the form of an unconditional Bank Guarantee issued by all Public-Sector Banks / private banks having branch in Gandhinagar\Ahmedabad in the format provided by the TENDERER to be submitted Within 15 calendar days from the date of final work order.
- 5.25.4** The Performance Guarantee shall be discharged by the TENDERER and returned to the successful bidder within 30 calendar days from the date of expiry of the Performance Bank Guarantee.

## **5.26 TERMINATION CLAUSE**

- 5.26.1 Termination by the TENDERER:** The TENDERER, reserves the right to suspend any of the services and/or terminate this agreement in the following circumstances by giving 30 days' notice in writing if: -
  - 5.26.1.1** The bidder becomes the subject of bankruptcy, insolvency, and winding up, receivership proceedings;
  - 5.26.1.2** In case the TENDERER finds illegal use of hardware, software tools, manpower etc. that are dedicated to the project;
  - 5.26.1.3** In case the bidder fails to delivered, Installed and commission ordered items within the prescribed time lines and extension granted if any. In such scenario the TENDERER reserve the right to procure the same from other bidders at the risk, cost and responsibility of the selected agency.
- 5.26.2 Termination by Successful bidder:** The successful bidder reserves the right to suspend any of the Services and/or terminate the Agreement at any time with 30 days' notice if the payment to the selected is due for more than 2 (two) consecutive quarters.
- 5.26.3** Upon occurrence of an event of default as set out in Clause above, either party will deliver a default notice in writing to the other party which shall specify the event of default, and give the other party an opportunity to correct the default.

**5.26.4** Upon expiry of notice period unless the party receiving the default notice remedied the default, the party giving the default notice may terminate the Agreement.

**5.26.5** During the notice period, both parties shall, save as otherwise provided therein, continue to perform their respective obligations under this Agreement and shall not, whether by act of omission or commission impede or otherwise interfere with party's endeavour to remedy the default which gave rise to the commencement of such notice period.

**5.26.6** The termination hereof shall not affect any accrued right or liability of either Party nor affect the operation of the provisions of the Contract that are expressly or by implication intended to come into or continue in force on or after such termination.

## **5.27 INDEMNIFICATION**

Selected agency will defend and/or settle any claims against the TENDERER that allege that Bidder branded product or service as supplied under this contract infringes the intellectual property rights of a third party. Selected agency will rely on Customer's prompt notification of the claim and cooperation with our defense. Bidder may modify the product or service so as to be non-infringing and materially equivalent or we may procure a license. If these options are not available, we will refund to Customer the amount paid for the affected product in the first year or the depreciated value thereafter or, for support services, the balance of any pre-paid amount or, for professional services, the amount paid. Bidder is not responsible for claims resulting from any unauthorized use of the products or services. This section shall also apply to deliverables identified as such in the relevant Support Material except that Bidder is not responsible for claims resulting from deliverables content or design provided by Customer.

## **5.28 LIMITATION OF LIABILITY**

Selected agency's cumulative liability for its obligations under the contract shall not exceed the value of the charges payable by the TENDERER within the remaining duration of the contract term from the day claim is raised and selected agency shall not be liable for incidental, consequential, or indirect damages including loss of profit or saving.

## **5.29 CONFIDENTIALITY**

**5.29.1** Selected agency understands and agrees that all materials and information marked and identified by the TENDERER as 'Confidential' are valuable assets of the TENDERER and are to be considered GIL/Home Department proprietary information and property. Selected agency will treat all confidential materials and information provided by the TENDERER with the highest degree of care necessary to ensure that unauthorized disclosure does not occur. Selected agency will not use or disclose any materials or information provided by GIL/Home Department without its prior written permission.

**5.29.2** Selected agency shall not be liable for disclosure or use of any materials or information provided by the TENDERER or developed by selected agency which is:

**5.29.2.1** possessed by selected agency prior to receipt from the TENDERER, other than through prior disclosure by the TENDERER, as documented by selected agency's written records;

**5.29.2.2** published or available to the general public otherwise than through a breach of Confidentiality; or

**5.29.2.3** Obtained by selected agency from a third party with a valid right to make such disclosure, provided that said third party is not under a confidentiality obligation to the TENDERER; or

**5.29.2.4** Developed independently by the selected agency.

**5.29.3** In the event that selected agency is required by judicial or administrative process to disclose any information or materials required to be held confidential hereunder, selected agency shall promptly notify the TENDERER and allow reasonable time to oppose such process before making disclosure.

**5.29.4** Selected agency understands and agrees that any use or dissemination of information in violation of this Confidentiality Clause will cause the TENDERER irreparable harm, may leave the TENDERER with no adequate remedy at law and the TENDERER is entitled to seek to injunctive relief.

**5.29.5** The TENDERER does not follow the practice of asking Confidential Information of selected agency, however if any confidential information is required/shared by the selected agency then selected agency has to clearly marked it as “Strictly confidential”. The TENDERER in turn will not share the same without prior concern of the selected agency.

**5.29.6** Above mentioned “confidentiality clause” shall be applicable on both the parties i.e. the TENDERER and the successful bidder.

**5.30 PAYMENTS TERMS**

As mentioned above, following payment terms will be applied/adhere only after a formal work order is issued upon successful completion of project milestones:

S/N	Activity	Payment (%)
1	<b>Hardware/Material component as per Schedule I of financial bid</b>	
	<b>A) Central Infrastructure</b>	
	Successful Delivery and Inspection of Hardware/Equipment at the central location/ Bidder's Warehouse	50% of the Sum total of schedule I of financial bid
	Successful Installation, commissioning and FAT	30% of the Sum total of schedule I of financial bid
	Successful Completion of 6 months from the date of FAT	20% of the Sum total of schedule I of financial bid
	<b>B) End Devices, and Edge Locations Infrastructure</b>	
	Successful Delivery and Inspection of each lot of 25 % at the central location/ Bidder's Warehouse	60% of the Sum total of schedule I of financial bid
	Successful Installation, Commissioning & FAT of each lot of 25%	30% of the Sum total of schedule I of financial bid
	Successful Completion of 3 months from the date of FAT	10% of the Sum total of schedule I of financial bid
2	<b>Operations &amp; Maintenance as per Schedule II of financial bid</b>	



S/N	Activity	Payment (%)
	Operational & Maintenance support during the contract period of 5 years	20 equal Quarterly Installments after the end of each quarter.

### 5.30.1 Payment Procedure:

#### a) Hardware/Material Component

- 1) The successful bidder shall raise the component wise invoice against the milestones achieved (as mentioned above in the payment schedule) and submit the invoice to the TENDERER.
- 2) The successful bidder shall submit 2 original copies of invoices along with the necessary supporting documents confirming milestone achieved and other documents as required by the TENDERER for processing of invoices. Invoice should be raised in English language only.
- 3) The TENDERER shall verify the Invoices raised against the milestone achieved and shall make the payment.

#### b) O&M Component

- 1) The payments to the successful bidder will be made quarterly at the end of each quarter on acceptance of the invoice by the TENDERER or its designated agency.
- 2) The invoice would be processed for release of payment within 45 days after due verification of the invoice and other supporting documents by the TENDERER or its designated agency.
- 3) In case the processing of the invoice gets delayed beyond 45 days from the date of acceptance of invoice, the successful bidder would be paid an adhoc amount of 50% of invoice value and the remaining amount would be released after getting clarifications, due verification and imposition of penalty, if any.

34.1 Payment shall be made in Indian Rupees. While making payment, necessary income tax and service tax deductions will be made.

## 5.31 SERVICE TERMS

**5.31.1** The entire scope of the work depends on the technical skill and experience in management of the same level or kind of capabilities.

**5.31.2** It is mandatory for Bidder to deploy qualified professional to install, commission & maintain the proposed applications, as defined under scope of work.

**5.31.3** The Bidder has to submit regular schedule of man power availability & get it approved by the TENDERER, before deployment.

**5.31.4** The Bidder will have to carry out reinstallation of any of the software equipment 'Free of Cost, if required.

**5.31.5** The Bidder need to manage & maintain various records related to the services extended to the Government.

**5.31.6** If required, the Bidder may need to coordinate and approach various agencies working for the TENDERER.

**5.31.7** The Bidder needs to maintain the required Information security of the databases as per the TENDERER'S Security guidelines.

- 5.31.8 The Bidder is responsible to maintain documentation on the progress of the work and will have to update the same on regular basis. Successful bidder will have to submit the progress reports regularly, as per the guide line issued by the TENDERER.
- 5.31.9 In case of any upgrade, customization and patches the bidder will have to take necessary permission from the TENDERER.
- 5.31.10 All expenses related to installation, testing and deployment, has to be borne by the Bidder as part of Contract Agreement.
- 5.31.11 Bidder shall submit test procedures covering various test cases and expected results of these tests relating to various systems being commissioned.

**5.32 WARRANTY SUPPORT**

- 5.32.1 Bidder shall provide a comprehensive on site free support for 5 years from the date of FAT for all applications.
- 5.32.2 Bidder shall provide the comprehensive support in respect of proper design, quality and security for all the software applications covered by the RFP. Bidder must warrant all software procured/developed and implemented as per this RFP against any bugs/issues during the support period.
- 5.32.3 Bidder shall provide the performance warranty in respect of performance of the installed software to meet the performance requirements and service levels in the RFP.
- 5.32.4 Bidder is responsible for sizing and procuring the necessary software/database licenses as per the performance requirements provided in the RFP. During the warranty period bidder shall augment or procure additional licenses at no additional cost in case the procured hardware or software is not adequate to meet the service levels.

**5.33 SERVICE LEVEL AND PENALTY CLAUSE**

- 5.33.1 SLA defines the terms of the successful bidder’s responsibility in ensuring the performance of the network based on the agreed performance indicators as detailed in the agreement. Successful bidder has to co-ordinate with ISP and get the complaint closed and also has to produce documentary evidence regarding failure of Bandwidth by ISP & not by Network equipment’s.
- 5.33.2 The table below summarizes the performance indicators for the services to be offered by the bidder-

S/N	SLA Terms	Description
1	Network Backbone	‘Network Backbone’ refers to Internet Protocol (IP) based routing infrastructure at which, successful bidder has installed network devices for city Wide Area Network.
2	Uptime	‘Uptime’ refers to network backbone availability across various segments of City wide area network i.e. between Zonal office and ward offices and ward offices and junction/locations. “%Uptime” means ratio of ‘up time’ (in minutes) in a month to Total time (in minutes) in the month multiplied by 100.

S/N	SLA Terms	Description																				
3	Latency	'Latency' refers to the average time required for round-trip packet transfers between Selected Junctions/locations on the selected portions of the network Backbone during a calendar month.																				
4	Packet Loss	'Packet Loss' refers to the average percentage of IP packets transmitted between Selected Junctions/locations during a calendar month that are not successfully delivered.																				
5	Planned Network Outage	'Planned Network Outage' refers to unavailability of network services due to infrastructure maintenance activities such as configuration changes, up gradation or changes to any supporting infrastructure. Details related to such planned outage shall be approved by the TENDERER or authorized authority and shall be notified to all the concerned stakeholder in advance (at least five working days). It is desirable that such outage shall be taken on Sundays or other Government holidays to the extent possible.																				
6	Unplanned Network Outage	'Unplanned Network Outage' refers to an instance in which no traffic can pass in or out through which users are connects to the network Backbone																				
8	Not keeping manpower	If successful bidder does not deploy the required specified quantity & quality of manpower as per RFP or a person deployed is not reporting to the duty, there would be a penalty per person per day as defined in below table and will be deducted from the quarterly payment																				
9	Accuracy of ANPR/RLVD System	a) The TENDERER or its nominated agency shall visit the CCC to check the accuracy of the said systems on random basis and mark out the difference if found lower than the accuracy level as per the SoW.																				
10	Incidence Resolution (Network)	<p>The network outage, security or performance related issues impacting the network availability/performance and leading to unavailability of the services. Resolution of incidence as per below priority Levels:</p> <ul style="list-style-type: none"> <li>• <b>L1 Level Severity:</b> Impacting DC or Command &amp; Control Center.</li> <li>• <b>L2 Level Severity:</b> impacting one or more Zones.</li> <li>• <b>L3 Level Severity:</b> Impacting one or Junctions/ Endpoints/ Offices</li> <li>• <b>L4 Level Severity:</b> Impacting one or more end devices/utilities</li> </ul> <table border="1"> <thead> <tr> <th>#</th> <th>Severity</th> <th>Initial Response Time</th> <th>Issue Resolution Time</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Level 1</td> <td>15 Mins</td> <td>1 Hour</td> </tr> <tr> <td>2</td> <td>Level 2</td> <td>30 Mins</td> <td>2 Hours</td> </tr> <tr> <td>3</td> <td>Level 3</td> <td>60 Mins</td> <td>6 Hours</td> </tr> <tr> <td>4.</td> <td>Level 4</td> <td>240 Mins</td> <td>24 Hours</td> </tr> </tbody> </table>	#	Severity	Initial Response Time	Issue Resolution Time	1	Level 1	15 Mins	1 Hour	2	Level 2	30 Mins	2 Hours	3	Level 3	60 Mins	6 Hours	4.	Level 4	240 Mins	24 Hours
#	Severity	Initial Response Time	Issue Resolution Time																			
1	Level 1	15 Mins	1 Hour																			
2	Level 2	30 Mins	2 Hours																			
3	Level 3	60 Mins	6 Hours																			
4.	Level 4	240 Mins	24 Hours																			
12	Security Breach	<ul style="list-style-type: none"> <li>• Detection of security Breach - within 30 minutes</li> <li>• Mitigation of Security Breach - within 1 hr. from the time of Breach</li> <li>• <b>Note:</b> The security breach will include but not limited to successful penetration of any Virus, trojan, malwares, zero-day attacks, intrusion, Denial of Service Attacks, etc., up to the server level. In case of any compromise of data due to the Security Breach then double penalty will be levied (this will not be counted within the maximum penalty cap limit).</li> </ul>																				

- Appropriate Penalties will be recovered from the quarterly payment if successful bidder is not able to achieve required Service levels as mentioned below:

S/N	SLA	Target	Penalties
1	Delay in Delivery of Hardware	As per Implementation Time Lines	<ul style="list-style-type: none"> <li>• 0.5% of Contract value of undelivered/delayed Items (as per Schedule-I of Price BID) per week or part thereof for delay in delivery</li> <li>• Delay beyond 90 days the TENDERER may terminate the contract and Forfeit the PBG.</li> </ul>
2	Delay in Implementation: Installation and Commissioning and FAT of hardware/software at Central and Site Location	As per Implementation Time Lines	<ul style="list-style-type: none"> <li>• 0.75% of Contract value of delayed part (as per Schedule-I of Price BID) per week or part thereof for delay in implementation</li> <li>• Delay Beyond 150 days the TENDERER may terminate the contract and Forfeit the PBG)</li> </ul>

*Note: The Overall Penalty for Schedule I shall be capped at 10 % of the contract value or 20 % of the unpaid item, whichever is less. However maximum cap is 10 % of the contract value (Schedule I)*

⇒ **Operational Penalties during the O&M Period:**

S/N	SLA	Target	Penalties
1	Availability/Uptime of End Points like CCTV camera, switches, routers, IR Illuminators etc.	99.00%	<ul style="list-style-type: none"> <li>• 99.00% or Better= NIL</li> <li>• 98.50% to 98.99%=0.50% of QP</li> <li>• 98.00 to 99.49% = 1.00% of QP</li> <li>• less than 98% = 1.50% of QP</li> </ul>
2	Not keeping required Manpower	As per SLA	<ul style="list-style-type: none"> <li>• <b>Management level staffs like PM/ Manager:</b> 5000/- per day per person for un-sanctioned/ non-reporting</li> <li>• <b>All other staffs other than computer operator:</b> 1000/- per day per person for un-sanctioned/ non-reporting</li> <li>• <b>Computer operator:</b> Rs. 500/- per day per person for un-sanctioned/ non-reporting</li> <li>• <b>Above charges are in addition to deduction of actual wages for the period of absence based on the rate schedule</b></li> </ul>
3	Latency (Device only)	Less than 50ms	<ul style="list-style-type: none"> <li>• Rs. 2000 per hour, per instance or part thereof.</li> <li>• Successful bidder has to analyse, report, escalate and get the issue resolved within 24 hours.</li> </ul>
4	Packet Loss (Device only)	<=0.5%	<ul style="list-style-type: none"> <li>• Rs. 2000 per hour, per instance or part thereof.</li> <li>• Successful bidder has to analyse report, escalate and get the issue resolved within 6 hours.</li> </ul>

5	Accuracy of ANPR/RLVD	As per SLA	<ul style="list-style-type: none"> <li>Rs. 500,000/- per month</li> <li>Any continuing default extending beyond 4 months will be a reasonable ground for termination of this contract.</li> </ul>
6	Delay in resolution of support/incidents for the devices installed by the bidder	As per SLA	<ul style="list-style-type: none"> <li>Level 1: 0.25% of QP for every 2 Hours Delay in resolution, capped to 3% of QP every incident</li> <li>Level 2: 0.10% of QP for every 2 Hours delay in resolution, capped to 1% of QP every incident</li> <li>Level 3: 0.10% of QP for every 6 Hours delay in resolution, capped to 1% of QP every incident</li> <li>Level 4: 0.10% of QP for every 12 Hours delay in resolution, capped to 1% of QP every incident</li> </ul>
7	Time Line for Retrieval from the Storage	Maximum 30 Minute for per request is allowed	<ul style="list-style-type: none"> <li>Rs. 500 for every instance of late retrieval beyond 30 minutes</li> <li>Note: Data Retrieval Request Through a Request Log Mechanism</li> </ul>
8	Uptime of all IT components & services under scope	99.741% (at each individual component level)	<ul style="list-style-type: none"> <li>For each component 99.241-99.741 - 1.0% of QP; 98.741-99.241 - 2.0% of QP</li> <li>And so on If the uptime goes below 96.741, additional penalty of 1% will be charged on QP for each slab 1% downtime.</li> </ul>
9	Uptime of all non-IT Components & services under scope	99.741% (at each individual component level)	<ul style="list-style-type: none"> <li>99.249-99.749 - 0.5% of QP; 98.749-99.249 - 1.0% of QP</li> <li>And so on If the uptime goes below 96.749%, additional penalty of 0.5% will be charged on QP for a slab of 1%.</li> </ul>
10	Security Breach	As per SLA	<ul style="list-style-type: none"> <li>3% Of QP for every 30 Minutes delay in detection and additional 1% for every 1 hour. delay in the mitigation of security breach</li> </ul>

- Successful Bidder shall be paid Quarterly Payment (QP) as per the services provided to the TENDERER. The overall penalty would be generally capped at 10% of QP amount. If the cap of overall penalty is reached in two consecutive quarters, the penalty cap for the third quarter onwards, for each quarter will increase by 5% over the penalty cap for the preceding quarter till it reaches 25% of the QP. In addition to the applicable penalty and the provisions pertaining to closure/termination of contract, the TENDERER shall be within its rights to undertake termination of contract if or anytime the penalty increases by 20 % of the QP. Once the penalty cap has increased beyond 10%, if the bidder through better performance delivery for any quarter, brings the leviable penalty below 10% then the computation of the 1st of the 2 consecutive quarters as referred above will reset and will begin afresh. Availability will be calculated on a quarterly basis.
- The above clause for penalties due to delay in FAT shall only be applicable for the delay attributed solely to the successful bidder as per his roles and responsibilities, delay due to other reasons shall not be considered.

### 5.34 APPROVALS/CLEARANCES

**5.34.1** Necessary approvals/ clearances concerned authorities, for establishing the proposed project are to be obtained by the Selected agency.

**5.34.2** Necessary approvals/ clearances from concerned authorities, as required, for fire protection, government duties / taxes/ Octroi are to be obtained by the Selected agency.

### **5.35 PROJECT IMPLEMENTATION**

**5.35.1** The home department may appoint a Third party auditor who will be responsible for the Project and all inspection, installation, commissioning and acceptance of work will be undertaken by them. All Invoices, Vouchers, Bills for supplied goods and services by the Successful bidder under the scope of the work will be verified measured and accepted by the TPA, for release of payment.

**5.35.2** As part of implementation, the successful bidder shall provide details of equipment that will be incorporated in the proposed system, material and manpower as required. The location for storing spare parts and quantity there on should also be clearly indicated.

**5.35.3** The successful bidder will implement the project strictly as per the plan approved by the TENDERER. The successful bidder shall install and implement the proposed system at such locations as may be selected by the TENDERER as per the project timeline as per Clause 4.2.10.

**5.35.4** The Successful bidder shall provide the necessary Training, technical support, Standard Operating Procedure (SOP) and other information to the TENDERER'S and its users in and after implementing the proposed system. The TENDERER at any time during the currency of the Agreement should have access to the proposed content.

**5.35.5** The successful bidder shall arrange to obtain all statutory and regulatory permission (If any) at no cost to the Government of Gujarat.

**5.35.6** The successful bidder may have to work during Holidays and Sundays, according to the urgency of work. It will be the responsibility of the Successful bidder to co-ordinate with all other agencies of Government of Gujarat in order to obtain NOC required to execute the job. However the Home department may assist in getting such approvals/NOC as the case may be.

**5.35.7** Successful bidder shall treat all matters connected with the contract strictly confidential and shall undertake not to disclose, in any way, information, documents, technical data, experience and know how, without prior written permission from the TENDERER.

**5.35.8** Any damage caused to the property of Government of Gujarat while executing the job shall be solely Successful bidder's responsibility. In case any damage to the property is caused, the same will be recovered from the Successful bidder.

### **5.36 THIRD PARTY**

The TENDERER may appoint/designate a Third Party for IT Infrastructure projects, which would monitor the project during implementation, commissioning and operation. The Third Party will also conduct User Acceptance Test and Final Acceptance Test as per the technical requirement of the Agreement and will issue the Certificate of Completion of each proposed Site. Third Party will verify the services provided by the successful bidder under the agreement. The successful bidder will co-operate with such Third Party.

### **5.37 FRAUDULENT AND CORRUPT PRACTICES**

**5.37.1** Fraudulent practice means a misrepresentation of facts in order to influence a procurement process or the execution of a Contract and includes collusive practice among Bidders (prior to or after Bid submission) designed to establish Bid prices at artificial non-competitive levels and to deprive the TENDERER of the benefits of free and open competition.

**5.37.2** "Corrupt Practice" means the offering, giving, receiving or soliciting of anything of value, pressurizing to influence the action of a public official in the process of Contract execution.

**5.37.3** The TENDERER will reject a proposal for award and may forfeit the EMD and/or Performance Bank Guarantee if it determines that the bidder recommended for award has engaged in corrupt or fraudulent practices in competing for, or in executing, contract(s).

**5.38 MIS REPORTS:**

**5.38.1** Bidder is required to submit various MIS reports to the TENDERER in support of SLA compliance along with its quarterly invoice and as and when asked by the TENDERER. Following is the minimum indicative list of types of MIS reports to be submitted by bidder:

S/n	Activity	Periodicity
1	<b>Video Management System</b>	<b>Daily</b>
2	No. of Camera Feeds latched onto the VMS	
3	Report of Working /Non-Working/Tampered Cameras	
4	Ageing Report of issues/Incidents	
5	Memory utilization of the Storage	<b>Weekly</b>
6	SLA compliance reports	<b>Quarterly</b>
7	Preventive maintenance reports	
8	Configuration change reports	
9	<b>Automatic Traffic Enforcement system</b>	
10	No. of Violations captured with Details	
11	Resource Consumption of the Hosted Applications	As and when required

**5.39 ACCEPTANCE TESTS**

Acceptance Test will be conducted in as follows:

**5.39.1** TENDERER reserves the right to inspect goods and services supplied as per the scope of this RFP document. The cost of all such tests shall be borne by the Vendor. Any inspected goods fail for confirm to the specification will be rejected, and Vendor shall have to replace the rejected goods as per the contract specification without any financial implication to the TENDERER.

**5.39.2** Final Acceptance Test (FAT): After successful installation of the System in accordance with the requirements as mentioned in Schedule of Requirement, Final Acceptance Test will be conducted. After successful testing, Acceptance Test Certificate will be issued by TENDERER or its designated agency to the Vendor.

**5.39.3** The date on which Acceptance certificate is issued shall be deemed to be the date of successful commissioning of the System.

**5.39.4** Any delay by the Vendor in the Acceptance Testing shall render the Vendor liable to the imposition of appropriate Penalties.

**5.39.5** Bidder is required to update the details of Hardware installed in the Assets Master of IWDMS and the TENDERER before completion of FAT.

**5.40 COPYRIGHT AND INTELLECTUAL PROPERTY RIGHTS**

**5.40.1** The TENDERER will have exclusive right to use and own the application software (as customized from time to time), its source code along with further development rights and its

derivatives. The software prepared cannot be used for any purpose whatsoever without the written consent of the TENDERER.

**5.40.2** No software or services covered by the contract shall be developed or done by the company in violation of any right whatsoever of third party, and in particular, but without prejudice to the generality of the foregoing of any patent right, trademark or Similar right, or of any charge, mortgage or lien. Vendor will indemnify the TENDERER for all such correspondence.



***SECTION-VI***  
***Price Bid***

# Price Bid

Amount in INR

S/N	ITEM	Make and Model	UOM	Qty. (in Nos.)	Unit Price with 5 Year Warranty (without Taxes)	Total Price (Without Taxes)	Rate of VAT/ Service Tax (%)
A	B	C	D	E	F	G=E*F	H
<b>SCHEDULE – I</b>							
<b>Central Infrastructure</b>							
<b>For Command and Control Centre</b>							
1.	Video Wall Solution for the state Center - 55", in a 4 X 3 arrangement (with video Controller)		Nos.	01			
2.	Online UPS Type 1-for CCC		Nos.	01			
3.	Access Control System		Nos.	01			
4.	Storage- Type 1 (For Applications for CCC); Capacity- 10 TB)		Nos	01			
5.	Storage- (For Video feeds at CCC)		Nos.	01			
6.	Enterprise Management System for CCC		Nos.	01			
7.	Workstations (3 monitors) for Live and Playback		Nos.	10			
8.	Desktop PC's		Nos.	20			
9.	Indoor Fixed Dome Cameras		Nos.	10			
10.	Router for CCC		Nos.	02			
11.	Internet Router for CCC		Nos.	02			
12.	L3 Switch for CCC		Nos.	02			
13.	L2 Switch for CCC		Nos.	02			
14.	UTM with centralized Management for CCC		Nos.	02			
15.	Web Application Firewall for CCC		Nos.	02			
16.	42U Server Rack		Nos.	02			
17.	42U Network Rack		Nos.	04			

S/N	ITEM	Make and Model	UOM	Qty. (in Nos.)	Unit Price with 5 Year Warranty (without Taxes)	Total Price (Without Taxes)	Rate of VAT/ Service Tax (%)
18.	Central Antivirus Software		Nos.	01			
19.	Blade Server with chassis		Nos.	10			
20.	VMS Software and Video Analytics for Stored videos, Mobile Application for Remote viewing of Video Feeds (with all required hardware for all locations)		Nos.	01			
21.	VMS License bank for Camera		Nos.	5000			
22.	Application and System Software and licenses for E-challan system (Application, System Software, applicable licenses with required hardware for all locations)		Nos.	01			
23.	Automatic Number Plate Recognition (ANPR) with Speed Detection System including all required Hardware, Application and System Software with applicable licenses		Nos.	01			
24.	Application and System Software and licenses for RLVD (Application, System Software, applicable enterprise licenses with required hardware for application)		Nos.	01			
25.	Server Load Balancer		Nos.	02			
26.	RDBMS Licenses		Nos.	01			
<b>For District Control Room's</b>							
27.	Video Wall Solution- Type 2 for the District Control Room, in a 4 X 2 arrangement (with video Controller)		Nos.	29			
28.	Online UPS Type 2-for District Control Centre		Nos.	29			
29.	Access Control System		Nos.	29			
30.	Storage- Type 2 (For Applications for District Control Centre); Capacity- 5 TB)		Nos.	29			
31.	Storage- (For Video feeds at District Control Rooms)- Category 1		Nos.	15			
32.	Storage- (For Video feeds at District Control Rooms)- Category 2		Nos.	10			

S/N	ITEM	Make and Model	UOM	Qty. (in Nos.)	Unit Price with 5 Year Warranty (without Taxes)	Total Price (Without Taxes)	Rate of VAT/ Service Tax (%)
33.	Storage- (For Video feeds at District Control Rooms)- Category 3		Nos.	05			
34.	Workstations (3 monitors) for Live and Playback		Nos.	150			
35.	Desktop PC's		Nos.	240			
36.	Indoor Fixed Dome Cameras		Nos.	150			
37.	Router for District Control Room Category 1		Nos.	30			
38.	Router for District Control Room Category 2		Nos.	20			
39.	Router for District Control Room Category 3		Nos.	10			
40.	L3 Switch for District Control Room Category 1		Nos.	30			
41.	L3 Switch for District Control Room Category 2		Nos.	20			
42.	L3 Switch for District Control Room Category 3		Nos.	10			
43.	L2 switch for District Control Room Category 1		Nos.	20			
44.	L2 switch for District Control Room Category 2		Nos.	20			
45.	L2 switch for District Control Room Category 3		Nos.	10			
46.	Firewall with IPS for District Control Centre- Category 1		Nos.	15			
47.	Firewall with IPS for District Control Centre- Category 2		Nos.	10			
48.	Firewall with IPS for District Control Centre- Category 3		Nos.	05			
49.	Server Load Balancer		Nos.	30			
50.	42 U Server Rack		Nos.	60			
51.	42 U Network Rack		Nos.	30			
<b>For City Control Room</b>							
52.	Video Wall Solution- Type 3 for the City Control Room, in a 2 X 2 arrangement (with video Controller)		Nos.	10			
53.	Online UPS Type 3-for City Control Centre		Nos.	10			
54.	Access Control System		Nos.	10			

S/N	ITEM	Make and Model	UOM	Qty. (in Nos.)	Unit Price with 5 Year Warranty (without Taxes)	Total Price (Without Taxes)	Rate of VAT/ Service Tax (%)
55.	Workstations (3 monitors) for Live and Playback		Nos.	20			
56.	Desktop PC's		Nos.	20			
57.	Router for City Control Room Category 1		Nos.	14			
58.	Router for City Control Room Category 2		Nos.	06			
59.	L2 Switch for City Control Room		Nos.	20			
60.	Indoor Fixed Dome Cameras		Nos.	50			
61.	19U Network Rack		Nos.	20			
62.	42U Server Rack		Nos.	10			
<b>For End Point Items</b>							
63.	Junction Box, with adjustable mounting trays		Nos.	1250			
64.	Poles including mounting/installation		Nos.	500			
65.	Gantry including mounting/installation		Nos.	100			
66.	IP Camera Type A: ANPR and Speed Detection		Nos.	454			
67.	IP Camera Type A: with 8MP for RLVD		Nos.	105			
68.	IP Camera Type B: Surveillance		Nos.	3500			
69.	IP Camera Type C: PTZ		Nos.	400			
70.	Managed Outdoor L2 Switch with PoE - 8-port with Fiber Port		Nos.	1250			
71.	Managed Outdoor L2 Switch with PoE - 8-port		Nos.	100			
72.	CCTV: Sign Board for location under surveillance		Nos.	2000			
73.	LIU (6 core for SC, FC, ST, & LC)		Nos.	1250			
<b>Total</b>							
<b>SCHEDULE – II</b>							
1.	Operations and Maintenance for the Project for 5 Years		Nos.	01			
<b>Total</b>							
<b>Grand Total (Sch. I+II)</b>							

**Note:**

- All the above-mentioned line items should comply to Technical specifications and Scope of work including all applicable Licenses, Active and passive Cabling and Accessories, Installation, Commissioning and Configuration with 5 Year Warranty and onsite Support.

2. The L1 Shall be calculated as  $L1\ Price = \{Sum\ Total\ of\ all\ the\ line\ Items\ i.e.\ Item\ no.1\ to\ 20\ and\ 22\ to\ 73\ of\ schedule\ I\} + (100 * Total\ Cost\ of\ Item\ no.\ 33\ of\ schedule\ I) + \{O\&M\ Charges\ as\ per\ Schedule\ II\}$ , without Taxes.
3. Above mentioned quantities are indicative and for evaluation purpose only, actual quantities may vary at the time of placing the order.
4. Price Bid-Schedule-II: Operations and maintenance cost for 5 years to be quoted by the bidder should not be less than 25% of sum total of all the line items of schedule-I
5. Sum Total of Schedule – II would be paid in 20 equated Quarters.
6. Bidder needs to upload detailed priced BOQ along with the Part code and pricing of all the line items
7. The Successful bidder needs to account for all Out of Pocket expenses due to Boarding, Lodging and other related items.
8. The tender rates shall be valid for 1 Year.
9. The TENDERER reserves the right to ask the Successful Bidder to submit proof of payment against any of the taxes, duties, levies indicated.

***SECTION-VII***  
**Formats & Annexures**

## Format I– Proposal Covering Letter

(To be on the Bidder’s letterhead duly Signed by Authorized Signatory)

Tender Ref No:

To

**DGM (Tech)**

**Gujarat Informatics Ltd.**

**Block no. 1, 8th floor, Udyog Bhavan,**

**Sector-11, Gandhinagar**

**Reference: “Request for proposal (RFP) for selection of Implementing agency for Supply, Installation and Operations & Maintenance of State Wide Surveillance and ITMS project across the State of Gujarat”**

Dear Sir,

We ..... (Name of the bidder) hereby submit our proposal in response to notice inviting tender date ..... and tender document no. .... and confirm that:

1. All information provided in this proposal and in the attachments, is true and correct to the best of our knowledge and belief.
2. We shall make available any additional information if required to verify the correctness of the above statement.
3. Certified that the period of validity of bids is 180 days from the last date of submission of proposal, and
4. We are quoting for all the items (including services) as per the price bid format Section-VII as mentioned in the RFP.
5. We the Bidder are not under a declaration of Ineligibility for corrupt or fraudulent practices or blacklisted by any of the Government agencies.
6. We have an office in the state and relevant documents for the same are attached. We undertake that if the local presence is not there in the state, that we shall establish an office at Gandhinagar/ Ahmedabad, within 45 days from the date of the award of contract.
7. Gujarat Informatics Limited may contact the following person for further Information regarding this tender: -
  - a. Name & Designation:
  - b. Full address of office
  - c. Email ID & Contact No.
8. We are uploading our Response to the RFP (Eligibility, technical and financial bid documents) as per the instructions set out in this RFP.

Yours Sincerely,

**(Signature)**

**Name of Authorized Signatory:**

**Designation:**

**Date:**

**Name of the bidder:**



## Format II: Format for Power of Attorney

(To be provided in original on stamp paper of value required under law duly Signed by 'bidder')

Dated:

### POWER OF ATTORNEY

#### To Whomsoever It May Concern

Know all men by these presents, we \_\_\_\_\_ (name and registered office address of the Bidder) do hereby constitute, appoint and authorize Mr./Ms./Mrs. \_\_\_\_\_ (Name of the Person(s)), domiciled at \_\_\_\_\_ (Address), acting as \_\_\_\_\_ (Designation and the name of the firm), as Authorized Signatory and whose Signature is attested below, as our attorney, to do in our name and on our behalf, all such acts, deeds and things necessary in connection with or incidental to our Proposal for award of Contract **"Request for proposal (RFP) for selection of Implementing agency for Supply, Installation and Operations & Maintenance of State Wide Surveillance and ITMS project across the State of Gujarat."** involving the deliverables including Provisioning for Software, Networking and IT infrastructure, Implementation Services, Operations, Maintenance and support for at least 5 years as per location provided in RFP issued by GIL, vide RFP (Tender Document) Document No. \_\_\_\_\_ dated \_\_\_\_\_, issued by Gujarat Informatics Limited, including Signing and submission of all documents and providing information and responses to clarifications / enquiries etc. as may be required by Gujarat Informatics Limited or any governmental authority, representing us in all matters before Gujarat informatics Limited, and generally dealing with GIL in all matters in connection with our Proposal for the said Project. We hereby agree to ratify all acts, deeds and things lawfully done by our said attorney pursuant to this Power of Attorney and that all acts, deeds and things done by our aforesaid attorney shall and shall always be deemed to have been done by us.

For -----

(Signature)

(Name, Title and Address)

Accept (Attested Signature of Mr./Ms./Mrs. \_\_\_\_\_)

(Name, Title and Address of the Attorney)

Notes: - To be executed by the Bidder - The mode of execution of the Power of Attorney should be in accordance with the procedure, if any, laid down by the applicable law and the charter documents of the executant(s) and when it is so required the same should be under common seal affixed in accordance with the required procedure. - Also, wherever required, the executant(s) should submit for verification the extract of the charter documents and documents such as a resolution / power of attorney in favor of the Person executing this Power of Attorney for the delegation of power hereunder on behalf of the executants(s).

## Format III-Authorization Letter from Original Equipment Manufacturer (OEM)

(To be provided as part of Technical Bid on letter head Signed by the authorized representative of OEM in favor of 'bidder')

To

**DGM (Tech)**

**Gujarat Informatics Ltd**

**Block no. 1, 8th floor, Udyog Bhavan,**

**Sector-11, Gandhinagar**

Tender Ref No:

Subject: **"Request for proposal (RFP) for selection of Implementing agency for Supply, Installation and Operations & Maintenance of State Wide Surveillance and ITMS project across the State of Gujarat"**

Dear Sir,

I/We ..... [manufacturer] having our office/works at .....hereby certify that M/s ..... [Bidder] is an authorized ..... [relationship] of ..... [manufacturer] and they are authorized to represent ..... [manufacturer] in submitting their bid for ..... [product& services] and conclude the contract with you.

We ..... [manufacturer] are confident of M/s [Bidder's] ability to represent us and provide full support in making your project successful. We ..... [manufacturer] have authorized ..... to quote for this tender.

I / We ..... hereby commit & confirm the following:

- a) The duration of the service support will be for a period of five years from the date of supply of equipment.
- b) The service support will be provided onsite and will not be charged extra.
- c) The service support will be comprehensive hence no extra charge is to be paid for any Hardware failure.

Signature .....

Name .....

Designation .....

## Format IV- Bank Guarantee format for Earnest Money Deposit

To

Dated:

**DGM (Tech)**

**Gujarat Informatics Ltd**

**Block no. 1, 8th floor, Udyog Bhavan,**

**Sector-11, Gandhinagar**

Whereas ----- (here in after called "the Bidder") has submitted its bid dated ----- in response to the Tender no: XXXXXXXXX for ----- KNOW ALL MEN by these presents that WE ----- having our registered office at ----- (hereinafter called "the Bank") are bound unto the -----, Gujarat Informatics Limited in the sum of ----- for which payment well and truly to be made to Gujarat Informatics Limited, the Bank binds itself, its successors and assigns by these presents. Sealed with the Common Seal of the said Bank this -----day of -----2017.

### **THE CONDITIONS of this obligation are:**

The EMD may be forfeited, In case of a Bidder if:

- 1) The bidder withdraws its bid during the period of bid validity.
  - a. The Bidder does not respond to requests for clarification of their Bid.
  - b. The Bidder fails to co-operate in the Bid evaluation process.
  - c. The bidder, fails to furnish Performance Bank Guarantee in time.
- 2) The bidder fails to Sign the contract in accordance with this RFP
- 3) The bidder is found to be involved in fraudulent and corrupt practices

We undertake to pay to the GIL up to the above amount upon receipt of its first written demand, without GIL having to substantiate its demand, provided that in its demand GIL will specify that the amount claimed by it is due to it owing to the occurrence of any of the above mentioned conditions, specifying the occurred condition or conditions.

This guarantee will remain valid up to 6 months from the last date of bid submission. The Bank undertakes not to revoke this guarantee during its currency without previous consent of the GIL and further agrees that the guarantee herein contained shall continue to be enforceable till the GIL discharges this guarantee

The Bank shall not be released of its obligations under these presents by any exercise by the GIL of its liability with reference to the matters aforesaid or any of them or by reason or any other acts of omission or commission on the part of the GIL or any other indulgence shown by the GIL or by any other matter or things.

The Bank also agree that the GIL at its option shall be entitled to enforce this Guarantee against the Bank as a Principal Debtor, in the first instance without proceeding against the SELLER and not withstanding any security or other guarantee that the TENDERER may have in relation to the SELLER's liabilities.

Dated at \_\_\_\_\_ on this \_\_\_\_\_ day of \_\_\_\_\_ 2017.

Signed and delivered by

\_\_\_\_\_  
For & on Behalf of

Name of the Bank & Branch &

Its official Address with seal

**Approved Bank:** Any Nationalized Bank operating in India having branch at Ahmedabad/ Gandhinagar

## Format-V- PERFORMANCE BANK GUARANTEE

(To be stamped in accordance with Stamp Act)

Ref:

Bank Guarantee No.

Date:

To,

**DGM (Tech)**

**Gujarat Informatics Ltd**

**Block no. 1, 8th floor, Udyog Bhavan,**

**Sector-11, Gandhinagar**

Dear Sir,

WHEREAS..... (Name of Bidder) hereinafter called "the Bidder" has undertaken, in pursuance of Agreement dated, (hereinafter referred to as "the Agreement for **Request for proposal (RFP) for selection of Implementing agency for Supply, Installation and Operations & Maintenance of State Wide Surveillance and ITMS project across the State of Gujarat**"), for the Home Department, Government of Gujarat.

AND WHEREAS it has been stipulated in the said Agreement that the Bidder shall furnish a Bank Guarantee ("the Guarantee") from a scheduled bank for the sum specified therein as security for implementing PROJECT.

1. WHEREAS we \_\_\_\_\_ ("the Bank", which expresSion shall be deemed to include it successors and permitted as Signs) have agreed to give the Gujarat Informatics Limited ("GIL") the Guarantee:

THEREFORE the Bank hereby agrees and affirms as follows:

The Bank hereby irrevocably and unconditionally guarantees the payment of all sums due and payable by the Bidder to GIL under the terms of their Agreement dated \_\_\_\_\_. Provided, however, that the maximum liability of the Bank towards GIL under this Guarantee shall not, under any circumstances, exceed \_\_\_\_\_ in aggregate.

2. In pursuance of this Guarantee, the Bank shall, immediately upon the receipt of a written notice from GIL in that behalf and without delay/demur or set off, pay to GIL any and all sums demanded by GIL under the said demand notice, subject to the maximum limits specified in Clause 1 above. A notice from GIL to the Bank shall be sent by Registered Post (Acknowledgement Due) at the following address:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Attention Mr. \_\_\_\_\_.

3. This Guarantee shall come into effect immediately upon execution and shall remain in force for a period of \_\_months from the date of its execution. The Bank shall extend the Guarantee for a further period which may mutually decided by the bidder and GIL.

The liability of the Bank under the terms of this Guarantee shall not, in any manner whatsoever, be modified, discharged, or otherwise affected by:

- Any change or amendment to the terms and conditions of the Contract or the execution of any further Agreements.
- Any breach or non-compliance by the Bidder with any of the terms and conditions of any Agreements/credit arrangement, present or Future, between Bidder and the Bank.

4. The BANK also agrees that GIL at its option shall be entitled to enforce this Guarantee against the Bank as a Principal Debtor, in the first instance without proceeding against the BIDDER and notwithstanding any security or other guarantee that GIL may have in relation to the Bidder's liabilities.
5. The BANK shall not be released of its obligations under these presents by reason of any act of omission or commission on the part of GIL or any other indulgence shown by GIL or by any other matter or thing whatsoever which under law would, but for this provision, have the effect of relieving the BANK.
6. This Guarantee shall be governed by the laws of India and the courts of Gandhinagar shall have jurisdiction in the adjudication of any dispute which may arise hereunder.

Dated this ..... Day of .....,2017

Witness

(Signature)

(Name)

(Official Address)

Dated:

(Signature)

Bank Rubber Stamp

(Name)

Designation with Bank Stamp  
Plus Attorney as per Power of  
Attorney No.

## Format VI- Financial Details of the Bidder

Turnover (In Crore)			Net Worth (In Crore)		
2014 - 2015	2015 – 2016	2016 – 2017	2014 - 2015	2015 – 2016	2016 – 2017

**Note:**

1. Upload the audited financial statement/ audited annual report of the last three financial years.
2. Annual financial turnover during the last three years is \_\_\_\_ Crore (each year) against System Integration and Services. Bidder shall upload a certificate from the statutory auditors.
3. Bidder should have a positive Net worth. In this regard bidder, should upload a certificate from the statutory auditors.

Name:

Designation:

Signature of the Authorized Signatory (with seal):

## Format VII- Bidder’s Experience

**DETAILS OF PAST EXPERIENCE**

S. No.	Client Name & Address	Project Name	Nos. of Access Points commissioned	User Capacity	Contact details (Name, Designation, Phone No., Email ID)
1					
2					
3					
4					
5					

**Note:**

1. Upload the copy of successful work completion/Work in Progress certificates from client, Work Order/ Purchase Order, Self-certificate of completion or work order and phase completion certificate from client etc.
2. Please mention only those projects which meet the eligibility criteria bidder.

Name:

Designation:

Signature of the Authorized Signatory (with seal):

**Format VIII: COMPLIANCE STATEMENT**

Sr. No	Proposed Hardware as per Specification	Make and Model	Quantity	Proposed Technical Specification	Complied / Not Complied	Comments
1						
2						

**Note:**

- 3.) The bidders will have to incorporate any additional hardware or software required for the implementation of the project and achievement of SLAs. Bidders should carry out independent assessment to as to what exact number of hardware might be required.
- 4.) SI should ensure that only one make and model is proposed for one component (for each line item) in Technical Bid

Name:

Designation:

Signature of the Authorized Signatory (with seal):

**Annexure A****List of Locations with No. of cameras**

<b>SR.No</b>	<b>District</b>	<b>Total No. Of Cameras</b>
1	AHWA DANG	31
2	SURAT RURAL	53
3	AMBAJI	30
4	SURENDRANAGAR	204
5	KHEDA - NADIAD	125
6	AMRELI	157
7	BOTAD	68
8	SABARKANTHA	121
9	KUTCH-BHUJ	177
10	ANAND	123
11	TAPI-VYARA	92
12	DEVBHUMI-DWARKA	52
13	NAVSARI	74
14	PORBANDAR	129
15	JAMNAGAR	282
16	GODHRA	121
17	JUNAGADH	229
18	DAHOD	136
19	GIR-SOMNATH	110
20	MEHSANA	112
21	RAJKOT RURAL	160
22	CHHOTA-UEDPUR	29
23	BANASKANTHA	90
24	PATAN	177
25	MAHISAGAR-LUNAWADA	56
26	GANDHINAGAR	196
27	VADODARA RURAL- Karjan	32
28	DAKOR	77
29	AMHMEDABAD RURAL	86
30	ARRAVALI-MODASA	59
31	GANDHIDHAM	255
32	PAVAGADH	46
33	PALITANA (BHAVNAGAR)	47
34	BHARUCH	205
35	NARMADA	63
36	VALSAD	90
37	SURAT CITY	245
38	DWARKA CITY	71
<b>Total</b>		<b>4410</b>



**Annexure B**

**Details of the Existing system**

Sr. No	Description	City Surveillance	CSITMS				City Surveillance	Smart City	City Surveillance
		Surat	Ahmedabad	Vadodara	Gandhinagar	Bhavnagar	Gandhinagar	Morbi	
1	Total Nos of Locations	134	82	10	6	59	37	46	
2	Total No. of Cameras (Fix+ PTZ)	537	226	20	18	155	128	124	
3	ANPR	64	28	0	0	1	48	16	
4	RLVD	1	1	0	0	No	No	No	
5	Project Implementation Year	2013	2015	2015	2015	2015	2016	2016	

**Annexure C**

**Category wise Item details**

<b>Details of the Network and Storage equipments at each Level</b>																	
Sr. No.	Location Categorization	Router			Internet Router			Managed L3 Switch		Managed L2 Switch		Firewall		Storage for Video Feeds	Video Wall 55"		
		Min Throughput	Required Port from Day1	Scalability	Min Throughput	Required Port from Day1	Scalability	Min Throughput	Required Port from Day1	Min Throughput	Required Port from Day1	Min Throughput	Required Port from Day1			Scalability	
1	Command and Control Center	20 Gbps	4X10G	2X10G	5 Gbps	4X1G	4X1G	25 Gbps	16 Port: 8X10G+8X1G	24 Port: 4X10G+20X1G	25 Gbps	24 Port: 4X10G+20X1G	20 Gbps	4X10G+2X1G	2X10G+2X1G	500TB	1Nos. (4 X3 matrix)
2	District Category 1	5 Gbps	5X1G	2X1G	-	-	7 Gbps	16 Port: 6X10G+10X1G	48 Port: 4X10G+44X1G	7 Gbps	7 Gbps	48 Port: 4X10G+44X1G	7 Gbps	8X10G+6X1G	2X10G+2X1G	400TB	1Nos. (2 X2 Matrix)
3	District Category 2	10 Gbps	3X10G	2X10G	-	-	10 Gbps	16 Port: 6X10G+10X1G	48 Port: 4X10G+44X1G	10 Gbps	10 Gbps	48 Port: 4X10G+44X1G	12 Gbps	4X10G+6X1G	2X10G+2X1G	800TB	1Nos. (2 X3 Matrix)
4	District Category 3	15 Gbps	6X10G	2X10G	-	-	15 Gbps	24 Port: 8X10G+8X1G	48 Port: 6X10G+42X1G	15 Gbps	15 Gbps	48 Port: 6X10G+42X1G	15 Gbps	8X10G+6X1G	2X10G+2X1G	1PB	1Nos. (3 X3 Matrix)
5	City Category 1	1 Gbps	3X1G	2X1G	-	-	2 Gbps	16 Port: 16X1G	16 Port: 16X1G	2 Gbps	2 Gbps	16 Port: 16X1G	-	-	-	-	1Nos. (2 X1 Matrix)
6	City Category 2	2 Gbps	6X1G	2X1G	-	-	2 Gbps	16 Port: 16X1G	16 Port: 16X1G	2 Gbps	2 Gbps	16 Port: 16X1G	-	-	-	-	1Nos. (2 X2 Matrix)