



Request for Proposal
for
Selection of Master System Integrator for
Jalandhar Integrated Smart Solutions

RFP No. 04/JSCL/2018

Volume II: Scope of Work

Jalandhar Smart City Limited (JSCL) office , Jalandhar

Disclaimer

This report is based on our assessment of data & information collected from or provided by various government departments, officials, websites as on date and our expertise & past experience and is accordingly, given for the specific purpose of internal use by Jalandhar Smart city Limited. Any observation or data if not entirely correct or accurate, should be communicated to us immediately, as the inaccuracy or incompleteness could have a material impact on our conclusions. We have taken reasonable steps to ensure that the data obtained from reliable sources and this report is accurate and authoritative in all respects however, there can be no assurance that the authorities or regulators may not take a position contrary to our conclusions.

This report is for sole information of Jalandhar Smart City Limited and we accept no responsibility to any other party.

Table of Contents

1. SCOPE OF WORK	7
2. PROJECT ACTIVITIES	99
3. GENERAL REQUIREMENTS	433
4.1 Jalandhar Integrated Command Control Centre (JICCC), DC & DR	609
4.2 CCTV City Surveillance	2108
4.3 Intelligent Traffic Management System	25452
4.4 Variable Messaging System (VaMS)	3139
4.5 Disaster Management	3217
4.6 Jalandhar Environmental Monitoring System (JEMS)	3228
4.7 Integration with NERS (Mohali, Punjab)	32925
4.8 E-Governance	3351
4.9 Geographic Information System (GIS)	3351
4.10 Helpdesk	3439
5 Annexure - Project Implementation Timelines, Deliverables and Payment Schedule	35450
6 Annexure –Bill of Materials	35854

Definitions/Acronyms

Sl. No	Term/Acronyms	Description
1.	AAA	Authentication, authorization, and accounting
2.	ABD	Area Base Development
3.	ANPR	Automated Number Plate Recognition
4.	AVLS	Automated Vehicle Locator System
5.	BOM	Bill of Material
6.	JICCC	Jalandhar Integrated Command and Control Centre
7.	CCTNS	Crime and Criminal Tracking Network & Systems
8.	CCTV	Closed Circuit Television
9.	COP	City Operation Platform
10.	COP	Common Operations Platform
11.	DC	Data Centre
12.	DNS	Domain Name Server
13.	DR	Disaster Recovery
14.	FRS	Functional Requirement Specifications
15.	GIS	Geographical Information System
16.	GoP	Government of Punjab
17.	GPRS	General Packet Radio Service
18.	GPS	Global Positioning System
19.	GSM	Global Systems for Mobile Communications
20.	GUI	Graphical User Interface
21.	ICT	Information and Communication Technology
22.	IDS	Intrusion Detection System
23.	IP	Internet Protocol
24.	IPS	Intrusion Prevention System
25.	ITIL	Information Technology Infrastructure Library
26.	JSCL	Jalandhar Smart City Limited
27.	LAN	Local Area Network
28.	LED	Light Emitting Diode
29.	MCJ	Municipal Corporation Jalandhar
30.	O&M	Operations & Maintenance

Sl. No	Term/Acronyms	Description
31.	OEM	Original Equipment Manufacturer
32.	OFC	Optical Fibre Cable
33.	OS	Operating Systems
34.	OTP	One Time Password
35.	PA System	Public Address System
36.	PDU's	Power Distribution Units
37.	PoE/ PoE+	Power over Ethernet
38.	PoP	Points of Presence
39.	PTZ	Pan Tilt Zoom
40.	QR Code	Quick Response Code
41.	RF	Radio Frequency
42.	RFID	Radio Frequency Identification
43.	RFP	Request for Proposal
44.	RLVD	Red Light Violation Detection
45.	RoW	Right of Way
46.	RPO	Recovery Point Objective
47.	RTO	Recovery Time Objective
48.	MSI	Master System Integrator
49.	SLA	Service Level Agreement
50.	SNMP	Simple Network Management Protocol
51.	SMPS	Switched Mode Power Supply
52.	SOP	Standard Operating Procedure
53.	UPS	Uninterruptible Power Supply
54.	VaMS	Variable Message System
55.	VLAN	Virtual Local Area Network
56.	VMS	Video Management Software/System
57.	WAN	Wide Area Network
58.	ATCS	Automated Traffic Control System

Preamble – Jalandhar

Jalandhar was the capital of Punjab since India's independence in 1947 until Chandigarh was built in 1953. Jalandhar is an ancient city and has an urban population of almost a million, and another million live in rural areas. On the Grand Trunk Road, it is a major rail and road junction and is 144 km northwest of the state capital, Chandigarh. The city was known as Jullundur in British India.

Jalandhar is the world's biggest manufacturer of leather tool pouches and aprons with major American and European customers. Jalandhar is also famous for its surgical tool industry. A place called Basti Sheikh has got many cottage projects. Jalandhar also has the biggest printing industry in India. Major publishing and advertising companies have their main offices in Jalandhar.

A few outlined demographics of Jalandhar are:

1. The popular spiritual places in Jalandhar include Baba Dasji Gurudwara, Tulsi Mandir, Devi Talab Mandir, Geeta Mandir and Gurudwara Chhevin Padshahi
2. Punjab Technical University (PTU) is one of the most reputed educational field.
3. Climate: Jalandhar city has a humid subtropical climate with cool winters and long, hot summers.
4. Population: Jalandhar city had a population of 8.62 lakhs;
5. Area: 2632 km²; Elevation: 228 m (748.03 ft); Literacy: 82.4%.

Jalandhar is governed by a number of bodies, the most important being the Municipal Corporation Jalandhar (MCJ) which is responsible for the master planning of the city.

Jalandhar Smart City Limited (JSCL)

The Jalandhar Smart City Limited (JSCL) is the Special Purpose Vehicle (SPV) constituted as per the directives of MoHUA, Govt. of India for executing SMART CITY MISSION (SCM) in Jalandhar.

JSCL is led by the CEO Jalandhar Smart City and works closely with the Municipal Corporation of Jalandhar (MCJ) and other nodal offices like Police, Fire etc. with the objective to achieve success in the implementation of Smart City Mission for Jalandhar.

JSCL has been established under the Companies Act, 2013 of the Ministry of Corporate Affairs, Government of India. It is supported by PMC, Authority and the implementing agency for the implementation of the mission.

Vision Statement for Jalandhar Smart City and Associated Objectives

Jalandhar: The Leading Sports and Manufacturing hub in Asia” The world of sports is a growing industry in India. A thriving sports sector has significant socio-economic impact, as it is instrumental in improving the physical health and mental agility of human resources, and in promoting unity and national pride. Sports as an industry have contributed 1%- 5% of the GDP of various countries. Manufacturing is the foundation of a strong economy. The most successful countries have a strong industrial and manufacturing presence underpinning the economic growth. Manufacturing has the potential to help take many residents, currently living in slums, above the poverty line by providing better paid and higher skilled jobs, goal highlighted in Make in India a successful mission. Jalandhar has the opportunity to build upon its existing sports and manufacturing base to create sustainable jobs, increase productivity and drive innovation. The city would benefit from taking a strategic approach that will focus on the sports and manufacturing sector, including:

- Becoming a leading hub for sports goods globally not just in manufacturing but also in research and development in terms of production methods and new cutting-edge sporting goods.
- Focusing on the potential of Small and Medium Enterprises ensuring they are ready to up-skill and expand from their current low-tech base to ensure their good search national and global consumers

In order to develop Jalandhar as envisaged and make it more liveable and sustainable, the strategic blue print for next 5-10 entails the following

1. Promote economic growth of the city by creating state of the art sports infrastructure that aggregates the youth and attracts national/international events, exhibitions, leagues & tournaments converging with the country's sports ecosystem
2. To create public & recreational spaces for the benefit of the city's residents which can also host cultural events.
3. Investing in public transport and traffic management. This will increase accessibility, reduce congestion, promote walkability and ensure better parking provision leading to higher productivity.
4. Upgrading the city's poor public realm urban environment. Currently, a lack of safe and inclusive spaces means that citizens cannot engage in active and social lifestyle.
5. The city's aging physical infrastructure needs to be upgraded to cater for an increased population.
6. Improving urban governance by introducing smart technologies/ICT solutions that help bring systemic efficiency in infrastructure service provision and improved two-way communication.

1. SCOPE OF WORK

Overview

The Jalandhar Smart City Limited (JSCL) intends to select a Master System Integrator (MSI) who will be responsible for the 'Design, Development, Implementation and Maintenance of the Jalandhar Smart City ICT Solutions' for a period of at least three (4) years, post the Go-Live date of the Overall Solution, on a turnkey basis. Under the Smart City initiative, it is envisaged to establish a Jalandhar Integrated Command & Control Centre (JICCC), Data centre, Disaster Recovery and connect Smart elements in real time at the Jalandhar City, which shall be the single & dedicated place for integrating, implementing, monitoring, controlling & commanding all City Wide Smart ICT for line departments.

The Overall Scope of Work for the MSI is to provide an end-to-end ICT Solutions, which shall cater to the following primary components:

1. Jalandhar Integrated Command Control Centre (JICCC)
2. Data Centre & Disaster Recovery (DC & DR)
3. City Surveillance System & Intelligent Traffic Management System (JITMS)
4. Helpdesk
5. Integration of ICCC with NERS
6. Disaster Management
7. Jalandhar Environmental Monitoring System (JEMS)
8. Body cameras
9. e-Governance
10. GIS Maps real time integration with Smart City Applications
11. Network Backbone

The other applications that support the Management and Operations in infrastructure are Unified Communications, Integrated dashboard, Video Wall & Controller System, Operator work station, Standard Operating Procedure Tools (SOP), Security Management, Intrusion Detection, Antivirus Management, Remote Device Management, Internet Connectivity, IT Service Management (ITSM), Building Management System (BMS)

It should be noted that the subsequent sections of this document detail out the expectations from the overall ICT Solution with respect to the above components. The activities defined /described/

discussed/ mentioned within this document are indicative in nature and may/may not be exhaustive. The MSI is expected to perform an independent & in-depth analysis of any additional work(s) that may be required to be carried out to fulfil the requirements for the Overall Jalandhar Smart City ICT Solutions and duly factor those in while preparing a response to this RFP. Ex: GIS Layers & Integration of applications. The MSI is advised to carry out detailed surveys prior to submission of the RFP response to ensure that the Bidders response caters to the complete solution, for all component requirements in order to finalize infrastructure, network bandwidth, operational & administrative challenges, etc.

2. PROJECT ACTIVITIES

Overview of Deliverables:

While this RFP lists out primary ICT objectives for catering to immediate pressing needs, keeping in view the long term scalability and sustainability of the ICT Solutions, the Bidders are encouraged to propose the State-of-Art, cutting edge ICT solutions to revive & revamp the Historic & Heritage City of Jalandhar using Hi-Tech solutions.

The MSI shall be responsible for carrying out the following activities:

- A. Project Mobilization, Project Planning & Management/ Maintenance Management
- B. Survey and Detailed Design of all Smart Solutions Components
- C. Prototype Acceptance and Factory Acceptance Testing
- D. Hardware Supply and Installation Stage
- E. Software Development
- F. System Study, Design, Development, Integration, Testing and Certification
- G. System Integration
- H. Testing
- I. Third Party Acceptance Testing, Audit and Certification
- J. Capacity building & Training
- K. Change Management
- L. Final Deployment and Documentation
- M. Operational System Acceptance
- N. Comprehensive Maintenance for System and Services
- O. Support Staff Required

A. Project Mobilization, Project Planning & Management/ Maintenance Management

MSI shall mobilize & deploy the proposed Project Manager on the date of signing of the contract agreement. The deployment of the other implementation team should be completed within 15 days from the date of contract agreement. MSI shall be responsible for end to end project management for the Implementation and Operations & Maintenance of the Jalandhar Smart City ICT components. MSI shall deploy a competent team of experts for Project Management which may include a Project Director, Project Manager along with Solution and Network Architect. The Project Director shall be the single

point of contact that shall assume overall responsibility of the Project and ensure end to end working of the project. The Project Manager shall be stationed full-time in Jalandhar during the Implementation Phase. He shall function as the primary channel of communication for all Authority requirements to the implementation team. In case of any absence of the Project Manager, the MSI shall ensure that an alternate Project Manager (as approved by the Authority or its representative) shall be provided during the absence period. MSI shall be responsible for preparing a master schedule of work which shall highlight implementation plan for all the Project Milestones. The schedule shall identify the manufacture, delivery, installation, integration of equipment (Software and Hardware), training programs, test procedures, delivery of documentation and the respective solutions. The schedule shall include Authority and any third party responsibilities along with the activities in the timeline. MSI shall conduct bi-weekly meetings between the Authority and the 'key personnel' to discuss project progress & implementation in Jalandhar. All key personnel associated with the project shall also be available for meetings whenever asked by the Authority or its representative. MSI shall also be responsible for effective risk and issue management and escalation procedures along with matrix as part of project management. MSI shall identify, analyze, and evaluate the project risks and shall develop cost effective strategies and action plan for mitigation of risks. As part of the Project MSI shall monitor, report and update risk management plans and shall be discussed during project meetings. MSI shall prepare minutes of every meeting which takes place in the absence of PMC and submit to Authority or its representative for tracking of the Project. MSI shall propose a suitable progress reporting mechanism for the project duration.

MSI will deploy Enterprise Project Management Tool which should cater to effective project management, configuration management, issue and risk management, escalation procedure and matrix document repository etc. shall be factored in the proposal submitted by MSI. Based on progress reports, MSI shall also accordingly update the master schedule of work on a continuous basis during the period of the contract. Project Management plan shall be submitted to JSCL before commencing the work. The Authority's representative will have at least 15 days to review and comment on every deliverable. The practice of submissions for all deliverables will be at least one hard copies and share all the documents with PMC and JSCL stake holders. All deliveries should be approved by PMC (Project Management Consultant) before submitting to Authority.

B. Survey and Detailed Design of all Smart Solutions Components

MSI shall survey the site to validate the conditions provided as part of the Bid document. MSI shall conduct end-to-end survey of the site area and based on the observations asses and validate the present

conditions, implementation approach and methodology, project challenges and mitigations and other project critical information. During the survey stage itself, MSI shall mobilize its entire staff and fully acquaint them with the site conditions. It is MSI's responsibilities to periodically survey the site and be updated on the conditions during the course of the contract.

During the design stage, MSI is also expected to:

- Conduct Workshops with different stakeholders for capturing business requirements, creating awareness of best practices, communicating the changes, building consensus on process design etc. These needs to be organized at different intervals and in different places throughout the duration of the projects as needed.
- Stake holder consultation - Other than the workshops with those stake holders, PMC & JSCL identified staff will provide critical inputs, reviews, suggestions, process description etc.
- Review sessions with different stake holders for signing off the deliverables, walking through the deliverables for facilitating quick understanding.

The MSI shall be responsible for the detailed design of the Jalandhar smart city solutions. MSI shall discuss in detail with the Authority or its representatives the detailed design of the Jalandhar Smart City Solutions and fine tune any requirements. It is the MSI's responsibility to satisfy the operational requirements of the Authority and adopt industry best practices for implementation during the design stage itself. Based on the survey observation, analysis and discussion with the Authority, the MSI shall submit a Detailed Design Report. The IT' deliverables would include following details and not limited to JICCC design/layout, System Architecture, Data centre Architecture, Network Architecture, Application Architecture, Security Architecture, Routing & Switching, Integration, Operational procedures etc.

The detailed design report shall include end-to-end design validation for the project including any project understanding, analysis, detailed design, integration plan, and construction drawings. Complete set of design and construction drawing including method of installation as applicable shall also be included in the Detailed Project Report. Construction details shall accurately reflect actual job conditions.

All technical data sheets of the products may be submitted ahead of time by the MSI. It is MSI's responsibility to get all technical data sheets approved by the Authority or its representative to meet the overall project schedule.

Design and Construction drawings shall include the following at a minimum for drawings for all the elements as part of holistic solution:

- Overall design
- Cable requirements, routing and location (as applicable)
- Design of IP address and schematic architecture diagram
- Typical mounting details
- Single Line Diagrams (SLDs)
- Splicing diagrams
- Wiring diagrams with diagram
- 3D layouts and renderings
- Any other layouts
- Any other requirement to meet the requirements of the RFP for troubleshooting and maintenance

All drawings shall be updated/revised to “as-built” conditions when installation is complete. Design submissions shall be based on project requirements and shall include as applicable, but not limited to, the following:

- Complete listing of specifications to be used along with detailed technical data sheet
- Detailed engineering drawings
- Shop drawings including product data sheets
- Revisions to original design submissions.

MSI will create requirement analysis documents for various components of the solution. This includes System Requirements Specification (SRS) and Functional Requirements Specification (FRS) documentation. The MSI shall be responsible for documenting any existing/planned ‘processes’ of the Authority as part of these deliverables.

C. Prototype Acceptance and Factory Acceptance Testing

After approval of the technical data sheets by the Authority or its representative, MSI shall submit the prototype of all the material presented in the Detailed Design Report for its review and approval. Note

that it shall be MSI's responsibility to get the prototypes approved in due course of time without affecting the overall schedule of completion of works.

Material provided as part of the Project shall undergo Prototype Acceptance Test (PAT) and Factory Acceptance Test (FAT) as per Project Plan. Details regarding the PAT and FAT are presented in Testing Section of the Scope of Work. MSI shall also present to the Authority and its representatives the test results for PAT and FAT in the form of Test Result Documentation presented in the Testing section. The Authority at its own discretion shall visit any FAT site. MSI shall be responsible for organizing all logistics required for this site visit. For all the software components, MSI shall also propose prototype of solution components in this phase and get the required approvals.

D. Hardware Supply and Installation Stage

MSI shall be responsible for the supply and installation of all components as part of the Jalandhar Smart City solutions to meet the Technical, Functional, Business and Performance requirements of this RFP. No deviations from these requirements shall be acceptable by the Authority. Any additional hardware or software component required to meet the technical and performance requirement of the project and not specified as part of this document but required to meet the overall requirements of the project shall be factored in as part of the Bid, and provided by the MSI. MSI shall deliver the project, install and handle the equipment in accordance with manufacturer's requirements. Installation process of the MSI shall be flexible and shall accommodate Authority's requirements without affecting the schedule as specified in the RFP.

MSI shall be responsible for all supply, storage and handling of the material provided as part of the bid document. The OEM proposed for the IT infrastructure shall be in line with the national security policy (as applicable).

If there is removal/change of any existing material during installation process and belongs to the Authority, the material shall be handed-over to the Authority. MSI shall also be responsible for reinstating any site in the project limits at no additional cost to the Authority. It shall be the MSI's responsibility to supply and install all hardware in compliance with the requirements of the RFP. Since this is a turnkey contract, MSI shall be responsible for all implementation works on the project including any civil, structural, electrical, etc. works required to meet the requirements of the project. All power conversions necessary to operate the equipment shall be under the scope of MSI. The Authority shall only provide raw power for all the equipment. In case of, there is NO power or insufficient power as per

the requirement of the equipment, it may be considered that the new power supply connection has to be applied by MSI on the name of the Authority and Authority will provide all necessary help to the Authority in procuring the raw power on actuals.

E. Software Development

MSI shall be responsible for development and deployment of all software to meet the requirements of the project. It is preferred that MSI will use a world class Commercially off the Shelf (COTS) or widely used software packages. However, some of the modules may require bespoke development. MSI shall be fully responsible for developing and implementing all software required for the project. The development model should be Agile. This software shall be developed based on the approved software and functional requirements specifications. The technology platform chosen for all software shall be based on industry standards based and shall be secure. Migration of data shall be the responsibility of the MSI. MSI is required to take the source data in the format which is available. Subsequently, MSI is required to take complete ownership of data migration and also develop a detailed plan for data migration. MSI will create SRS for application development and get approval from JSCL for UX design before commencing development and also periodic review meetings should be scheduled for review of application and progress of the project.

All licenses for the software shall be perpetual along with Software Assurance (SA) during the course of the contract. The MSI shall ensure that full support from the OEM's is provided during the course of the contract. All OEMS should give the Manufacturer's Authorization Form (MAFs) and other supporting documents. MSI shall be responsible to provide any upgrades, patches, fixes to the software during the course of the contract at no additional cost to the Authority.

F. System Study, Design, Development, Integration, Testing and Certification

MSI would be responsible for development, adding functionality/Customizing over and above the applications (COTS product) or any bespoke software (If required) based on the unique requirements of the Authority (JSCL/MCJ/Other Stakeholders). For the additional functionality that the Authority wants to be added, the MSI shall carry out a detailed systems study to refine the Functional Requirements Specifications provided in this RFP and formulate the System Requirements Specifications (SRS). The study should also include different integration points of JICCC with external agencies as per Authority's requirement. The MSI should also prepare a detailed document on the implementation of the customized or developed product with respect to configuration, customization and extension as per the requirement

of Authority. The MSI would also prepare a change/reference document based on changes or deviations from the base version of the application (COTS product).

Overall holistic operations shall be ensured by MSI. The MSI should also prepare a detailed document on the implementation of the customized or developed product with respect to configuration, customization and extension as per the requirement of Authority. The MSI would also prepare a change/reference document based on changes or deviations from the base version of the application (COTS product).

The MSI will also be responsible for:

- Conducting Site preparation study for hardware, networking and office infrastructure
- Preparation of System Requirements Specifications (SRS) for additional functionalities and different integration points with External Agencies.
- Preparation of implementation document with respect to Configuration, Customization and extensions as per the requirement of Authority.
- Preparation of the Solution Design.
- Solution Development and/or Customization and/or Configuration and/or Extension as required.
- Development of reports.
- Formulation of test plans and test cases for additional functionalities and different integrations with external agencies.
- Preparation of Change/Reference document which will include all the changes or deviations from the base version of the product.
- Testing of the configured solution and additional functionalities.

Enhancements of functions / additions of new modules / integration requirements to various interfaces (as and when they happen) shall also be incorporated in the SRS and shall form the scope of work for the MSI.

Creation of Test Plans: - Once the SRS is approved and design is started, the MSI would prepare all necessary Test Plans (including test cases), i.e., plans for Unit Testing, Integration and System Testing and User Acceptance Testing. Test cases for UAT would be developed in collaboration with domain experts identified by the Authority. The Test Plans also include planning for the testing any integration with 3rd party COTS solutions, any external agencies. The Test Plans should also specify any assistance required from the Authority and should be followed upon by the MSI. The MSI

should have the Test Plans reviewed and approved by Authority. The Authority will sign off on the test plans.

High Level Design (HLD): - Once the SRS is approved, the MSI would complete the HLD and all HLD documents of the additional functionalities, integration with external agencies upon the approved SRS. The MSI would prepare the HLD and have it reviewed and approved by the Authority. The Authority will sign off on the HLD documents on the advice of Authority.

Detailed (Low Level) Design (LLD): - The LLD would interpret the approved HLD to help application development and would include detailed service descriptions and specifications, application logic (including pseudo code) and UI design (screen design and navigation). The preparation of test cases will also be completed during this stage. The MSI would have the design documents reviewed and approved by the AUTHORITY. The Authority will sign off on the LLD documents.

Application Development and Unit Testing: - The MSI would develop the application in accordance with the approved requirements specifications and design specifications and according to the approved Project Plan; and carry out the Unit Testing of the application in accordance with the approved test plans. The MSI would also implement the changes proposed in the Change/Reference document and carry out a thorough regression testing for the functionality. The user acceptance testing and fine-tuning of the application would be at Authority's location.

Regression, Integration, System and Functional Testing: - After successful unit testing of all components, the MSI would conduct full-fledged integration testing, system testing and functional testing in accordance with the approved Test Plans for the configured/customized product, additional functionalities and also integration with external agencies. This would include exhaustive testing including functional testing, performance testing (including load and stress), scalability testing and security testing. Functional testing will be led by the MSI's experts. A thorough regression testing should be conducted for those functionalities identified in Change/Reference document to provide a general assurance that no additional errors have cropped up in the process of addressing the customizations and/or Extensions. Making all necessary arrangements for testing including the preparation of test data, scripts if necessary and setup of test environment (across multiple platforms) shall be the responsibility of the MSI. The MSI along with Authority should take the responsibility in coordinating with Authority and other stakeholders for a smooth integration.

Test Reports: - The MSI shall create test reports from testing activities and submit to Authority for validation.

Test Data Preparation: - The MSI shall prepare the required test data and get it vetted by Authority. The test data shall be comprehensive and address all scenarios identified in the test cases. The MSI should also prepare the test data for all required integrations with external agencies.

User Acceptance Testing (UAT): - Test Plans for UAT would be prepared by the MSI in collaboration with the Authority and his nominated domain experts. The MSI will plan all aspects of UAT (including the preparation of test data) and obtain required assistance from Authority to ensure its success. Authority will assemble representatives from different user groups based on inputs from the MSI and would facilitate UAT. The MSI would make the necessary changes to the application to ensure that the customized/developed product successfully goes through UAT.

G. System Integration

MSI shall be responsible for the integration of all hardware and software supplied as part of this Project as per the technical and performance requirements of this bid document. The system integration scope also includes integration of the project components with the components provided by others as per the details of the RFP.

In case the integration of any of the systems is not as per the requirements specified in the bid document, MSI shall be responsible to provide any upgrades required to meet the integration requirements at no additional cost to the Authority unless otherwise agreed by the Authority. It shall be the responsibility of MSI to take approval of the Authority for the Integration of the overall system as per the bid document. Post systems integration, the Authority shall review and approve the overall performance of the integrated system as per the requirements of the bid document. MSI shall be responsible for fixing any requirements that are not found in compliance with the original bid requirements and approved detailed design at no additional cost to the Authority.

MSI shall carry out SMS Gateway Integration with the JICCC to be provided by Centre for e-Governance (CeG), Government of Punjab to send mass SMSs to groups/individuals, which can be either manual or system generated.

H. Testing

All materials, equipment, systems, manufacturing or configuration processes, or other items to be provided under the Contract shall be inspected and tested in accordance with the requirements specified in the RFP and will be subject to Authority or its representative's approval. The testing shall include any existing civil infrastructure equipment or materials to be taken over by the MSI. Approvals or passing of any inspection by the Authority shall not, however, prejudice the right of the Authority or its representative to reject the material if it does not comply with the specification or requirements of the RFP when erected or give complete satisfaction in service. The MSI shall design and successfully complete tests to demonstrate that all equipment, materials and systems furnished and installed function in the manner intended and in full compliance with the requirements outlined in the RFP and the approved detailed design of the MSI.

All tests shall be subject to inspection or witnessing of tests by the Authority or its representative. Inspection or witnessing of tests may be waived at the sole discretion of the Authority or their representative, subject to the MSI furnishing the Authority or their representative with properly completed test certificates in accordance with the requirements of the RFP. Failure of the Authority or their representative to witness any test shall not relieve the MSI of the obligation to meet the requirements of the Contract. MSI shall submit an Acceptance Test Procedures document (ATP), for Authority's approval prior to undertaking any testing.

The ATP shall clearly address:

- Type of testing and device to be tested
- How each testable specification requirement will be demonstrated, including the test environment and set-up, specific functionality to be tested, method for performing the test and quality assurance procedures;
- The results that will constitute success for each test
- Timing of test within the overall Contract schedule
- The location for testing
- Personnel required to conduct the test

- Approximate time required to execute the test or set of tests
- Responsibilities of both the MSI and Authority's representatives during each test; and
- A cross-reference to which Contract requirements from the Compliance Matrix (to be developed by the MSI) are being addressed by each test procedure

The ATP shall include an updated Compliance Matrix to include the test relevant stage at which each contract requirement will be demonstrated; and a cross-reference to the test procedure(s) that serve to address each contract requirement. The Compliance Matrix shall be used as a “punch list” to track which requirements have not yet been demonstrated at each stage of testing. A requirement classified as having been “demonstrated” during a certain ATP stage can be subsequently redefined as having been “not demonstrated” if compliance issues emerge prior to System Acceptance. ATP shall be submitted to Authority at least three (3) weeks in advance of any intended testing.

The equipment shall be inspected for standards of construction and electrical and mechanical safety. MSI will take appropriate certificate from the supplier. Test results shall be recorded for all tests conducted under this Contract. The MSI shall make test results available to Authority or their designate for review immediately after completion of the tests. ATP for each test shall be collated, bound and delivered as part of the close-out documentation requirements specified herein. ATP submission shall include a hard copy of the originally marked test results and a neatly typed summary. One (1) hard copy and one (1) electronic copy shall be provided

ATP shall incorporate the following distinct stages for each deployed stage:

- **System Integration Testing (SIT):** The MSI is responsible for the proper and harmonious operation of all subsystems installed under this Contract. Where connections of the new systems to existing subsystems or equipment supplied by others are required, the MSI is responsible for connection of equipment specified in the Contract and for initial system integration tests. Such a test will verify the full functionality of each subsystem as they are interconnected. This will require testing to be coordinated by the MSI with the Authority or their designate. This work will be carried out under the direction of the Authority or their designate.

The MSI shall:

- Complete all equipment and subsystem tests required in the Contract

- Test each subsystem independently on the communications subsystem
- Add subsystems one at a time and monitor the overall performance
- Fail safe testing of all subsystems one at the time while monitoring overall systems performance

A SIT certificate will be issued when all system tests have been completed satisfactorily, and the MSI has supplied a full set of Test Certificates and a Test Certificate for the complete system, together with final copies of all Operating and Maintenance Documentation for the System.

Stress and Load Testing: Comprehensive stress and load testing of e-Governance and Smart elements applications shall be conducted to demonstrate robustness and reliability of the system where necessary like Surveillance, Vehicle Tracking for SWM, Mobile App users etc.

Security Testing (including penetration and vulnerability test): Security test shall be conducted to demonstrate security requirements at network layer and software applications. Components shall pass vulnerability and penetration testing for rollout of each phase. Components shall also pass web application security testing for portal, Mobile App, and other systems. Security testing shall be carried out for exact same environment/architecture that shall be set up for go-live. Penetration test shall be carried out periodically and vulnerability analysis shall be carried half-yearly during maintenance phase. For all applications hosted on-cloud or hosted on premises, the security testing shall be a mandatory requirement.

System Acceptance Tests (SAT): SAT shall be conducted after the entire system has been installed, integrated and commissioned. Deficiencies, if any shall be rectified before the initiation of Burn-in Test. SAT shall be conducted on full system completion only to determine if the system functional and technical requirements as specified in the bidding documents are meet. SAT shall be witnessed by Authority's representatives. Data migration, if any will be carried out by ST prior to commencement of this stage. SAT shall also include any performance and load testing for the software applications.

Operational Acceptance Test: shall be conducted after successful SAT and Burn-in tests. Continuous fault free running of the System shall be tested. Post the completion of Operational Acceptance Test, System shall be considered for Operational System Acceptance and Defect Liability

Period (DLP) shall commence. Operational Acceptance Test shall include the following as a minimum:

- Completion of all activities and fulfilment of all business, functional and technical requirements listed in RFP
- Scrutiny of all inspection reports, audit findings, Contracts, licensing agreements etc.

Authority may authorize the MSI to proceed to the next testing stage with certain deficiencies not yet resolved.

The MSI shall provide written notice to Authority at least five days in advance of any testing, indicating the specific tests to be completed as well as the date, time and location. The MSI shall be required to reschedule testing if Authority witnessing representatives cannot be present or if other circumstances prevent testing from taking place.

MSI shall provide written Test Results Documentation (TRD) within one week of completing each stage of testing. The TRD shall document the results of each ATP procedure and provide an updated Compliance Matrix that indicates which contract requirements have been demonstrated. The TRD must be approved before Authority will grant System Acceptance. A sample format for the TRD is provided below:

Item #	Date		
Item Description	Tester		
Test			
Test Setup:			
Clause	Test Procedure	Expected Results	Actual Results
Witnessed: (This Does Not Constitute Approval) Reviewed and Approved:			

MSI shall be responsible to carry out all the testing as per the satisfaction of the Authority and its representatives. All the costs those are associated with any testing are to be borne by the MSI including the costs of travel and accommodation of the Authority or its representatives from their home locations in their cost bid. In the interest of the MSI maximum of three (3) people shall be nominated by the Authority to attend any such testing wherever it is carried out. In case of failure of any testing, the failure component shall be repaired and the test shall be rerun. If a component has been modified as a result of failure, that component shall be replaced in all like units and the test shall be rerun for each unit.

MSI shall provide the Authority with a copy of the manufacturer's quality assurance procedures for information. Documentation certifying the showing that each item supplied has passed factory inspection shall also be submitted by the MSI.

I. Third Party Acceptance Testing, Audit and Certification

The primary goal of Acceptance Testing, Audit & Certification is to ensure that the system meets requirements, standards, and specifications as set out in this RFP and as needed to achieve the desired outcomes. The basic approach for this will be ensuring that the following are associated with clear and quantifiable metrics for accountability:

- Functional requirements
- Test cases and Requirements Mapping
- Infrastructure Compliance Review
- Availability of Services in the defined locations
- Performance and Scalability
- Security / Digital Signatures
- Manageability and Interoperability
- SLA Reporting System
- Project Documentation
- Data Quality Review

As part of Acceptance testing, audit and certification, performed through a third party agency, JSCL shall review all aspects of project development and implementation covering software, hardware and networking including the processes relating to the design of solution architecture, design of systems and sub-systems, coding, testing, business process description, documentation, version control, change management, security, service oriented architecture, performance in relation to defined requirements, interoperability, scalability, availability and compliance with all the technical and functional requirements of the RFP and the agreement. Here, it is important to mention that there may be two agencies selected, one for audit & certification of security and control aspect of the system and the other for audit & certification of overall application S/w. JSCL will establish appropriate processes for notifying the MSI of any deviations from defined requirements at the earliest instance after noticing the same to enable the MSI to take corrective action. Such an involvement of the Acceptance Testing & Certification agencies (STQC/CERT-IN Empanelled Agency), nominated/appointed by MSI with prior approval of JSCL, will not, however, absolve the MSI of the fundamental responsibility of designing, developing, installing, testing and commissioning the various components of the project to deliver the services in perfect conformity with the SLAs.

Following discusses the acceptance criteria to be adopted for system as mentioned above:

1. **Functional Requirements:** - The system developed/customized by MSI shall be reviewed and verified by the agency against the Functional Requirements signed-off between JSCL/Concerned Department Authority and MSI. Any gaps, identified as severe or critical in nature, shall be addressed by MSI immediately prior to the deployment of the system in production. One of the key inputs for this testing shall be the traceability matrix to be developed by the MSI from system. Apart from Traceability Matrix, agency may develop its own testing plans for validation of compliance of system against the defined requirements. The acceptance testing w.r.t. the functional requirements shall be performed by both independent third party agency (external audit) as well as the select internal department users (i.e. User Acceptance Testing).
2. **Infrastructure Compliance Review:** - Third party agency shall perform the Infrastructure Compliance Review to verify the conformity of the Infrastructure supplied by the MSI against the requirements and specifications provided in the RFP and/or as proposed in the proposal submitted by MSI. Compliance review shall not absolve MSI from ensuring that proposed infrastructure meets the SLA requirements.
- **Security Review:** - The software developed/customized for system shall be audited by the agency from a security & controls perspective. Such audit shall also include the IT infrastructure and network deployed for system. Following are the broad activities to be performed by the Agency as part of Security Review. The security review shall subject the system for the following activities:
 - a) Audit of Network, Server and Application security mechanisms
 - b) Assessment of authentication mechanism provided in the application /components/modules
 - c) Assessment of data encryption mechanisms implemented for the solution
 - d) Assessment of data access privileges, retention periods and archival mechanisms
 - e) Server and Application security features incorporated etc.
3. **Performance:** - Performance is another key requirement for system and agency shall review the performance of the deployed solution against certain key parameters defined in SLA described in this RFP and/or agreement between JSCL and MSI. Such parameters include request-response time,

work-flow processing time, concurrent sessions supported by the system, Time for recovery from failure, Disaster Recovery drill etc. The performance review also includes verification of scalability provisioned in the system for catering to the requirements of application volume growth in future.

- a) The MSI must provide System and Database Performance System for all servers in the Data centre
 - b) The MSI must provision for End-User response time monitoring and transaction based deep-dive analysis for Web based applications.
 - c) The MSI must provision for Integrated Performance Management System for Monitoring Networks, Systems & Databases.
 - d) The MSI must provide a Traffic Analysis and Reporting System for deep-dive diagnostics.
4. **Availability:** - The system should be designed to remove all single point failures. Appropriate redundancy shall be built into all the critical components to provide the ability to recover from failures. The agency shall perform various tests including network, server, security, DC/DR fail-over tests to verify the availability of the services in case of component/location failures. The agency shall also verify the availability of services to all the users in the defined locations. The MSI would need to provide an Infrastructure Fault Management System for the following functions:
- a) **Infrastructure Fault Analysis**
 - 1. The proposed solution must automatically discover manageable elements connected to the network and map the connectivity between them. The Network Fault Management consoles must provide the topology map view from a single central console.
 - 2. The proposed system must support multiple types of discovery including IP range discovery, Seed router based discovery & Trap-Based Discovery
 - 3. The system should provide discovery & inventory of heterogeneous physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and do mapping of LAN & WAN connectivity with granular visibility up to individual ports level.
 - 4. The system must be able to support mapping and modelling of the infrastructure grouped by network connectivity, physical location of equipment and user groups or departments
 - 5. The system should support maps grouped by network topology, geographic locations of the equipment's and user group/departments. These should help in understanding physical Network, virtual Network services and the relationships between them.

6. The system must provide visualization tools to display network topology and device to device connectivity. The system must also be able to document connectivity changes that were discovered since the last update.
7. The proposed solution must provide a detailed asset report, organized by vendor name and device, listing all ports for all devices. When a report is run the administrator must have an option of specifying the number of consecutive days the port must be —unused— in order for it to be considered —available.
8. The proposed solution should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis.
9. It should have a strong event correlation engine which can correlate the events on the basis of event pairing, event sequencing etc.
10. The system must be able to “filter-out” symptom alarms and deduce the root cause of failure in the network automatically.
11. The proposed solution must support an architecture that can be extended to support multiple virtualization platforms and technologies

b) Configuration Management for Critical Network Devices

1. The system should be able to clearly identify configuration changes as root cause of network problems
2. The proposed fault management solution must be able to perform real-time or scheduled capture of device configurations
3. The proposed fault management solution must be able to store historical device configurations captured in the database and thereby enable comparison of current device configuration against a previously captured configuration as well as compare the current configuration against any user-defined standard baseline configuration policy.

c) Advanced IP Services Management for technologies like QoS and Multicast

1. The proposed solution should be able to support response time agents to perform network performance tests to help identify network performance bottlenecks.
2. The proposed solution should be able to monitor QoS parameters configured to provide traffic classification and prioritization for reliable VoIP transport. The proposed solution should discover and model configured QoS classes, policies and behaviours.

3. The proposed solution should provide the ability to discover, map & monitor multicast sources & participating routers wherein the system should be able visualize the distribution tree in the topology map.

d) Infrastructure-based SLA Management and Integration Requirements

1. The proposed service management system should provide a detailed service dashboard view indicating the health of each of the departments / offices in the organization and the health of the services they rely on as well as the SLAs.
 2. The system must be capable of managing IT resources in terms of the business services they support, specify and monitor service obligations, and associate users/Departments/ Organizations with the services they rely on and related Service/Operational Level Agreements.
 3. Root cause analysis of infrastructure alarms must be applied to the managed Business Services in determining service outages. SLA violation alarms must be generated to notify whenever an agreement is violated or is in danger of being violated.
 4. The system must provide the capability to designate planned maintenance periods for services and take into consideration maintenance periods defined at the IT resources level. In addition, the capability to exempt any service outage from impacting an SLA must be available.
 5. The proposed NMS should provide unified workflow between the fault and performance management systems including bi-directional and context-sensitive navigation
 6. The system must support seamless bi-directional integration to helpdesk or trouble ticketing system
 7. The proposed network fault management system should integrate with the helpdesk system by updating the Asset with CI information to support viewing history or open issues in helpdesk on the particular managed asset and associate an SLA to the ticket in the helpdesk.
5. **Manageability Review:** - The agency shall verify the manageability of the system and its supporting infrastructure deployed using the Enterprise Management System (EMS) proposed by the MSI. The manageability requirements such as remote monitoring, administration, configuration, inventory management, fault identification etc. shall have to be tested out.

6. **SLA Reporting System:** - MSI shall design, implement/customize the Enterprise Management System (EMS) and shall develop any additional tools required to monitor the performance indicators listed under SLA prescribed in this RFP. The Acceptance Testing & Certification agency shall verify the accuracy and completeness of the information captured by the SLA monitoring system implemented by the MSI and shall certify the same. The EMS deployed for system, based on SLAs, shall be configured to calculate the monthly transaction-based payout by JSCL to MSI. The MSI may provide an end to end Service Level Management System for the Data centre and Network Infrastructure
 1. Provide end-to-end, comprehensive, modular and integrated management of IT infrastructure components to maximize the availability of IT services and SLA performance.
 2. The management system needs to aggregate events and performance information from the domain managers and tie them to service definitions. This capability is critical for the administrators to have a complete view of the performance and availability of various application services being managed.
 3. The proposed tools should automatically document problems and interruptions for various IT services offered and integrate with the service level management system for reporting on service level agreements (SLAs).
 4. The system must be capable of managing IT resources in terms of the business services they support, specify and monitor service obligations, and associate users/Departments/Organizations with the services they rely on and related Service/Operational Level Agreements.
 5. Provide a detailed service dashboard view indicating the health of each of the departments / offices in the organization and the health of the services they rely on as well as the SLAs.
 6. Provide a high level view for executives and other users of the system using a real time business services Dashboard.
 7. Provide an outage summary that gives a high level health indication for each service as well as the details and root cause of any outage.
 8. Support for a User Definition Facility to define person(s) or organization(s) that uses the business Services or is a party to a service level agreement contract with a service provider or both. The facility must enable the association of Users with Services and SLAs.

9. The Service Level Agreements (SLAs) definition facility must support defining a set of one or more service Guarantees that specify the Service obligations stipulated in an SLA contract for a particular time period (weekly, monthly, and so on). Guarantees supported must include one that monitors service availability (including Mean Time to Repair (MTTR), Mean Time between Failure (MTBF), and Maximum Outage Time thresholds) and the other that monitors service transaction response time.
10. SLA violation alarms must be generated to notify whenever an agreement is violated or is in danger of being violated.
11. Provide the capability to designate planned maintenance periods for services and take into consideration maintenance periods defined at the IT resources level. In addition, the capability to exempt any service outage from impacting an SLA must be available.
12. A historical reporting facility that will allow for the generation of on-demand and scheduled reports of Business Service related metrics with capabilities for customization of the report presentation.

A list of SLAs that needs to be measured using the proposed monitoring tools is given below. These SLAs must be represented using appropriate customizable reports to ensure overall service delivery. Monitoring system should be capable of sending alerts through SMS, email alarm etc.

a) Service Level Category: Network Infrastructure

Network Specific SLAs

- Uptime SLA
- MTBF (Mean Time Between Failures) & MTTR (Mean Time to Repair)
- Latency & Response Time (DNS / DHCP / SMTP etc.)
- Traffic-based SLAs

b) Service Level Category: Data Centre IT Infrastructure

System Specific SLAs

- System Availability
- System Response Time
- Utilization based SLAs (CPU / Memory etc.)

c) Application Specific SLAs

End-User Based SLAs

- End-to-End Response Time for End-User Web Pages to Load

- Avg. Response Time, Errors Per Interval, Response per Interval
- SLAs from Critical Processes (e.g. Submit Button Click, Upload Action in Portal)

d) Transaction Based SLAs

- SLAs for Business Process involving with multiple steps / pages
- Completion Time SLA for Critical Business Processes

e) Application Deep-Dive SLAs

- Application Component-Wise SLA within the DC
- SLA for DB Query to Complete
- Web Services Call etc.
- 3rd Party interaction SLAs between Applications

f) Project Documentation: - The Agency shall review the project documents developed by MSI including requirements, design, source code, installation, training and administration manuals, version control etc. Any issues/gaps identified by the Agency, in any of the above areas, shall be addressed to the complete satisfaction of JSCL.

g) Data Quality: - The Agency shall perform the Data Quality Assessment for the Data digitized/migrated (If required) by MSI to the system. The errors/gaps identified during the Data Quality Assessment shall be addressed by MSI before moving the data into production environment, which is a key mile stone for Go-live of the solution.

J. Capacity building & Training

Post the system integration, MSI shall train Authority representatives to operate the equipment installed and to conduct any routine diagnostics and routine maintenance work. Training shall be done during Pilot Deployment and before Final Deployment. The period of training shall be mutually agreed upon by Authority and MSI. The actual number of each of above categories of trainees will be provided at Design Stage. The number of trainees during go live shall be 150 and shall decline as we move towards completion of four-year O&M period.

The main challenges to be addressed effectively by the MSI are the diverse trainee base, wide variability in education and computer proficiency and minimal availability of time. The MSI holds the responsibility for

creation of a detailed and effective training strategy, user groups and classifications, training plan and guidelines, detailed training material, training program designed and their delivery to the target groups.

- **Develop Overall Training Plan:** MSI shall be responsible for finalizing a detailed Training Plan for the program in consultation with Authority covering the training strategy, environment, training need analysis and role based training curriculum. MSI shall own the overall Training plan working closely with the Authority. MSI shall coordinate overall training effort. Following is the indicative list of the training programs that needs to be administered to the group of officials as identified above. The overall responsibility of administering the training program lies with the MSI.
 - Awareness and sensitization of benefits of IT
 - Basic Computer Awareness & Role based training for application users
 - Trainers Training
 - System Administration & Support Training

The Training Plan (TP) shall be developed for each component / module and shall include the training schedule and course outlines. The MSI must provide the Training Plan for review to Authority at least three weeks in advance of the start of training. The Training Plan must be approved by Authority before the start of training.

MSI shall deliver training to the end users utilizing the infrastructure at the designated Training Centres. Role based training for the Senior Officers will be carried out at a suitable location by the MSI. Most of the training would be an Instructor-Led Training (ILT) conducted by trained and qualified instructors in a classroom setting. To maintain consistency across trainings, standard templates should be used for each component of a module.

Post the system integration, MSI shall train Authority or its representatives/stake holders involved to operate the equipment installed and to conduct any routine diagnostics and routine maintenance work. Training shall be done before Go-live. The period of training shall be mutually agreed upon by Authority and MSI.

- **Develop Training Schedule and Curriculum:** MSI shall develop and manage the training schedule in consultation with Authority, aligned with the overall implementation roadmap of the project and coordinate the same with all parties involved. Training schedule shall be developed by solution and shall be optimized to reduce business impact and effective utilization of Training infrastructure and capacities. The training curriculum should be organized by modules and these should be used to develop the

training materials. The training curriculum outlines the mode of delivery, module structure and outline, duration and target audience. These sessions should be conducted such that the users of the application/modules are trained by the time the application “goes-live” with possibly no more than a week’s gap between completion of training and going live of modules. Continuous reporting and assessment should be an integral function of training. MSI shall also identify the languages to be used by the end-user for entering data and ensuring multi-language training to the end users as per requirement.

- **Learning Management System and Training Portal:** Developing a Learning Management System and Training Portal for providing access to all training content online including documents, demo, audio, video, simulation and practice, assessment, self-learning and context sensitive help and monitoring, support and reporting. Learning management tool shall be a simple webpage comprising of training materials arranged in modular approach. The tool shall have user manuals, audio, video etc. with user specific roles and responsibilities. The training material shall be accessed from within JICCC network only.
- **Training Programs / Curriculum:** Following is the indicative list of the training programs that needs to be administered to the group of officials as identified below. The overall responsibility of administering the training program lies with the MSI.
 - Basic IT skills and use of computers to creating awareness about the benefits of ICT and basic computer skills
 - Role-based training on the COTS based applications – Basic and Advanced. This training should be in a role based, benchmarked and standardized format, and shall be available in English/Hindi/Punjabi and lead to learning completion and assessment. It should also allow for self-learning and retraining. Training would include mechanism for demonstration using audio / video / simulated / demo practice exercises.
 - System Administrator training; a few members of the various departmental staff with high aptitude would be trained to act as system administrators and trouble shooters for the system.
 - Customization of the Training Manuals, User Manuals, Operational and Maintenance Manuals provided along with the Software.

An indicative content structure for the training programs is listed as below:

SL No.	Type of Training	Training Content	Days (minimum)
1	Awareness and sensitization of benefits of ICT	This module shall cover Principles of e-governance; it shall also cover the advantages of use of ICT in MCJ. It shall briefly cover the technology trends and how it can be put to use by use of live examples of ICT use across the world	1
2	Basic computer awareness	This module shall cover the fundamental concepts of Computer, Internet, Peripherals, System software and Application Software. It shall also cover the use of MS-Office suite in detail. It can also touch upon use of office tools such as printers, fax machine, copiers and scanners as well as basics in use of computers (checking network connections, etc.).	1
3	Role based system training on The JICCC Application Software	This module is required to train the at various levels in operating the application. The training is to be provided to the staff depending upon their role and responsibilities in the workflow. During this training, the trainees could also be asked to carry out the routine functions using the software. The training should be module based and cover all modules of JICCC. Training materials should be provided to users	2
4	System Administration support and Trouble Shooting	Skills in Troubleshooting vis-à-vis application, standard software and networking (for those with the aptitude and/or prior training)	3

In cases where the training material may be made available by the OEM, it is the MSI's responsibility to ensure the relevance of the material to authorities, customize if necessary and own up the delivery and effectiveness. MSI shall ensure that the training content meets all the objectives of the training course. The material shall be developed in English/Hindi/Punjabi language. MSI shall also develop the training material for delivery through Computer Based Training, Instructor Led Training, Online User Material/Help Manuals

and Job Aids. MSI shall provide detailed training material providing step-by-step approach in soft and hard copies to all offices for reference.

Trainees: The MSI shall provide training courses for at least:

- Master trainers
- Decision Makers/ Management
- Authority's operations personnel
- Users of Various Systems/Applications developed as part of the project.

Authority will also identify and nominate the master trainers and MSI shall be responsible to provide the training. All future recurring trainings shall be conducted by these master trainers. It is MSIs responsibility to ensure that the master trainers are well trained and also ensure that the master trainers have a better understanding the system through simple evaluation. The number of master trainers to be trained by MSI is inclusive of the indicative number of trainees mentioned above.

- **Training Material:** MSI shall provide all training materials in both Office Suite and Adobe PDF formats,

consisting of graphics, video and animations on Digital Video Disc (DVD) with a permission to reproduce copies later on.

MSI shall furnish all special tools, training videos, self-learning tools, equipment, training aids, and any other materials required to train course participants, for use during training courses. Training shall include, as a minimum, a four (4) hour session on system maintenance and configuration, and a four (4) hour session on system operations.

MSI shall also be responsible for full capacity building of relevant staff. Training and capacity building shall be provided for all individual modules along with their respective integrations. All training materials shall be developed by the MSI.

The instructors shall demonstrate thorough knowledge of the material covered in the courses, familiarity with the training materials used in the courses, and the ability to effectively lead the staff in a classroom setting. If at any stage of training, the Authority feels that on-field sessions are required, the same shall be conducted by the MSI. The language of training shall be in English, Hindi, Punjabi as indicated by the Authority during this stage.

If any instructor is considered unsuitable by Authority, either before or during the training, the MSI shall provide a suitable replacement within one week of receiving such notice from Authority.

MSI has to ensure that training sessions are effective and the attendees shall be able to carry on with their work efficiently. For this purpose, it is necessary that effectiveness of the training session is measured through a comprehensive feedback mechanism.

- Training Effectiveness Evaluation:** MSI shall evaluate the effectiveness of all end user's trainings using electronic or manual surveys. MSI shall be responsible for analyzing the feedback and arrange for conducting refresher training, wherever needed. Authority will periodically monitor the training effectiveness through the performance metrics and Service levels and the MSI shall comply with the same.

The indicative no. of trainees is as provided below. However, the MSI is required to fully access the training requirements and arrive at the final nos. of trainees based on its own study.

Department	No of Trainees
Civil Police	50
Traffic Police	150
Municipal Corporation	50
District Administration	10
JSCL and PMC	50
Other	20
Total	330

K. Change Management

MSI shall help the agencies with complete Change Management exercise needed to make this project a success. In fact, Change Management will have to subsume 'training' as a key enabler for change. Following outlines, the responsibilities of MSI with respect to designing and implementation of change management plan for the Project.

- Change Management initiative, to be designed & implemented by MSI, shall focus on addressing key aspects of Project including building awareness in personnel on benefits of new system, changes (if any) to their current roles & responsibilities, addressing the employee's concerns & apprehensions w.r.t. implementation of new system and benefits that are planned for the employees.

- It is required that if MSI doesn't operate in the Change Management, Communication and Training domain then he collaborates with/ hires services of a specialist agency who will be responsible for complete Change Management, Awareness and Communication implementation and monitoring, on the lines suggested below
- The agencies requiring change management as part of the project shall form various stakeholder groups to address the Change Management Initiative. Stakeholders are all those who need to be considered in achieving the project goals and whose participation and support are crucial to its success. A key individual stakeholder or stakeholder group is a person or group of people with significant involvement and/or interest in the success of the project.
- Stakeholder analysis identifies all primary and secondary stakeholders who have an interest in the issues with which the Jalandhar Integrated Command & Control Centre is concerned. The stakeholder groups will be the set of core users (Change Agents) who will directly participate in the awareness and communication initiatives, workshops, and provide feedback to the governance Committee
- Stakeholder groups can be categorized into below categories, based on their influence and role in managing the change and making it successful.

L. Final Deployment and Documentation

After addressing the Authority's feedback and any deficiency observed during the Pilot deployment and upon completion of System Acceptance Tests (SAT), final deployment of the Jalandhar Smart City solutions shall be considered by the MSI. For achievement of final deployment, MSI shall also be responsible for development of a cutover strategy which shall include initial data take on, sequence of data takes on, set up of support mechanisms to minimize business impact due to any cutover activities.

Post the final deployment, MSI shall handover detailed documentation that describes the site conditions, system design, configuration, training, as-built conditions, operation and maintenance. All documentation shall be in English, Hindi & Punjabi (as agreed with the Authority), shall utilize metric measurements, and shall be submitted directly to Authority in paper hardcopy and electronically in Word/AutoCAD/Excel/Project and Adobe Acrobat that should be editable or updated.

All installation drawings shall be prepared in AutoCAD, GIS and Adobe Acrobat and provided on CD-ROM as well as hard copies. The drawings shall contain sufficient detail including but not limited to equipment dimensions, interfaces, cable details, equipment mounting and fire protection. Electrical and electronic drawings shall be supplied to show engineering changes made to any component or module any time during the contract period.

'As-built' Documents delivered by the MSI shall include:

- An inventory of all components supplied including model name, model number, serial number and installation location
- An inventory of all spare parts supplied including brand, model number, and serial number and storage location
- All reference and user manuals for system components, including those components supplied by third parties
- Point of Contact for each OEM for maintenance
- Warranties and Maintenance schedules for the hardware procured
- All warranties documentation, including that for components supplied by third parties
- As-built in CAD and GIS
- A diagram indicating the as-built inter-connections between components
- Software documentation which also includes the version number of all software, including that supplied by third parties
- Cable run lists and schedules
- All network and equipment details such as IP addresses, user names, and passwords
- Data communication protocols; and
- 'As-Built' drawings for all components installed

MSI shall submit to the Authority copies of comprehensive operating and maintenance manuals, and log sheets for all systems and hardware supplied as part of this RFP. These shall be supported with the manufacturer's operating and maintenance manuals. The manuals shall be complete, accurate, up-to-date, and shall contain only that information that pertains to the system installed. Maintenance documents shall include:

- Equipment installation and operating documentation, manuals, and software for all installed equipment

- System Installation and setup guides, with data forms to plan and record options and configuration information
- The schedule/procedures for preventative maintenance, inspection, fault diagnosis, component replacement and on-site warranty support administration on each system component
- Hard copies of manufacturer's product specification sheets, operating specifications, design guides, user's guides for software and hardware, and PDF files on CD-ROM or non-volatile memory stick of the hard-copy submittal
- Complete list of replaceable parts including names of vendors for parts not identified by universal part numbers (such as EIA codes)
- Manufacturer's product specification sheets, operating specifications, design guides, user's guides
- Permits
- Contractor names and telephone number lists for all project trades

MSI shall provide Systems Manuals (SM), documentation including:

- The configuration and topology of central systems hardware and software
- Central systems software functions and operations
- Scheduled maintenance required for the central systems; and
- Database structure and data dictionary

MSI shall also provide following documents for any be-spoke software development:

- Business process guides
- Program flow descriptions
- Data model descriptions
- Sample reports
- Screen formats
- Frequently Asked Questions (FAQ) guides
- User Manuals and technical manuals
- Any other documentation required for usage of implemented solution

Documentation of processes shall be done using standard flow charting software. An intuitive online learning tool depicting standard operating procedures of system usage are required to be deployed. There shall be a provision of training system in the deployment architecture so as new employees can be inducted easily.

All pages of the documentation shall carry a title, version number, page number and issue date, and shall contain a complete subject index. MSI shall be responsible for fully coordinating and cross referencing all interfaces and areas associated with interconnecting equipment and systems.

Documentation shall require re-issues if any change or modification is made to the equipment proposed to be supplied. MSI may re-issue individual sheets or portions of the documentation that are affected by the change or modification. Each re-issue or revision shall carry the same title as the original, with a change in version number and issue date.

Each volume shall have a binder (stiff cover and spine), and drawings shall be protected by clear plastic to withstand frequent handling. The binding arrangement shall permit the manual to be laid flat when opened. The paper used shall be of good quality and adequate thickness for frequent handling.

M. Operational System Acceptance

At the completion of operational acceptance test, the system shall be considered for operational system acceptance. At the close of the work and before issue of final certificate of completion by the Authority, the MSI shall furnish a written guarantee indemnifying Authority against defective materials and workmanship for a period of one (1) year after completion which is referred to as Defect Liability Period. The MSI shall hold himself fully responsible for reinstallation or replace free of cost to Authority during the Defect Liability period. MSI shall provide approved temporary replacement equipment and material such that the system remains fully functional as designed and commissioned during repair or replacement activities at no cost to the Authority

N. Comprehensive Maintenance for System and Services

MSI shall be responsible for comprehensive maintenance of both hardware and software, required upgradations in the system, expansion of the system, technical manpower, spares management and replenishment, performance monitoring and enhancements of the Jalandhar Smart City solutions deployed as part of this project and shall maintain service levels as defined in the RFP. All equipment and material supplied by the MSI shall be provided with five warranty against defects of design and manufacturing and against faults and failures associated with workmanship of MSI and its sub-contractors commencing from operation acceptance of the system. All equipment found to be defective during comprehensive maintenance shall be repaired or replaced by the MSI at no cost to the Authority.

MSI shall provide all the technical, managerial, and other staffing required to manage day to-day maintenance of the Jalandhar Smart City solutions during the Contract period. MSI shall deploy project manager stationed at Jalandhar who shall be the single point of contact to the Authority and shall be responsible for operation and maintenance of the system.

All spares required for the smooth operation of the Jalandhar smart city solutions shall be maintained by the MSI for the entire duration of the contract to meet SLA requirements. The cost of the spares, repairs, and replacement shall all be deemed to be included in the price quoted by the MSI. MSI shall also institutionalize structures, processes and reports for management of SLA. Root cause analysis and long term problem solutions shall also be part of MSI scope.

MSI shall maintain all data regarding entitlement for any upgrade, enhancement, refreshes, replacement, bug fixing and maintenance for all project components during Warranty. MSI shall be responsible for updates/upgrades and implementation of new versions for software and operating systems when released by the respective OEM at no extra cost to the Authority during entire duration of contract. Requisite adjustments / changes in the configuration for implementing different versions of system solution and/or its components shall also be done by MSI. The MSI shall also ensure application of patches to the licensed software covering the appropriate system component software, operating system, databases and other applications. Software License management and control services shall also be conducted by the MSI during this phase. Any changes/upgrades to the software during comprehensive maintenance shall be subjected to comprehensive and integrated testing by MSI to ensure that changes implemented in system meets the specified requirements and doesn't impact any other function of the system. Issue log for errors and bugs identified in the solution and any change done in solution (vis-à-vis the FRS, BRS and SRS signed off) shall be periodically submitted to the Authority. MSI shall also be responsible for operating City website, city portal, and city application including all support, content updates and upgrades throughout the duration of contract.

Periodically, IT audits will be conducted by JSCL/ PMC during the support period.

MSI shall ensure OEM support during Comprehensive Maintenance stage for system performance, performance tuning, upgrades etc. MSI shall provide all support for formulation of all policies and procedures related to System Administration, Data Base Management, applications, archives, network management & security, back up and data recovery and archive, data synchronization after crash. Assistance to Authority

shall be provided as needed in management of legacy data interfaced, print spools, batch jobs, printer configuration etc.

MSI shall prepare a detailed System administration manual, Data administration manual, operational manual, User manual which shall be used by Authority's employees to run Jalandhar Smart City system's production environment. This shall also include how the various parameters shall be monitored/ tuned in a live system. Preparation of requisite system configuration for disaster recovery management and fail over system plan shall also be under the supervision of MSI. The MSI shall also maintain the following minimum documents with respect to ICT components:

- High level design of system;
- Module level design of system;
- System Requirement Specifications (SRS);
- Any other explanatory notes about system;
- Traceability matrix;
- Compilation environment

MSI shall also ensure Updating of following documentation of software system

- Documentation of source code;
- Documentation of functional specifications;
- Application documentation is updated to reflect on-going maintenance and enhancement including FRS and SRS, in accordance with the defined standards;
- User manuals and training manuals are updated to reflect on-going changes/enhancements;
- Adoption of standard practices in regards to version control and management

The communication costs (Internet charges, telephone charges, 4G/GPRS connectivity charges) and any other incidental charges related to maintenance period shall be in the scope of the MSI and considered to be included in the proposal submitted by the MSI for the entire contract duration. Any planned and emergency changes to any component during maintenance period shall be through a change management process. For any change, MSI shall ensure

- Detailed impact analysis;
- Change plan with roll back plan;
- Appropriate communication on change required has taken place;
- Approvals on change;
- Schedules have been adjusted to minimum impact on production environment;
- All associated documentation is updated post stabilization of the change;
- Version control maintained for software.

Any software changes required due to problems/bugs in the developed software/application will not be considered under change control. The MSI will have to modify the software/application free of cost. This may lead to enhancements/customizations and the same needs to be implemented by the MSI at no extra cost.

If the Operating System or additional copies of Operating System are required to be installed/reinstalled/ de-installed, the same should be done as part of the post implementation support.

O. Support Staff Required

Three (4) types of support staff shall be provided by MSI during Operations and Maintenance phase:

- JICCC Operations & Helpdesk Staff
- Maintenance Support Staff
- Helpdesk Support staff
- Facility Management Staff

▪ **JICCC Operations & Helpdesk Staff**

MSI shall depute JICCC Operators for staffing the operations room on a 3-shift basis, according to the following:

Operations Staff:

- One (1) Day-Shift comprising of 4 personnel;
- Other Management personnel during day shift
 - Project Manager
 - Project Management support
 - Intelligent Signalling & Surveillance expert
 - Security expert
 - Network administrator
 - Data scientists
- One (1) Evening-Shift comprising of 3 personnel;
- One (1) Night-Shift comprising of 1 personnel

MSI shall also provide adequate support staff at Helpdesk. The support staff at Helpdesk shall provide 24*7 services, work in a shift based system and provide full support coverage of Helpdesk and maintain the system as per SLAs defined. At a minimum, 3 support personnel shall be deputed at Helpdesk during maintenance phase in following shifts:

- **IT Helpdesk:**

Three (3) shifts comprising of minimum 2 personnel each for morning and evening and one for night shift.

- **Maintenance Support Staff**

Well trained, efficient and effective Maintenance Support Staff shall be provided by the MSI during the maintenance phase of the project to support Authority's operational and technical requirements in day to day operations of the smart city solutions provided by MSI. Any fault originating for the Jalandhar smart city components shall be addressed by the MSI Maintenance Support staff in the least time possible. The staff assigned shall be well qualified to attend to the emergency situations and shall be able to communicate in an effective and efficient manner. The supports staff shall provide 24*7 services, work in a shift based system and provide full support coverage of the Jalandhar smart city solution and maintain the system as per the SLA's defined.

- **Facility Management Staff**

Facilities management which include but not limited to building and grounds maintenance, cleaning, catering and vending, security, space management, utilities management etc. and associated manpower shall also be under the scope of the MSI during maintenance phase. At a minimum, MSI shall depute Facility Management staff of atleast 5 personnel which shall work in a shift based system to provide 24*7 services. Staff requirement per each shift is as per below:

- Two (2) shifts comprising of 3 personnel each;
- One (1) Night shift comprising of 1 personnel each.

One personnel shall be appointed as supervisor. Any additional staff required for management, HR, payroll etc. of Maintenance staff, Helpdesk and Facility Management staff, if required by MSI, shall also be under the scope of the MSI.

Note: The above-mentioned staffing is indicative and MSI need to depute additional staff as per the requirement of project.

3. GENERAL REQUIREMENTS

The MSI is required to draft / prepare and then finalize the detailed architecture for the overall ICT systems for the Smart City features, by incorporating findings of site surveys. The Solution so envisaged by the MSI should be able to provide real time Jalandhar Integrated Command and Control Centre (JICCC). All the components & Sub-Components of the Overall Smart City Solution and the respective Technical Architecture should:

- at least comply with the published e-Governance standards, frameworks, policies and guidelines available on <http://egovstandards.gov.in> (updated from time-to-time); and
- be of leading industry standards
- comply with the Cyber Security Model Framework for Smart Cities issued by MoHUA

Technical Architecture requirement:

While responding to the RFP, the Bidders are to submit the detailed Technical Architecture for all the components along with the detailed description of each of the Smart City ICT Component, their Sub-Components. The Solution should factor in and take into consideration following guiding principles:

- a) **Scalability** - Important technical components of the architecture must support scalability to provide continuous growth to meet the growing demand of the Jalandhar City. The system should also support vertical and horizontal scalability so that depending on changing requirements from time to time, the system may be scaled upwards. There must not be any system imposed restrictions on the upward scalability in number of cameras, data centre equipment or other smart city components. Main technology components requiring scalability are storage, bandwidth, computing performance (IT Infrastructure).

The architecture should be scalable (cater to increasing load of internal and external users and their transactions) and capable of delivering high performance till the system is operational. In this context, it is required that the application and deployment architecture should provide for Scale-Up and Scale out on the Application and Web Servers, Database Servers and all other solution components. The data centre infrastructure shall be capable of serving at least 200 concurrent internal users and 1000 mobile users. The Applications proposed for various vertical solutions shall be capable of handling 100% growth for the next 4 years. MSI shall clearly quantify the expansion capabilities of the application software without incurring additional cost.

- b) **Availability** - The architecture components should be redundant and ensure that there are no single point of failures in the key solution components. Considering the high sensitivity of the system, design should be in such a way as to be resilient to technology sabotage. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage. The MSI shall make the provision for high availability for all the services of the system. Redundancy has to be considered at the core / data centre components level. All required inventory for high availability has to be planned by MSI.
- c) **Security** - The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc. MSI must make provisions for security of field equipment as well as protection of the software system from hackers and other threats. Using Firewalls and Intrusion Prevention Systems such attacks and theft should be controlled and well supported (and implemented) with the security policy. The virus and worm attacks should be well defended with gateway level Anti-virus system, along with workstation level Anti-virus mechanism Appropriate insurance cover must be provided to all the equipment supplied under this project.

Field equipment installed through this project would become an important public asset. During the contract period of the project, the MSI shall be required to repair / replace any equipment if stolen / damaged / faulty. Appropriate insurance cover must be provided to all the equipment supplied under this project

All the system(s) implemented for the Jalandhar Smart City Project should be highly secure, with adequate security & protection of the sensitive data relating to the Jalandhar City and its residents. Few such overarching security considerations are briefly described below; the MSI is expected to submit the most appropriate Security Features for the overall ICT Solution:

1. The Generic architecture of smart city generally consists of four layers - a sensing layer, a communication layer, a data layer and an application layer, and these four layers are overseen by the smart city security system. Architecture of information Technology Systems deployed in Smart City need to be open, interoperable and scalable

2. The message exchange between various applications in the smart city should be fully encrypted and authenticated. Any application outside the Data Centre (DC) should talk to the applications hosted in the datacentre through only predefined API's.
3. Convergence of multiple infrastructures into one Central platform for ease of management in a Smart City is mandatory. Applications hosted in the central data centre should support multi-tenancy with adequate authentication and Role based access control mechanism for each tenant pertaining to their respective line department infrastructure
4. The smart city architecture should be capable of managing heterogeneous data, which would be continuously communicated through numerous devices following different protocols. In order to ensure that the flow of data between devices does not run into latency issues, appropriate protocols need to be deployed so as to minimize latency. The following communication protocols could be used for the different layers for data flow.
 - **Between applications and back end systems:** HTTP, SQL, FTP, SNMP, SOAP, XML, SSH, SMTP
 - **Between back end systems and field devices:** Message Queue Telemetry Transport (MQTT), xMPP, RESTful HTTP, Constrained Application Protocol (CoAP), SNMP, IPv4/6, BACnet, LoNworks, Low Power Wide Area Network (LoRa), Fixed, 4G/5G, Wi-Fi, WiMax, 2G/3G from field devices: ZigBee oLP, ETSI LTN, IPv4/6, 6LowPAN, ModBus, Wi-Fi, 802.15.4, enocean, RFID, NFC, Bluetooth, DashT[®] Fixed, ISM & short-range bands.
5. Data Layer (termed as City Digital platform/ fabric) should be capable of communicating with various types of sensors/ devices and their management platforms/applications for single/multiple services irrespective of software and application they support. Data exchange between various sensors and their management applications must strictly happen through this layer, thus making it one true source of data abstraction, normalization, correlation and enable further analysis on the same. Adequate security checks and mechanisms as described in later points to be deployed to protect data layer from data confidentiality breach and unauthorized access.
6. The entire information Technology (IT) infrastructure deployed as part of Smart city will follow standards like - ISO 27001, ISO 22301, ISO 37120, ISO 3712, ISO 27017, ISO

27018, BSI PAS 180, BSI PAS 18'1, BSI PAS'182, for Wi-Fi access - PEAP (Protected Extensible Authentication Protocol), 3rd Generation Partnership Project (3GPP), etc. or preferably MSI should engage with TPA at the requirement formulation stage for STQC/Cert-in. Cost of the certification will be borne by MSI.

7. Application Program Interfaces (APIs) should be published and the IT systems be running on standard protocols like JSON / XML or REST etc.
8. From a network security perspective all information that flows on the network should be encrypted to ensure safety and privacy of confidential data. The devices at each endpoint of the network should be authenticated (using mechanisms based on attributes one of which could use passwords). The authentication system so used on these endpoint devices should ensure that only authorized users are sending data over the network, and there is no rogue data that is sent to the control systems to generate false alarms or sabotage the systems
9. All sensors deployed as part of IT and IT based systems in the Smart cities should talk only to the identified Jalandhar Smart City network, and do not hook on to the rogue networks' The guidelines to secure Wi-Fi networks as published by Department of Telecom must be followed
10. Wireless layer of the Smart City Network should be segmented for public and utility networks by using Virtual Private Networks (VPN's) or separate networks in the wired core, so that any traffic from the internet users is not routed into the sensor networks and vice-versa.
11. All traffic from the sensors in the Smart city to the application servers should be encrypted Secure Socket Layer (SSL), PKI and authenticated prior to sending any information. The data at rest and in transit must be encrypted
12. Authentication of sensors in the Smart city should happen at the time of provisioning the sensors, and adding them into the system, and should be based on physical characteristics of the sensors like MAC ID, Device ID etc.

13. Sensors deployed in solutions to set up Smart city should be hardened devices with the ability to be upgraded remotely for firmware through encrypted image files.
14. As various sensors use multiple protocols to communicate with the underlying network with varied security capability, the system should allow provisioning necessary authentication and encryption at the gateway or the nearest data aggregation level if the sensor is not able to do the same.
15. The Sensors or edge device deployed in Smart city should not have any physical interface for administration. Monitoring of systems and networks should be undertaken remotely.
16. All the sensors in the Smart city should connect to an identified network for Jalandhar Smart City.
17. The data centre should be segmented into multiple zones with each zone having a dedicated functionality e.g. all sensors for one operational domain can connect to the data centre in one zone, and the internet facing side of the data centre should be in another zone
18. The internet facing part of the data centre should have a Demilitarized zone where all the customer application servers would be located that are customer facing. Only these servers can access the data from the actual utility application servers on predefined ports
19. The customer application servers should be accessed only by the web server that is hosted in a different zone of the data centre.
20. The following should be implemented in the data centre - firewalls, intrusion detection & Intrusion prevention systems, Web Application Firewalls, Behavioural analysis systems for anomaly detection, Correlation engine, Denial of Service prevention device, Advanced Persistent Threat notification mechanism, Federated identity and access management system, etc.

▪ **Web Proxy Solution:**

Offered solution should be hardened Web Proxy, Caching, Web based Reputation filtering, URL filtering, Antivirus and Anti-malware appliance. All these functionalities

should be preferably in a single appliance. Provided operating system should be secured from vulnerabilities and hardened for web proxy and caching functionality.

▪ **NGIPS:**

Solution should include Next Generation Intrusion Prevention System (NGIPS) to provide Advanced Threat Protection solution with future enhancements and protocols. Solution should be for both passive (i.e., monitoring) and inline (i.e., blocking) modes. Detection should be capable of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, zero-day threats, etc.). Solution should also be able to detect threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioural anomaly detection techniques.

21. All "applications' and "apps" will undergo static and dynamic security testing before deployment and be tested with respect to security on regular basis at least once in a year'
 - a. All applications and "Apps" deployed as part of Smart city be hosted in India'
 - b. The said architecture Provide:
 - Automatic and secure updates of software and firmware etc.
 - All systems and devices should provide auditing and logging capabilities'
 - Ensure vendor compliance to remove any backdoors, undocumented and hard cored accounts.
 - End-to End solution should be provided with annual end-to-end service availability of 99.999 percent. The end to end service agreement should be in place for minimum period of four years form the date of operation. Appropriate teams may be set up to monitor cyber incidents and mitigation of same.
22. All the information on incidents be shared regularly with Indian Computer Emergency Response Team (CERT-India) and NCIIPC (National Critical Information Infrastructure Protection Centre) and take help to mitigate and recover from the incidents.

23. The solution should provide for maintaining an audit trail of all the transactions and should also ensure the non-repudiation of audit trail without impacting the overall performance of the system
24. The security services used to protect the solution shall include: Identification, Authentication, Access Control, Administration and Audit and support for industry standard protocols
25. The solution shall support advanced user authentication mechanisms including digital certificates and biometric authentication
26. Security design should provide for a well-designed identity management system, security of physical and digital assets, data and network security, backup, recovery and disaster recovery system
27. The solution should provide for maintaining an audit trail of all the transactions and should also ensure the non-repudiation of audit trail without impacting the overall performance of the system
28. The overarching requirement is the need to comply with ISO 27001 standards of security
29. The application design and development should comply with OWASP top 10 principles
 - d) **Manageability** - Ease of configuration, ongoing health monitoring, and failure detection are vital to the goals of scalability, availability, and security and must be able to match the growth of the environment. Network should be auto/manual configurable for various future requirements for the ease of maintenance / debugging.
 - e) **Interoperability** - The system should have capability to take feed from cameras installed by private / Govt. at public places, digitize (if required) & compress (if required) this feed & store as per requirements.
 - f) **Open Standards** - Systems should use open standards and protocols to the extent possible.

- g) **Single-Sign On** - The application should enable single-sign-on so that any user once authenticated and authorized by system is not required to be re-authorized for completing any of the services in the same session. For employees of the department concerned, the browser based application accessed on the intranet, through single-sign-on mechanism, will provide access to all the services of the departments concerned (based on their roles and responsibilities), Help module, basic and advanced reporting etc. Similarly, for external users (citizens, etc.), based on their profile and registration, the system shall enable single-sign on facility to apply for various services, make payments, submit queries /complaints and check status of their applications
- h) **Support for Public Key Infrastructure (PKI) based Authentication and Authorization** - The solution shall support PKI based Authentication and Authorization, in accordance with IT Act 2000, using the Digital Certificates issued by the Certifying Authorities (CA). In particular, 3 factor authentications (login id & password, biometric and digital signature) shall be implemented by the MSI for officials/employees involved in processing citizen services.
- **Interoperability Standards** - Keeping in view the evolving needs of interoperability, especially the possibility that the solution shall become the focal point of delivery of services, and may also involve cross-functionality with the e-Government projects of other departments / businesses in future, the solution should be built on Open Standards. The MSI shall ensure that the application developed is easily integrated with the existing applications. The code does not build a dependency on any proprietary software, particularly, through the use of proprietary ‘stored procedures’ belonging to a specific database product. The standards should:
 - at least comply with the published e-Governance standards, frameworks, policies and guidelines available on <http://egovstandards.gov.in> (updated from time-to-time); and
 - be of leading industry standards

All the personnel working on the Project and having access to the Servers / Data Centre should be on direct payroll or possess valid authorization letter of the MSI/OEM/Consortium Partner. The MSI would not be allowed to sub-contract work, except for the following activities:

- Any Passive Networking or Site Preparation/Civil/Electrical work(s) during implementation and O & M period

- Viewing Manpower at the JICCC / viewing centres & Mobile Vans during post-implementation
- FMS staff for non- IT support during post-implementation

However, even if the work is sub-contracted, the sole responsibility of the timely completion of the work & the quality of the work done shall lie with the MSI. The MSI shall be held responsible for any delay/error/non-compliance/penalties/negligence etc. of its sub-contracted vendor. The details of the sub-contracting agreements (if any) between both the parties would be required to be submitted to the JSCL and approved by the Competent Authority before any such resource mobilization.

- i) **GIS Integration** - MSI shall undertake a detailed assessment for an integration of all the Smart City ICT components with the Geographical Information System (GIS) and any additional layers required for CCTC surveillance by police. MSI is required to carry out the seamless integration to ensure ease of use of GIS in the Dashboards in Jalandhar Integrated Command and Control Centre (JICCC). If this may require any field surveys, it needs to be carried out by the MSI. Any such data readily available with the JSCL, shall be shared with MSI. However, the MSI is to check the availability of such data and its suitability for achieving the project outcomes. MSI is required to update GIS maps from time to time.
- j) **SMS Gateway Integration** - MSI shall carry out SMS Gateway Integration with the Smart Jalandhar City System and develop necessary applications to send mass SMS to groups/individuals, wherever required. Any external/third party SMS gateway can be used, but this needs to be specified in the Technical Bid proposal, and approved during Bid evaluation. Also, wherever feasible, it is envisaged that the MSI proposes to leverage the existing State Solutions, such as NIC Gateways for this purpose.
- k) **Application Architecture** - The Applications designed and developed for the Departments concerned must follow the Industry Best Practice(s) and Industry Standard(s). In order to achieve the high level of stability and robustness of the application, the System Development Life Cycle (SLDC) must be carried out using the industry standard best practices and adopting the security constraints for access and control rights. The various modules / application should have a common Exception Manager to handle any kind of exception arising due to internal/ external factors.

The modules of the application are to be supported by the Session and Transaction Manager for the completeness of the request and response of the Authority request. The system should have a module exclusively to record the activities/ create the log of activities happening within the system / application to avoid any kind of irregularities within the system by any User / Application.

MSI shall design and develop the Smart Jalandhar City System as per the study that would be done by the MSI and as per the scope defined in the RFP.

- a. The Modules specified will be developed afresh based on approved requirement
- b. Apart from this, if some services are already developed/under development phase by the specific department, such services will be integrated with the Smart Jalandhar City System. These service will be processed through department specific Application in backend
- c. The user of citizen services should be given a choice to interact with the system in local languages including English, Hindi and Punjabi. The application should pave the provision for uniform user experience across the multi lingual functionality covering following aspects:
 - Front end Web Portal in English and local language
 - E-forms (Labels & Data entry in local languages). Data entry should be provided preferably using the Enhanced In script standard (based on Unicode version 6.0 or later) keyboard layout with option for floating keyboard
 - Storage of entered data in local language using UNICODE (version 6.0 or later) encoding standard
 - Retrieval & display in local language across all user interfaces, forms and reports with all browsers compliant with Unicode version 6.0 and above
 - Facility for bilingual printing (English and the local language)
- d. The application(s) should comply with World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.0 Level AA/Other time to time issued Govt. Of India/Govt. of Punjab guidelines for making web content accessible to differently-abled person.

- e. Application should have a generic workflow engine for citizen centric services. This generic workflow engine will allow easy creation of workflow for new services. At the minimum, the workflow engine should have the following features:
 - Feature to use the master data for auto-populating the forms and dropdowns
 - Creation of application form, by “drag & drop” feature using Meta Data Standards
 - i. Defining the workflow for the approval of the form
 - ii. First in First out
 - iii. Defining a Citizen Charter/Delivery of service in a time bound manner
 - Creation of the “output” of the service, i.e. Certificate, Order etc.
 - Automatic reports
 - i. of compliance to citizen charter on delivery of services
 - ii. delay reports
- f. The application should have a module for Management of Digital Signature including issuance, renewal and suspension of Digital Signatures based on the administrative decisions taken by the Govt. of India / Govt. of Punjab. MSI shall ensure using Digital signatures/e-authentication to authenticate approvals of service requests, etc.
- g. e-Transactions & SLA Monitoring Tools
 - i. The MSI should be able to measure and monitor the performance of the deployed infrastructure and all SLAs set out in this RFP. More importantly, it should be possible to monitor in REALTIME, the number of citizens touched through e-Services each day, month and year, through appropriate tools and MIS reports.
 - ii. The Infrastructure Management and Monitoring System shall be used by MSI to monitor the infrastructure (Both IT and Non-IT) hosted at the Data centre and DR site.
 - iii. For monitoring of uptime and performance of IT and non IT infrastructure deployed, the MSI shall have to provision for monitoring and measurement tools, licenses, etc. required for this purpose.
- h. The Smart Jalandhar City Application should have roadmap/capability to integrate with all the key ICT / E-Governance initiatives of the Government of Punjab (GoP) and Govt. of India (GoI), such as Portal Services, Citizen Contact Centres, and Certifying Authorities, etc., as and when required by JSCL.

- i. Complete 'Mobile Enablement' of the 'Smart Jalandhar City System.

Other Key Expectations from the MSI

1. MSI shall engage early in pro-active consultations with all the Competent Authority, Jalandhar City Police and all other key stakeholders to establish a clear and comprehensive project plan, which is in line with the priorities of all project stakeholders and the project objectives.
2. MSI shall plan the redundant bandwidth required for operationalizing each Smart Jalandhar City initiative till the time Competent Authority's own fiber is laid by the MSI as part of the scope of work of this RFP. The bandwidth requirement shall be analysed and procured by the MSI at its own cost / risk
3. MSI will coordinate with the Network Service Provider, shall study the existing fiber layout and existing network in the Jalandhar City to understand the existing technology adopted in each of the following areas (not limited to):
 - OFC/Network/Wi-Fi
 - Surveillance Infrastructure – CCTV Cameras, Data Communication, Monitoring, Control Room and Infrastructure
 - Any other Smart City initiatives envisaged for Jalandhar
4. MSI shall assess existing infrastructure's current ability to support the entire solution and integrate the same with the proposed solution wherever applicable and possible
5. MSI shall be responsible for planning and design of the access network architecture (access controllers, backhaul connectivity, routers, switches, etc.) to meet the technical, capacity and service requirements for all smart Jalandhar City initiatives
6. MSI shall judiciously evaluate the resources and time planned for undertaking the current state assessment, given the overall timelines and milestones of the project.
7. Validate / Assess the re-use of the existing infrastructure if any with Competent Authority site
8. Supply, Installation, and Commissioning of entire solution at all the locations
9. MSI shall Install and commission connectivity across all designated locations
10. MSI shall establish high availability, reliability and redundancy of the network elements to meet the Service Level requirements by providing network on a ring topology.

11. MSI shall be responsible for upgradation, enhancement and provisioning additional supplies of network (including active / passive components), hardware, software, etc. as requisitioned by Competent Authority
12. MSI shall ensure that the infrastructure provided under the project shall not have an end of life during the entire contract period.
13. MSI shall ensure that the end of support is not reached during the concurrency of the contract and 4 years thereafter
14. MSI shall include periodic proactive maintenance of field level equipment's like cameras, junction boxes, switches etc. for O & M period of 4 years
15. Video feeds shall be stored at edge location for one day in case of failure of connectivity
16. All traffic and CCTV surveillance data and metadata required for trend analysis shall be available for at least two years
17. MSI shall ensure compliance to all mandatory government regulations as amended from time to time
18. The MSI shall ensure that all the peripherals, accessories, sub-components required for the functionality and completeness of the solution, including but not limited to devices, equipment, accessories, patch cords (fiber), cables, software, licenses, tools, etc. are provided according to the requirements of the solution
19. Competent Authority shall not be responsible if the MSI has not provisioned some components, sub-components, assemblies, sub-assemblies as part of Bill of Materials in the RFP. The MSI shall have to provision these & other similar things to meet the solution requirements at no additional cost and time implications to Competent Authority
20. All the software licenses that the MSI proposes shall be perpetual software licenses along with maintenance, upgrades and updates (SA) for the currency of the contract. The software licenses shall not be restricted based on location and Competent Authority shall have the flexibility to use the software licenses for other requirements if required. Software assurance may be considered.
21. The MSI shall ensure there is a 24x7 comprehensive onsite support for duration of the contract for respective components to meet SLA requirement. The MSI shall ensure that all the OEMs have an understanding of the service levels required by Competent Authority. MSI is required to provide the necessary MAF (Manufacturer Authorization Form) as per the format provided in the RFP in support of OEMs active support in the project

22. Considering the criticality of the infrastructure, MSI is expected to design the solution considering the RFP requirement of no single point of failure with high level of redundancy and resilience to meet the system uptime requirements
23. MSI shall be responsible for periodic updates & upgrades of all equipment, cabling and connectivity provided at all locations during the contract period
24. MSI shall be responsible for setting up / building / renovating the necessary physical infrastructure including provisioning for network, power, rack, etc. at all the locations
25. MSI is expected to provide following services, including but not limited to:
 - i. Provisioning hardware and network components of the solution, in line with the proposed Competent Authority's requirements
 - ii. Size and propose for network devices (like Router, switches, security equipment including firewalls, IPS / IDS, routers, etc. as per the location requirements with the required components/modules, considering redundancy and load balancing in line with RFP
 - iii. Size and provision the WAN bandwidth requirements across all locations considering the application performance, data transfer, DR and other requirements for smart Jalandhar City initiatives
 - iv. Size and provision the internet connectivity for Service Provider network and Network Backbone
 - v. Size and provision for bandwidth as a service for operations of JICCC till operationalization of network backbone
 - vi. Liaise with service providers for commissioning and maintenance of the links
 - vii. Furnish a schedule of delivery of all IT/Non-IT Infrastructure items
 - viii. All equipment proposed as part of this RFP shall be rack mountable
 - ix. Competent Authority may at its sole discretion evaluate the hardware sizing document proposed by the MSI. The. MSI needs to provide necessary explanation for sizing to the Competent Authority
 - x. Complete hardware sizing for the scope with provision for upgrade
 - xi. Specifying the number and configuration of the racks (size, power, etc.) that shall be required at all the locations.
 - xii. The MSI shall provide for all required features like support for multiple routing protocols, congestion management mechanisms and Quality of Service support
 - xiii. The MSI shall ensure that all active equipment (components) are Simple Network Management Protocol (SNMP) V3 compliant and are available for

maintenance/management through SNMP from the date of installation by a Network Monitoring System

26. MSI shall directly interact with electricity board for provision of mains power supply at all desired locations for any Field Infrastructure solution. The Jalandhar Smart City shall facilitate, if any documentation is required from its side.
27. All existing road signs which are likely to be effected by the works are to be carefully taken down and stored. Signs to be re-erected shall be cleaned, provided with new fixings where necessary and the posts re-painted in accordance with Jalandhar Smart City guidelines. Road signs, street name plate etc. damaged by the MSI during their operation shall be repaired or replaced at the MSI's cost.
28. The infrastructure of existing Traffic signal systems or any other filed Infrastructure including the poles, cantilevers, aspects, controllers and cabling and associated mountings and civil infrastructure as required based on detailed study may need to be dismantled (where ever applicable) and replaced with the new systems proposed and shall be in the scope of MSI. The dismantled infrastructure shall be delivered at the Jalandhar Smart City designated location without damage, at no extra cost.
29. Prior to starting the site clearance, the MSI shall carry out survey of field locations as specified in Intelligent Signalling section. The Jalandhar Smart City shall be fully informed of the results of the survey and the amount and extent of the demolition and site clearance shall then be agreed with the Authority.
30. Lightning Proof Measures:
 - a. The MSI shall comply with lightning-protection and anti -interference measures for system structure, equipment type selection, equipment earthing, power, signal cables laying.
 - b. Corresponding lightning arrester shall be erected for the entrance cables of power line, video line, data transmission cables. All crates shall have firm, durable shell. Shell shall have dustproof, antifouling, waterproof functions; capable to bear certain mechanical external force.
 - c. Signal separation of low and high frequency; equipment protective field shall be connected with their own public equal power bodies; small size/equipment signal lightning arrester shall be erected before the earthing.
 - d. The Internal Surge Protection Device for Data Line Protection shall be selected as per zone of protection described in IEC 62305, 61643-11/12/21, 60364-4/5. Data

line protection shall be used for security system, server data path and other communication equipment.

- e. Data line protection shall be installed as per zone defined in IEC 62305.
 - Type 1 device shall be installed between zone 0B and zone 1.
 - Type 2 devices shall be installed before the equipment in zone 2 and 3.

31. After signing of contract, the Master Systems Integrator (MSI) needs to deploy the team proposed for the project and ensure that a Project Inception Report is submitted to Authority which should cover following aspects:

- a. Names of the Project Team members, their roles & responsibilities
- b. Approach & methodology to be adopted to implement the Project (which should be in line with what has been proposed during bidding stage, but may have value additions / learning in the interest of the project).
- c. Responsibility matrix for all stakeholders
- d. Risk and mitigation plan
- e. Detailed Project Plan, specifying dependencies between various project activities / sub-activities and their timelines.

32. Feasibility Report for all ICT projects mentioned in the report should be conducted. Master System Integrator (MSI) should provide as part of feasibility report the detailed To-Be designs (Junction layout plans) specifying the following:

- a. High Level Design (including but not limited to)
- b. Application architecture documents
- c. ER diagrams and other data modelling documents
- d. Logical and physical database design
- e. Data dictionary and data definitions
 - Application component design including component deployment views, control flows, etc.
 - Field equipment deployment architecture
 - Low Level Design (including but not limited to)
 - i. Application flows and logic including pseudo code o GUI design (screen design, navigation, etc.)
 - ii. Database architecture, including defining data structure, data dictionary as per standards laid-down by Government of India/ Government of Punjab

- Location of all field systems and components proposed at the junctions/other locations,
 - Height and foundation of Traffic Signals and Standard Poles for Pedestrian signals.
 - Height and foundation of Poles, cantilevers, gantry and other mounting structures for other field devices
 - Location of Junction Box
 - i. Location of PoP (Pump Out Plug)
 - Electrical power provisioning
33. Any functionality not expressly stated in this document but required to meet the needs of the organization to ensure successful operations of the system shall essentially be under the scope of the MSI and for that no extra charges shall be admissible.

SPECIFIC SCOPE OF SERVICES

4.1 Jalandhar Integrated Command Control Centre (JICCC), DC & DR

As part of the project, a common Jalandhar Integrated Command Control Centre (JICCC) shall be implemented in around ~ 5000 Sq. Ft area. The location where Viewing centres/ Video feeds as required shall finalized at the times of system study conducted by MSI.

Jalandhar Integrated Command Control Centre (JICCC)

The JICCC shall provide a comprehensive system for planning, optimizing resources and response pertaining to the standard functions of the concerned authorities. With a view of enabling varied and respective stakeholders to operate specified Smart City Components, it is proposed to build Jalandhar Integrated Command Control Centre (JICCC), which will cater to the City Operations, City Surveillance, Emergency Response System, Helpdesk and the components.

While the entire Smart City initiative is built around various components of smart interventions for different citizen centric services and facilitating administration, an Integrated Command Control Centre or JICCC brings all the outputs onto a single platform and give an integrated view. This works as a monitoring system that helps in decision making process a lot simpler and comprehensive. It acts as a support mechanism to the city administration/authorities in their daily routine activities as well as during exigency situations. This dynamic response to situations, both pre-active and re-active will truly make the city operations “SMART”.

Apprehending the huge volume of information generation with the help of Pan City ICT infrastructure, it is envisaged to have a centralized command control centre. All the smart solutions, network, components will converge at the centralized command control centre. Jalandhar Integrated Command Control Centre (JICCC) involves leveraging on the information provided by various departments and providing a comprehensive response mechanism for the day-to-day challenges across the city. JICCC shall be a fully integrated, web-enabled solution that provides seamless incident -response management, collaboration and geo-spatial display. Additional third party modules can be integrated as per solution requirements.

1. The JICCC shall facilitate the viewing and controlling mechanism for the selected field locations in a fully automated environment for optimized monitoring, regulation and enforcement of services. The

- JICCC shall be accessible by operators and concerned authorized entities with necessary role based authentication credentials
2. Activities at the JICCC will comprise of monitoring services, incident management and response as per the Standard Operating Procedures (SOPs) with defined escalation procedures.
 3. The JICCC will manage and monitor entire the project and services. All the information and data collected through various components of the smart city project will be viewable through a centralized Application.
 4. Integrated Dashboard for entire project – JICCC will comprise of a centralized dashboard for entire smart city project for the reporting and viewing of all the project components and key performance indicators of systems such as CCTV Camera Surveillance System, Intelligent Signalling, Smart Water Quality Monitoring, Environmental Monitoring etc. through a single interface.
 5. JICCC will act as the centralized monitoring and decision making hub for managing Smart Applications and related Infrastructure project activities. Various smart elements will be able to use the data and intelligence gathered from operations of other elements so that civic services are delivered lot more efficiently and in an informed fashion.
 6. The benefits of the JICCC will be measured from two perspectives:
 - In times of disaster – The solution will improve the response time, coordination amongst various agencies and faster restoration of services post disaster.
 - In day-to-day non-emergency scenarios – The solution will improve the response time of Municipal Corporation towards citizen complaints, which in turn will lead to citizens using the system more frequently. This will also enable the various departments to offer better services to citizens including, utilities, security, traffic, etc.

Various Components of JICCC

The Integrated Command and Control Centre shall comprise of:

- a. Data Centre & ICCC
- b. Video Wall & Controller system
- c. City Operations Platform
- d. GIS - PMU
- e. Emergency Response Control Centre
- f. Data Analytics Centre for all the Smart City Operations
- g. Integrated Dashboard - Provision for generating configurable reports through dashboard and also real time monitoring

- h. Standard Operating Procedure Tool
- i. Helpdesk, Technical and Operations Staff
- j. Furniture, Fixtures, Operator Workstation and accessories
- k. Conference / Situation Room

The Jalandhar Integrated Command Control Centre (JICCC) will be the nodal point of availability of all online data and information related to smart services. It will be a full-fledged system equipped with all the operation rights to its specified users. This will have integration with various components with data feed view and sharing. It will also have management console to perform all the operations

The Component Modules

The scope will entail design, development, installation, operation and maintenance of the following components JICCC:

- Centralized Command Control Room
- Data Centre to cater to all Smart components of Smart City
- City Surveillance
- ITMS
- Body cameras
- Environmental sensors
- GIS Integration
- Mobile Application for Smart Solutions
- Disaster Management
- Emergency Response System
- Data Analytics Centre
- Helpdesk - Common

Viewing Centres:

Viewing centres shall have the following:

- LED screens for viewing and controlling video feeds
- Work station, Connectivity to Central Integrated Command Control Centre

- Partition for Viewing centre & Biometric access control with air conditioner

The detailed activities to be undertaken by the Master System Integrator (MSI) during the phases at JICCC and viewing canters as applicable based on scope of work:

1. Pre –Implementation Phase

- Conducting site survey, obtaining necessary permissions, developing functional & system requirements, standard operating procedures, departments involved in operations for communications etc.
- Assessment of IT Infrastructure and Non IT Infrastructure requirements, assessment of business processes, assessment of software requirements, assessment of integration requirement, assessment of connectivity requirement at all locations.
- Formulation of solution architecture, detailed design of smart city solutions, development of test cases (Unit, System Integration and User Acceptance).
- Assessment and study of use cases and development of SOPs for all use cases with respective department

2. Implementation Phase

Integrated City Operations Platform (ICOP) shall be procured and configured data centre by MSI. MSI shall install, configure, integrate and manage all the applications in data centre and enable holistic approach for day to day operations from JICCC.

- Helpdesk setup, Data Analytics Centre setup, physical infrastructure setup, procurement of equipment, edge devices, COTS software (if any), licenses
- IT and Non IT Infrastructure installation, development, testing and production environment setup.
- Software Application customization (if any), development of bespoke solution (if any), data migration, integration with third party services/application (if any) and APIs shall be exposed for integration
- Preparation of User Manuals, training curriculum and training materials.
- Role based training(s) on the Smart City Solutions. g) Integration of solutions with JICCC.

- Facilitating user acceptance testing and conducting the pre-launch security audit of applications.
- User training and roll-out of solution.
- Integration Requirements:
 - i. Integration of the solution with existing / standalone systems.
 - ii. Integration of the solution with PPP components / other components being implemented separately as part of Smart City project.
 - iii. Integration with any and all other future components, which are to be implemented during the execution of the MSA contract.
 - iv. Develop provisions for a scalable system which can integrate with more devices of the same kind (as those deployed today) and can integrate with future applications and sensors through open standards and data exchange mechanisms.

3. Post Implementation Phase

- Deploying manpower for solution maintenance and monitoring support which includes change request management, bug tracking and resolution, production support, performing version and patch updates in O&M
- Deploying man power for Data Analytics Centre and management for the O&M period and showcase the KPIs of Smart city components
- Annual technical support for all hardware and software components for the O&M period.
- Additional SOPs and detailing of SOPs and their optimization is to be performed during operation and maintenance phase.
- Optimizing field infrastructure for better operations, e.g., shifting of cameras or changing their alignment / angle.
- Identifying, scripting and implementing the automation required to manage the IT during O&M phase.
- Continuously study the additional requirements, fine-tune the applications and implement features that will assist the line departments in carrying out the operations thereby stabilizing the overall infrastructure within 3 months of Go Live.
- Preventive, repair, maintenance and replacement of hardware and software components as applicable under the warranty and AMC services during the contract period.

- Provide a centralized Helpdesk and Incident Management Support till the end of contractual period.
- Recurring refresher trainings for the users and Change Management activities.
- Develop a capacity building schedule and enable capacity building for the designated officials.

The Component Scope

Various components of the project, including expected system users, are as below and also depicted in the component architecture diagram below.

1. Field IT Infrastructure Layer
2. Network Layer
3. Data Centre Layer
4. Application Layer
5. Integration Layer
6. Command and Communication Centre Layer
7. Security Layer

This component architecture is indicative in nature and is given to bring clarity on the overall scope of project and its intended use. The MSI is expected to carry out the detail requirement analysis and finalize the technical architecture in consultation with authority and its consultants. The architecture of the complete network of smart elements is as follows.

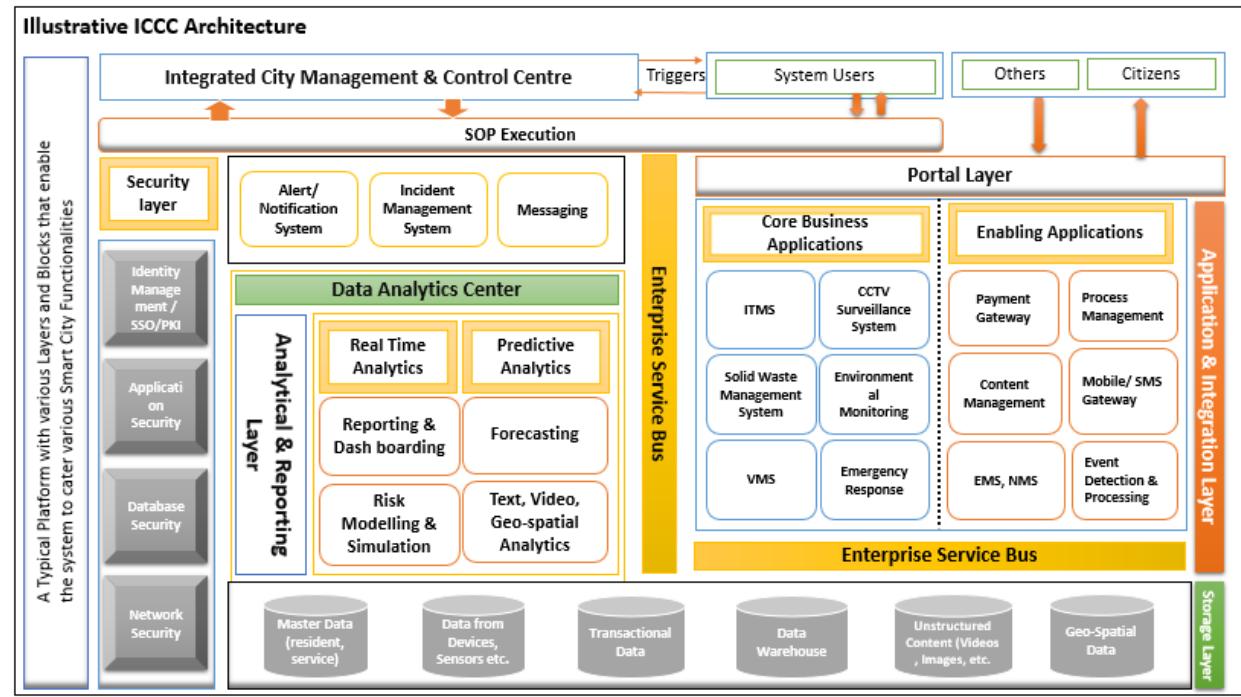


Figure: Logical diagram of JICCC

1. **Street IT Infrastructure Layer** –The sensor layer will help the city administration gather information about the ambient city conditions or capture information from the edge level devices like GPS devices, cameras, etc. MSI is expected to deploy multiple environmental sensors across the city, to measure ambient conditions such as light intensity, temperature, water level (for chronic flood spots), air pollution, noise pollution and humidity, etc. The output field devices layer will contain display devices or bi-directional (input & output) devices connected to the network which will be used by citizens to consume - and for administrators to provide - actionable information. Such field devices include digital messaging boards, environmental data displays, PA systems, surveillance cameras among others.
2. **Network Layer** – The secured network layer will serve as the backbone for the project and provide connectivity to gather data from sensors and communicate messages to display devices and actuators. The MSI will size the bandwidth required for the overall solution, and supply and install the edge devices to utilize the network.

Network Architecture:

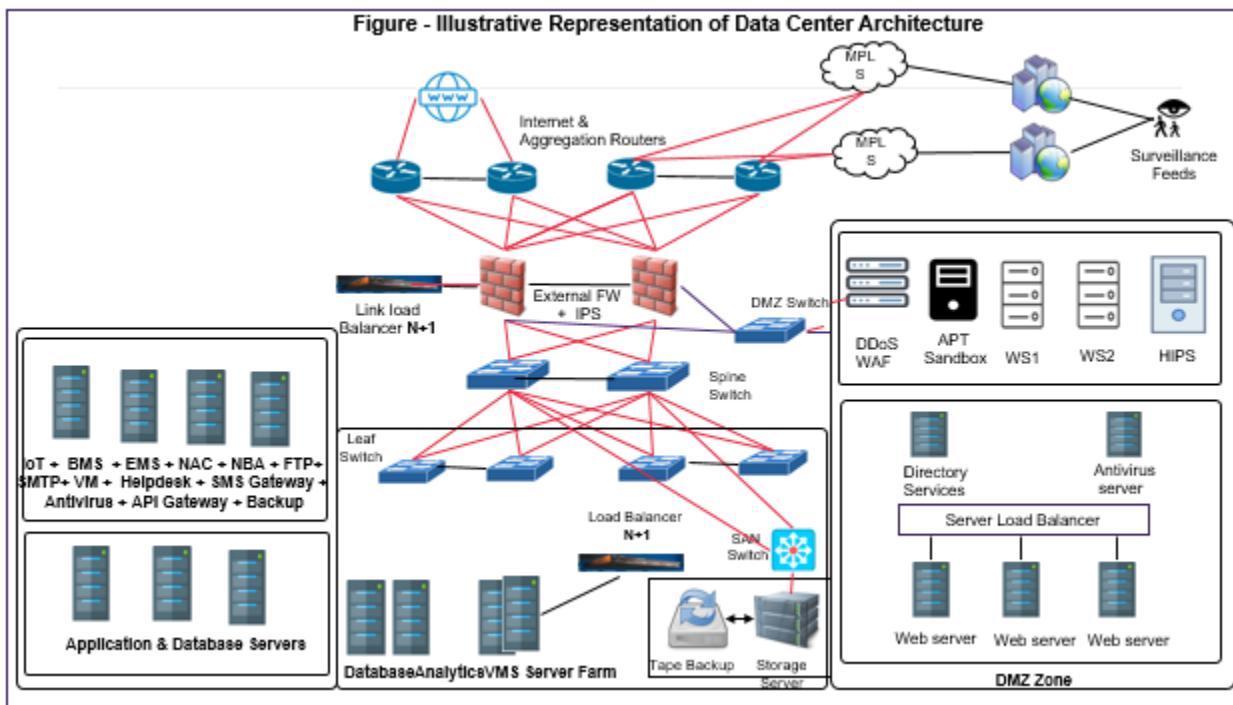


Figure: Illustrative High Level Network Architecture Diagram

3. **Data Centre Layer** – The data centre layer will house centralized computing power required to store, process and analyse the data to decipher actionable information. This layer includes servers, storage, ancillary network equipment elements, security devices and corresponding management tools. A disaster recovery site, which includes servers, storage, network equipment and security management systems will be used in case of fall back mechanism for the data centre.
4. **Application Layer** – The applications layer will include applications that interface and control the street infrastructure, enterprise management system to monitor and manage all IT infrastructure and street infrastructure deployed in the city, and surveillance applications.
5. **Integration Layer** – While aspects of ambient conditions within the city will be gathered through various sensors deployed as a part of the solution, some city specific data will come from other government and non-government agencies. It is through the integration layer – that data will be exchanged to and from the under lying architecture components and other data from system developed by government (such as police department, meteorological department, street lights department, water department, irrigation department, transport organizations within Jalandhar, etc.) and non-government agencies.

6. **Command and Communication Centre Layer** – The command centre will enable citizens and administrators alike to get a holistic view of city conditions, and make informed decisions.

7. **Security Layer** – As ambient conditions, actuators and display devices are now connected through a network, security of the entire system becomes of paramount significance and the master system integrator (MSI) will have to provide: Infrastructure security, Network security, Identity and Access Management, and Application security.

GIS Data Creation and Integration

One of the goals of the smart city initiative is to create a single integrated solution for managing citizen services using GIS as a base platform.

The broad scope of MSI shall be:

- Identify the GIS layers with required attributes for day to day operations for each of the component of the RFP as applicable
- Collection of required GIS/CAD data from various line departments and conversion to GIS ready format
- Mapping of ICT related information for Smart city assets with detailed attribute details
- Provide the required GIS data in standard format for Application Development
- Responsible to procure any server based GIS License as per solution
- To provide necessary API/Inputs to MSI to integrate various City wide applications.
- Creation GIS data layers on GIS Map

General Requirements

- MSI shall be responsible for compliance with all local standards and certifications, including building, electrical and occupational requirements;
- MSI shall integrate JICCC with various other city systems and infrastructures. MSI shall coordinate with all the stakeholders of these city systems for integration purposes;
- MSI shall be responsible for setting up the required software platform and interfacing JICCC with other city components;

- Define SOPs with the Authority or its representative for the operations to ensure that JICCC systems are configured to support the operational procedures;
- Creation of KPIs and dashboards as per the requirement of the Authority
- Build and certify JICCC as per ISO 27001:2011 standards.

The Key Performance Indicators

1. The vision of the Jalandhar Integrated Command Control Centre (JICCC) is to have an integrated view of all the smart initiatives undertaken by Authority with the focus to serve as a decision support engine for city administrators for day-to-day operations or during exigency situations. This dynamic response to situations, both pre-active and re-active will truly make the city operations “SMART”.
2. JICCC involves leveraging the information provided by various departments and providing a comprehensive response mechanism for the day-to-day challenges across the city. JICCC shall be a fully integrated, Web-Based or Authority-Server integrated with web based access/services, solution that provides seamless incident – response management, collaboration and geo-spatial display. Additional 3rd party modules may be integrated as per solution requirement.
3. JICCC shall facilitate the viewing and controlling mechanism for the selected field locations in a fully automated environment for optimized monitoring, regulation and enforcement of services. The smart city operations centre shall be accessible by operators and concerned authorized entities with necessary authentication credentials.
4. Various smart elements are able to use the data and intelligence gathered from operations of other elements so that civic services are delivered lot more efficiently and in an informed fashion.
5. JICCC will provide 24*7 City Surveillance System for effective management of the city.
6. JICCC shall leverage state of the art technology to effectively manage Road Traffic, and
7. JICCC should be able to integrate with various utility systems such as ITMS, Emergency Response System etc.

The Technology Principles:

The following principles must be adopted in the design and development of the JICCC:

- a) Requirements-based Change – Changes to technology and applications are made only in response to changes in processes / service needs.
- b) Controlled Technological Diversity – Technological diversity is controlled to minimize the costs of maintaining expertise in and connectivity between multiple processing environments.
- c) Adherence to Standards – Software and hardware should conform to all mandatory and necessary standards.

The standards help ensure consistency, thus improving the ability to manage systems and improve user satisfaction, and protect existing IT investments, thus maximizing returns on investment and reducing costs. Standards for interoperability, additionally, help ensure support from multiple vendors for their products, and facilitate supply chain integration.

The Processes:

The JICCC is the centralized component that holds all the smart city projects together and gives the decision makers a complete picture of the issues currently being faced by different stakeholders. The supporting process that are to be designed and executed within the JICCC are:

- a. Definition of role-based access mechanism
- b. Definition, logging and periodic review of standard operating procedures
- c. System health monitoring for each of the smart city components integrated with JICCC
- d. Periodic review of risks identified under monitoring and mitigation plan
- e. System backup and archival process f. Audits and (Re)certifications.

Types of Operations:

A. Normal Operations

Normal operation is when the services function as per pre-planned operation schedule or methodology. Under normal operating conditions, various members of Operations team shall coordinate their activities and exchange information through voice and data communications systems about the equipment /

facilities under their supervision to facilitate a safe and secure arrangement throughout the entire Jalandhar City. Under the normal condition, the operations team shall continuously supervise the main assets and identify any fault, anywhere in system promptly. Operation team shall isolate faulty element and operate the system in a manner to arrange alternatives wherever appropriate alternative is possible (element redundancy, rerouting of services, alternate feeding path etc.). Faulty elements are further referred to appropriate team for respective corrective action. The JICCC Framework shall be able to enable faster isolation of faulty elements & identification & implementation of inbuilt alternatives in system.

B. Degraded Operation

Degraded modes of operation occur when certain systems fail to meet the levels of service expectation. In such scenario the applicable Standard Operating Procedure (SOP) would be followed

For example: Various failures in power installation may affect the distribution of power in various sectors of the Jalandhar City. Load shedding need to be planned looking at many aspects, few of the incidents/situations may include Student Exams, Hospitals and Industries.

C. Emergency Operation

In a Smart City, the emergency situations, need to be averted beforehand. Emergency operations are enforced in case of an unforeseen or abnormal situation, when it's not possible to carry on the services. An emergency or disaster is a sudden or great calamity leading to deep distress affecting men and machinery. Many of the accidents / incidents like an act of vandalism, terrorist attack, an accidental fire, critical system failure, force majeure, etc. may lead to crisis / disaster. In cases of disasters, the main objective is to disperse the affected persons, as early as possible, from the affected site of occurrence and avoid loss of life and properties. Management of such situation requires sharing of clear and accurate information and necessary actions shall be initiated without any delay to ensure the restoration of normalcy.

- This requires seamless & timely sharing of information amongst multi-disciplines (viz. Traffic, Parking, Helplines, Smart Lights, Signal & Telecommunication, etc.) involved in Operations
- Necessitates that appropriate actions are initiated without any delay and the situation is tackled in the most appropriate and efficient manner, so that distress is relieved expeditiously.

Thus, for effective management of such scenarios, it is preferable to have visibility and ability to manage critical disciplines at one place. The JICCC framework shall support Automation of Disaster Management Procedure. The CCTV Cameras throughout the City and analytical tools would perform the emergency operations during such situations. The following table is tentative space requirement calculated for JICCC.

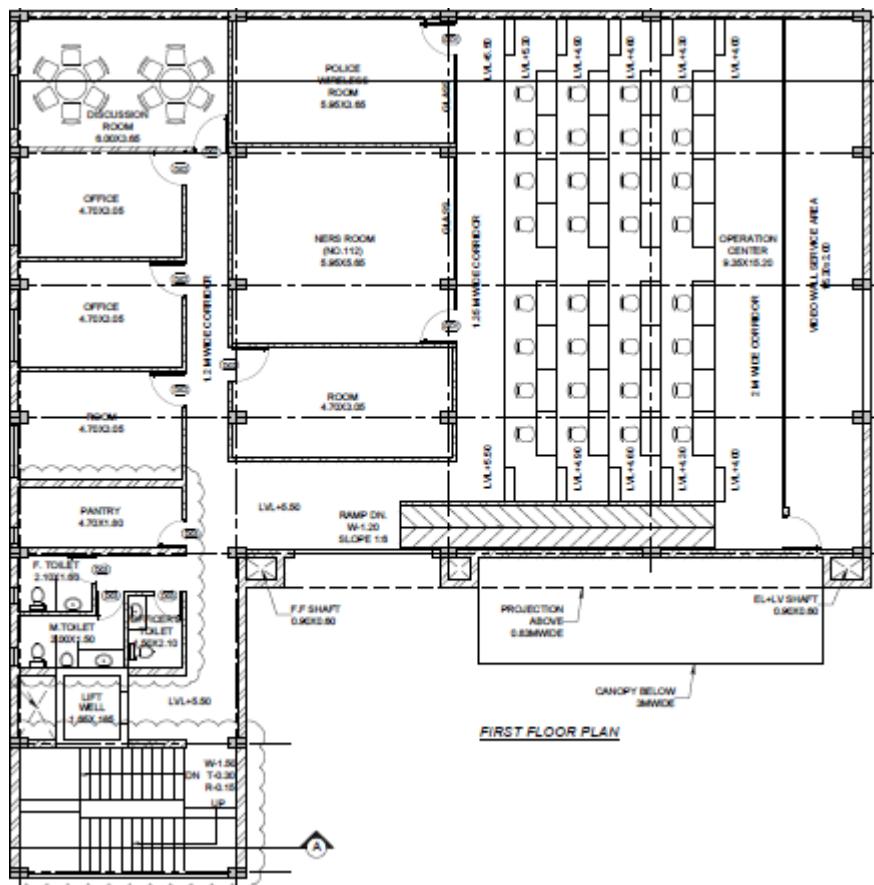
ICCC BUILDING-FINISHES SCHEDULE			
ROOM NO.	ROOM NAME	ROOM AREA(SQM)	ROOM AREA(S.ft)
COMMON AREAS			
C01	STAIRCASE	22.0	237
C02	LIFT LOBBY	6.0	65
C04	M. TOILET	5.0	54
C05	F. TOILET	3.5	38
C06	OFFICER'S TOILET	3.0	32
C07	PANTRY	8.0	86
GROUND FLOOR			
G01	ENTRANCE STEPS AND RAMPS		
G02	RECEPTION CUM LOBBY	30.0	323
G03	TRAININIG AREA	82.0	883
G04	DCP'S ROOM	17.0	183
FIRST FLOOR			
F01	ROOM 01	13.5	145
F02	ROOM 02	21.0	226
F03	OFFICE 01	13.5	145
F04	OFFICE 02	13.5	145
F05	DISCUSSION ROOM 01	21.0	226
F06	NERS ROOM(NO.112)	37.5	404
F07	POLICE WIRELESS ROOM	24.0	258
F08	OPERATION CENTRE	142.0	1528
SECOND FLOOR			
S01	C.P ROOM WITH DISCUSSION AREA	33.0	355
S02	C.E.O ROOM WITH DISCUSSION AREA	33.0	355
S03	C.P' S TOILET	2.5	27
S04	C.E.O'S TOILET	2.5	27
S05	C.P STAFF	13.5	145
S06	C.E.O STAFF	13.5	145

S07	DISCUSSION ROOM 02	30.0	323
TERRACE			
T01	TERRACE		
T02	ROOF SHEET		

Site Preparation for JICCC including Data Centre

The Integrated Control and Command Centre will be proposed to be setup at Police Line, Jalandhar. Basic civil structure shall be provided by Jalandhar Smart City. Civil, Interiors and Electrical Infrastructure along with the safety infrastructure forms the basic pre-requisite for the setup of JICCC shall be done by MSI. An indicative layout is presented below:

The civil construction is not scope of the MSI as part of this RFP. The MSI shall be responsible for minor site preparation works related to the equipment under its scope along with the installation and setup of facility management systems like Building Management System, Fire Alarm and Repellent System, CCTV System, Access Control System, etc. However, the MSI shall be required to coordinate extensively with the civil contractor for preparation of the JICCC site according to its requirements.



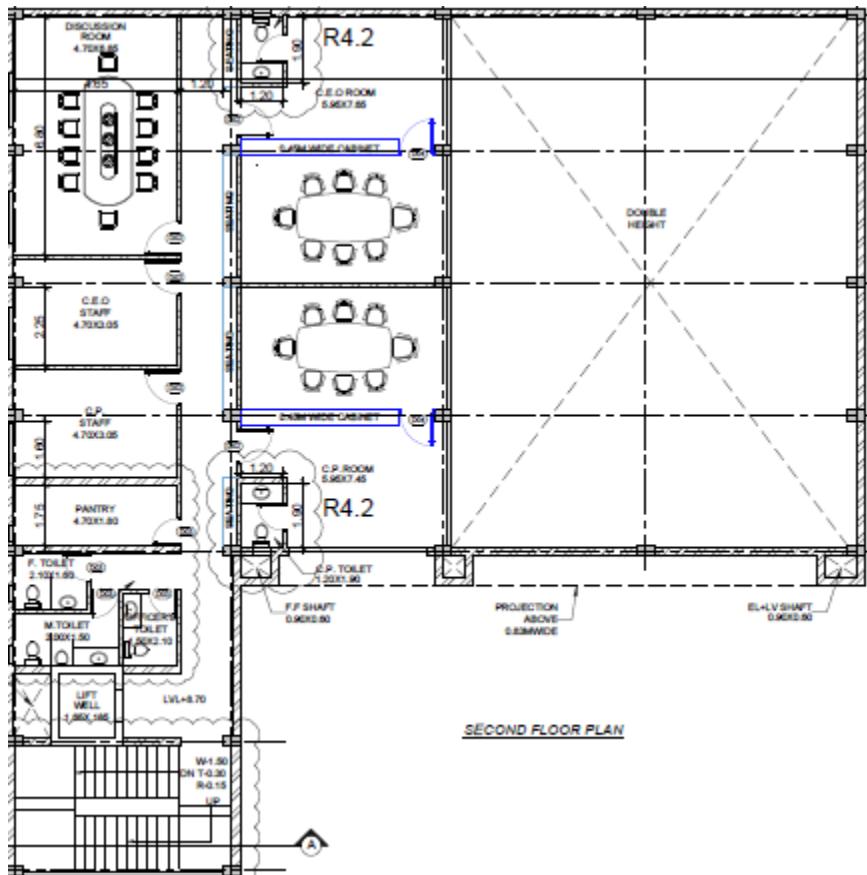


Figure: Illustrative layout of Command Control Centre

The following shall be the responsibility of the MSI with regard to JICCC Non-IT Infrastructure:

- A. UPS Requirements and Features: UPS system shall provide a redundant power supply to the following needs:

- Servers and important network and storage equipment
- Access control, Fire Detection & suppression system and surveillance system

The system shall be automatic with power supply from the mains and automatic switchover

to DG set as secondary source.

- B. Diesel Generator Set: MSI has to specify the technical specifications based on the requirement. The MSI shall be responsible for regular operations and maintenance of the DG set. The MSI shall be responsible for but not limited to:

- Fuel

- Preventive maintenance
 - Corrective maintenance
 - AMC, if any
 - Replacement of any parts etc.
 - Security and Theft during the project
- C. Fire Detection and Suppression System: The facility shall be equipped with adequate and advanced Fire Detection and Suppression system. The system shall raise an alarm in the event of smoke detection. The system shall have proper signage, response indicators and hooters in case of an emergency. The system shall be based as per NFPA standards. The facility is to be equipped with gas based (Suitable for Data centre environments) fire suppression system appropriately sized for the given size of the Data centre and JICCC.
- D. Building Management System: Building Management System shall be implemented for effective monitoring, management, control and integration of various building systems such as HVAC, lighting, electrical, fire detection and suppression system, CCTV system, Access Control System etc. over a single platform. BMS shall perform various functions such as data collection and archival, alarm and event management, trending, reports and MIS generation, preventive maintenance etc. Design-Build of the BMS shall be under the scope of MSI. IO summary and other BMS related provisions shall fall under the scope of the MSI.
- E. Access Control System: The Biometric/Access card based Access Control System shall be deployed with the objective of allowing entry and exit to and from the premises to authorized personnel only with appropriate door locks and controller assemble. The system deployed shall be based on proximity as well as biometric technology for critical areas and proximity technology for non-critical areas.
- F. CCTV System: The MSI shall provide CCTV system within the Data centre and JICCC on 24X7 bases. All important areas of the Data centre, JICCC along with the non-critical areas like locations for DG sets, entry exit of Jalandhar Integrated Command Control Centre (JICCC), Entry and Exit of building premises need to be under constant video surveillance. Monitoring cameras shall be installed strategically to cover all the critical areas of all the respective locations.
- G. Water Leak Detection System: The Water Leak Detection System shall be installed to detect any seepage of water into the critical area and alert the security control room for such leakage. It shall consist of water leak detection cable and alarm module. The cable shall be installed in the ceiling and floor areas around the periphery.
- H. Rodent Repellent: The entry of rodents and other unwanted pests shall be controlled using non-chemical, non-toxic devices. Ultrasonic pest repellents shall be provided in the false flooring and

ceiling to repel the pests without killing them. However, the MSI shall conduct periodic pest control using chemical spray once in a quarter as a contingency measure to effectively fight pests.

All the relevant certificates in support of the following listed requirements to be submitted along with the bid

1. BIFMA X5.5, OHSAS 18001, ROHS, ASTM E84, Green guard Certified certifications and Jalandhar Seismic Zone 4 qualified control desk.
2. Control Room should be designed as per ISO 11064 and HFE norms, relevant Report & Control centre animation of minimum 60 seconds must be submitted along with the BID.
3. Control Room wall panelling and ceiling must be 100% modular for future technological expansions, OEM to submit an undertaking for the same.
4. Wall panelling and Ceiling tiles must be a combination of perforated and non-perforated tiles to have Sound absorption.
5. Wall Panelling and Ceiling must be seismically tested & certified for Jalandhar Seismic Zone (4) Vibrations and ROHS certified. Valid report from government approved test lab (for Seismic test) to be enclosed with the bid. Control Room Interiors must be Green guard certified to reduce health hazards because of interior finishes.
6. Wall Panelling and Ceiling tiles must be Class A fire rated certified for surface burning characteristics as per ASTM e84 or equivalent. Certificate to be attached with the bid.
7. For Control room interiors Wood, Gypsum, POP and paint etc. shall be deemed unacceptable to ensure 10 year's maintenance free working environment. OEM to submit an undertaking for the same

Data Centre (DC) & Disaster Recovery (DR)

The Jalandhar Smart City intends to establish a Data Centre (DC) in the premises of the JICCC. It will be the obligation of the MSI to implement and commission the DC at the selected location as approved by the Authority.

The MSI is required to implement all the hardware/software and related items for the data centre as per the smart city solution including SLA monitoring and Help desk management, in a Tier III Data Centre complying with standard guidelines as per Telecommunications Infrastructure UPTIME/TIA-942.

The Data centre shall be available for 24x7x365 operation. The smart city infrastructure shall have built in redundancy and high availability in compute and storage to ensure that there is no single point of failure. The MSI shall submit to Authority adequate documentation/ evidences in support of the choice of the data centre to meet the project requirements.

Data Centre

1. MSI is required to co-locate all the hardware/software and related items for the smart city infrastructure including SLA monitoring and Help Desk Management, in a Tier III or above data Centre complying to standard guidelines as per Telecommunications Infrastructure UPTIME/TIA-942.
2. The Data centre shall be available for 24x7x365 operation.
3. The smart city infrastructure shall have built in redundancy and high availability in compute and storage to ensure that there is no single point of failure.
4. The MSI is free to take the colocation services from any existing data centre located within India (preferably in the same city where possible) which meets the prevailing data centre standards, since this is one of the most critical components of the smart city infrastructure. However, the system SLA as defined in the RFP to be met solely by the MSI.
5. The MSI shall submit to Authority adequate documentation/ evidences in support of the choice of the data centre to meet the project requirements.
6. Min Guiding factors for selection of the Data Centre: Following are the benchmark requirements which should act as guiding factors for the MSI to select and propose the locations for the Data Centre
7. There should be dedicated rack space available in the data centre for the entire Smart City Project Infrastructure.
8. Access to the Data Centre Space where the Smart City Project Infrastructure is proposed to be hosted should be demarcated and physical access to the place would be given only to the authorized personnel
9. Racks to be caged.
10. Smart City Data Centre should be at least a Tier III Data Centre as per Telecommunications Infrastructure Standard for Data Centres and should be 27001 Certified. The required certification to be enclosed along with the technical bid response.
11. It should have access control system implemented for secured access.

12. Indoor CCTV Cameras would be required to be installed to monitor the physical access of the system from remote location
13. Physical Access to the building hosting Data Centre should be armed and it must be possible to even depute police personnel for physical security of the premises.
14. Min 90 days Data Backup of the video feeds and the transaction data for min 1 year shall be stored within the Data Centre Infrastructure preferable in a cost effective and innovative manner.
15. In case the data centre services are to go down due to any unforeseen circumstance, the Command Centre should have access to the video feeds of previous 90 days and the transaction data for min 1 year from this data backup facility.
16. Access logs to be stored for the entire duration of contract and handed over to Authority upon termination/expiry of the contract.
17. MSI should optimize the overall system within intranet and internet communications during maintenance phases based on utilization of applications and submit reports accordingly
18. Enterprise Management System and Network and Security Management Solution.
19. Centralized System for Security Solution.

Functional Specifications - DC/ DR

Data Centre specifications:

1. Design Standard: Tier-III or above
2. The availability of data must be guaranteeing to 99.982% availability.
3. Receiving Power: Commercial power substation next to DC
4. UPS: UPS system with N+N redundancy
5. Generator: Gen-set with N+1 redundancy
6. Power Provision: Dual power feed, PDU sources to each rack, Power supply to a rack as per requirement

Server Infrastructure Zone

This zone shall host servers, server racks, storage racks and networking components like routers, switches to passive components. All the Data centre LAN connections shall be provided through switches placed in this area. MSI shall be required to undertake a detailed assessment of the space and size of the building proposed by Authority for JICCC with co-hosted data centre with respect to their

system requirements and if required may propose a suitable solution. Access to this zone, where the surveillance project IT infrastructure is hosted, shall be demarcated and physical access to the place shall be given only to the authorized personnel. Indoor CCTV Cameras shall be installed to monitor the physical access of the system from remote location.

UPS and Electrical Zone

This zone shall house all the Un-Interrupted Power Supply units, Main Power Distribution Units (PDUs) to feed the components such as PAC, UPS, lighting, fixtures etc. This shall also house all the batteries accompanying the UPS components. As these generate good amount of radiation, it is advised to house these components in a room separate from server infrastructure zone.

Functional requirements:

Integrated Command Control Centre

The following are the indicative functional requirements of JICCC required for smart city operations. MSI is expected to use all the functionalities of IOT platform/City Operations Platform for holistic management of Smart city applications and integrate applications within the scope of this RFP and ‘other applications’ mentioned which shall be taken up as separate projects.

Proposed components/requirements of Integrated Command and Control Centre for Jalandhar city:

1. Integrated Command and Control Application.
2. Unified Communications and Contact Centre.
3. Integrated Dashboard – Provision for generating configurable reports through dashboard and also real time monitoring.
4. Video Wall & Controller System.
5. Operator Workstation and Accessories.
6. Alerting System.
7. Integration with Third Party Shared Services.
8. Helpdesk Service and Call centre for public grievance redressal system on 24X7 basis.
9. Necessary Civil, Electrical work including furniture, including Air-conditioning for Data Centre, and Command & Control Centre.

Sl. No	Minimum Specifications
--------	------------------------

1	JICCC shall provide a holistic and real time view of all city operations on a video wall along with individual views on operator workstations
2	JICCC shall enable monitoring, control and automation of various city operations in order to ease and organise city operations.
3	JICCC shall enable system and cross system analytics through smart city platform in order to make city operations intelligent
4	JICCC shall leverage information provided by multiple city systems in order to provide an integrated, seamless, proactive and comprehensive response mechanism for day-to-day city operations and challenges
5	JICCC shall provide real time dashboards, visualizations, KPIs, historical trending, analytics and other intelligent features to facilitate city operations analysis by city administrators.
6	JICCC shall provide alarm features for immediate notification to city administrators in case critical event occurs in the city
7	The Digital Content Management System (DCMS) provided as part of JICCC will manage and drive all visual content to the various display devices, including the video display wall. All city systems will display content through the DCMS
8	The operators will also manage and control various systems, and dispatch to system maintenance staff. They will be responsible for monitoring and managing all integrated city systems out of the JICCC.
9	All workstation units of the operator workstations shall be installed at the central rack rooms so that space at the JICCC operator desks can be optimized. The operators and other personnel
10	Direct connections and data from devices / systems shall include real-time city systems data, KPIs and video feeds from CCTV cameras.

Facilities Management and Building Management Systems (BMS)

11	Interface with the Building Management Systems (BMS) installed in JICCC for monitoring and control of all the building systems and parameters available through the BMS.
12	Interface with all the BMS or IP enabled fire alarm system for monitoring of essential parameters
13	Log calls / jobs on the helpdesk database utilizing helpdesk software (inquiries may be received by telephone, facsimile, email or in person).
14	Allocate and dispatch work orders to directly employed (or subcontracted) maintenance team
15	Take ownership of the Preventative Maintenance (PM) schedule and track reactive maintenance (RM) service requests.
16	Track progress of PM and RM service requests against pre-determined KPIs
17	Report back to Authority and contract staff on progress of each PM and RM service request and close out service requests when completed
18	Maintain asset information
19	Update site specific facilities management files and other documentation for helpdesk compliance
20	Dispatch of emergency services

City Security

21	Accurately and promptly observe, monitor and operate closed circuit television (CCTV) cameras and related equipment, and, where necessary direct Police Officers to real time incidents
22	To identify, report, and record anything suspicious, in line with JICCC procedures
23	To operate the cameras and equipment effectively ensuring that best possible evidential quality images are recorded
24	To ensure all equipment is functioning correctly, carry out equipment checks as required and report all faults to relevant personnel, carry out basic non-technical system maintenance as required

Traffic Management	
25	Recognize, identify and monitor the infracting vehicles in real-time / off-line mode for various violations at junctions and in streets
26	The system shall have the ANPR Non-intrusive modes of enforcement on traffic light violation and Speed
27	The system at the JICCC should be integrated with the E-Challan system to enable E-Challan generation, payment and billing process
28	Public Address (PA) System is disseminate the information to the citizen particularly emergency situation messages to reach quickly
29	The system should be able to integrate other network PA systems or third party application systems where the alerts are generated to broadcast messages at JICCC
30	The system should be able to generate various statistics, reports & MIS from time to time at JICCC.
31	Variable Message Sign (VaMS) board shall provide feedback to the JICCC on the VaMS status of Active / Inactive.
32	The system should maintain the history of messages archived for future reference and analysis
33	The ATCS & ATCC system shall provide multiple interfaces to share the data seamlessly to different sub systems e.g. Signaling system to configure and determine the traffic signal duration based on the traffic congestion, weather conditions, traffic pattern and other factors
34	The system at the JICCC shall feed the traffic density information to the associated junctions of critical junction subsystem to determine the expected traffic from its previous junction and traffic signal duration
Environmental Sensors	
35	Monitor key inputs from pollution sensors, noise sensors, particle sensors, etc.
36	Create awareness within the city based on dynamic inputs received from sensors and display output to various interfaces including city application, multi-services digital kiosks and Digital Display Screen (DDS).
37	Inputs to various regulations and permissions as needed in terms of carbon content, and content of other particles and gases in around Jalandhar
Smart Mobility & Vehicle Location Systems	
38	CAD/AVL System: Vehicle location monitoring for the following vehicles shall be done at JICCC:
	SWM vehicles
	PCR Vans

City Operations Platform (COP):

Sl. No	Functions	Minimum Specifications
1	Solution & Platform	<p>The Command & Control solution should be implemented and complied to the industry open standards based Commercial-of-the-shelf (COTS) products.</p> <p>The Platform should support distributed deployment architecture</p>

Sl. No	Functions	Minimum Specifications
		The solution should be providing option to connect legacy system through APIs with either read, write or both options. It should connect diverse on premise and/or cloud platforms and makes it easy to exchange data and services between them.
		The system shall allow seamless integration with all of the department's existing and future initiatives (e.g. open source intelligence, situation management war room, etc.)
		System must provide a comprehensive API (Application Programming Interface) or SDK Software Development Kit) to allow interfacing and integration with existing systems.
		Software (Application, Database and any other) must not be restricted by the license terms of the OEM from scaling out on unlimited number of cores and servers for future expansion.
		The platform should be able to normalize the data coming from different devices of same type (i.e. different lighting sensors from different OEMs, different energy meters from different OEMs etc.) and provide secure access to that data using data API(s) to application developers
		Platform should be able to correlate and handle multiple data streams, while providing real-time logic, analysis and routing applied to incoming data streams and aggregating data over time
		The platform should be able to integrate with any type of sensor platform being used for the urban services irrespective of the technology used.
		Must have built-in fault tolerance, load balancing and high availability & must be certified by the OEM.
		The platform shall provide enhanced situational awareness using IoT elements and ability to replay the scenarios
		The platform should be able to combine data from various sources and present it as different views tailored to different operator's needs and provide Common Operational Picture
		The Platform should provide tools for users to collaborate in real-

Sl. No	Functions	Minimum Specifications
		<p>time using instant messaging features</p> <p>The Platform should provide a single web based dashboard to send notifications to target audiences using multiple communication methods like voice- based notification on PSTN/Cellular, SMS, Voice mail, E- mail etc.</p> <p>Provide inbuilt collaborative tools</p> <p>Platform should support easy deployment of Sensors. Platform shall have the ability to add / remove sensors including new vendor types without a need for shutdown.</p> <p>Platform should support Cross collaboration APIs thereby enabling contextual information and correlation across domains and verticals.</p>
2	Command and Control Centre Components	<p>Web Server to manage client requests. Client/User should be provided with web-based portals to event information, overall status, and details.</p> <p>The User Interface (UI) to present customized information in various preconfigured views in common formats. All information to be displayed through easy-to-use dashboards.</p> <p>Application Server to provide a set of services for accessing and visualizing data. Should be able to import data from disparate external sources, such as databases and files. It should provide monitoring services for incoming data records to generate key performance indicators. It should also provide the users to view key performance indicators, standard operating procedures, notifications, and reports, spatial-temporal data on a geospatial map, or view specific details that represent a city road, building or an area either on a location map, or in a list view. Analytics functionality can be part of application server or separate server.</p>
3	Industry Standards for the Command and Control Centre	The solution should adhere to the industry standards for interoperability, data representation & exchange, aggregation, virtualization and flexibility. IT Infrastructure Library (ITIL) V3 or above standards for Standard Operations Plan & Resource

Sl. No	Functions	Minimum Specifications
4	Availability, Scalability, Performance and Usability	Management
		Geo Spatial Standards like GML & KML etc.
		Business Process Model and Notation (BPMN) or equivalent for KPI Monitoring.
		The solution system shall be highly available platform.
		The system shall be tolerant to losses or reduction of communication such that the system shall recover gracefully from such incidents, with no human interaction required.
		Should have a high performance and high availability architecture.
		Shall be flexible, modular and tolerant to failures/errors and able to exchange information with other systems
		The communications use standard components that are widely available.
		Should allow scalability and flexibility to include more applications / solutions in the future
		The server shall refresh system GUI within seconds of an incident trigger requiring a change of state in the information in the database.
5	Convergence of Multiple feeds/	The server hardware shall be based on high availability, fault tolerant design and capable of operating in mirrored server configuration.
		The system shall have a resilient processing architecture such that failure of a single component does not affect entire common operations platform/ application.
		The system shall be able to operate at minimum network bandwidth
		The system shall be able to operate at low network latencies

Sl. No	Functions	Minimum Specifications
	services	<p>be able to monitor them and operate them.</p> <p>The solution should provide option to integrate existing deployed solution by City and also need to provide scalability option to implement new use cases.</p> <p>System should have capability to source data from various systems implemented in the city (being implemented as part of this project or other projects) to create actionable intelligence</p>
6	Integrated User Specific & Customizable Dashboard	Should provide integrated dashboard with an easy to navigate user interface for managing profiles, groups, message templates, communications, tracking receipts and compliance
		Collects major information from other integrated City sensors/platforms.
		Should allow different inputs beyond cameras, such as, User desktop screens, web page, and other external devices for rich screen layout
		Multi-displays configurations
		Support for GIS tool which allows easy map editing for wide area monitoring (Google map, Bing map, ESRI Arc GIS map, etc.).
		Should provide tools to assemble personalized dashboard views of information pertinent to incidents, emergencies & operations of command centre
		Should provide dashboard filtering capabilities that enable end-users to dynamically filter the data in their dashboard based upon criteria, such as region, dates, product, brands, etc. and capability to drill down to the details
		Should provide historical reports, event data & activity log. The reports can be exported to PDF or HTML formats.
		Use authentication information to authenticate individuals and/or assign roles.
7	Authentication & Encryption	Support LDAP authentication mechanism
		Support for PKI implementation

Sl. No	Functions	Minimum Specifications
8	Flexible Single Sign-On (SSO)	SSO to Web-based applications that can span multiple sites or domains with a range of SSO options.
9	Security & Access Control	Provide Role based security model with Single-Sign-On to allow only authorized users to access and administer the alert and notification system.
10	Internet Security	Provide comprehensive protection of web content and applications on back-end application servers, by performing authentication, credential creation and authorization.
11	API Integration	Platform OEM should have published the normalized APIs in their website for the listed domains ((Parking, Outdoor Lighting, Traffic, Environment, Urban mobility etc.) to allow sensor vendors and app developers to develop their connectors / adaptors to the platform
12	API Security	<p>The access to data should be highly secure and efficient.</p> <p>Access to the platform API(s) should be secured using API keys.</p> <p>Software should support security standards: such as OAuth 2.0 or HTTPS over SSL, and key management help protect the data across all domains.</p> <p>Should support security features built for many of its components by using HTTPS/TLS for all its public facing API implementations. For deployment where CCC Software API(s) exposed to application eco system, API Management, API security features and API Key management functions are required.</p>
13	Developer Tools	Common operations platform should provide Developer tools that help City to produce new applications, and/or use solution APIs to enhance or manage existing solution free of cost.
14	Service management	Data brokerage, ID Management: Performs service management
15	Authorization	Comprehensive policy-based security administration to provide all users specific access based on user's responsibilities. Maintenance of authorization policy in a central repository for administration

Sl. No	Functions	Minimum Specifications
		purposes.
16	User group	Should provide support to enable assignment of permissions to groups, and administration of access control across multiple applications and resources. Secure, web-based administration tools to manage users, groups, permissions and policies remotely
17	Provide multidimensional access control	Provide policies using dimensions of authorization criteria like Traditional static Access Control Lists that describe the principals (users and groups) access to resource and permissions
18	Rule Engine & Optimization	<p>Should have ability to respond to real-time data with intelligent & automated decisions</p> <p>Should provide an environment for designing, developing, and deploying business rule applications and event applications.</p> <p>The ability to deal with change in operational systems is directly related to the decisions that operators are able to make.</p> <p>Should have decision management tool</p> <p>Should provide an integrated development environment</p>
19	Remote Video Display	<p>The system should support dynamic reduction of bit rate and bandwidth for each stream based on the viewing resolution at the remote location</p> <p>The system should have efficient bandwidth usage for multiple operation centre and only transmits video stream required to display.</p> <p>The solution may have video processing server. This server must be able to cater to following functional requirements:</p> <p>a. To process and transmit video streams adaptive to each video requests to optimize network bandwidth usage.</p> <p>b. Shall be able to distribute real-time video streams without any loss in original video quality</p>

Sl. No	Functions	Minimum Specifications
20	Device Engine	<p>Aggregation and abstraction of sensors: provides aggregation of sensors from diverse sensors</p> <p>Normalization of sensor data: organizes sensor data and assigns attributes based on relations</p>
21	Location Engine	<p>Map services and geospatial coordinates: provides the geographical coordinates of specific facilities, roads, and city infrastructure assets, as well as unmapped facilities</p> <p>Geospatial calculation: calculates distance between two, or more, locations on the map</p> <p>Location-based tracking: locates and traces devices on the map</p>
22	Enterprise Resource Planning (ERP) Integration capabilities	System should allow integration of business process in ERP workflows like property, water tax collection etc.
23	Data Engine	Data archive and logging: stores data feeds from the device engine and external data sources
24	Incident Management Requirements	<p>Should provide facility to capture critical information such as location, name, status, time of the incident and be modifiable in real time by multiple authors with role associated permissions (read, write).</p> <p>Incidents should be captured in standard formats to facilitate incident correlation and reporting.</p> <p>The system must provide Incident Management Services to facilitate the management of response and recovery operations</p> <p>Should support comprehensive reporting on event status in real time manually or automatically by a sensor/CCTV video feeds.</p> <p>Should support for multiple incidents with both segregated and/or overlapping management and response teams.</p> <p>Should support for sudden critical events and linkage to standard operating procedures automatically without human intervention.</p>

Sl. No	Functions	Minimum Specifications
		<p>The system must identify and track status of critical infrastructure / resources and provide a status overview of facilities and systems</p> <p>A reference Section in the tool must be provided for posting, updating and disseminating plans, procedures, checklists and other related information.</p> <p>Should provide detailed reports and summary views to multiple users based on their roles.</p> <p>Should have mobile application for field response staff</p> <p>Provide User-defined forms as well as Standard Incident Command Forms for incident management.</p>
25	Event Correlation	Common operations platform should be able to correlate two or more events coming from different subsystems (incoming sensors) based on time, place, custom attribute and provide correlation notifications to the operators based on predefined business and operational rules in the configurable and customizable rule engine.
26	Events and Directives control	<p>Should provide the capability for the events that are produced from a sub- system and are forwarded to the ICCC. Events could be a single system occurrence or complex events that are correlated from multiple systems. Events could be ad hoc, real-time, or predicted and could range in severity from informational to critical. At the ICCC, the event should be displayed on an operations dashboard and analysed to determine a proper directive.</p> <p>Directives issued by the ICCC should depend on the severity of the monitored event. Directives will be designed and modified based on standard operating procedures, as well as state legislation. A directive could be issued automatically via rules, or it could be created by the operations team manually.</p>
27	Device Status, Obstruction Detection and Availability Notification	<p>Should provide icon based user interface on the GIS map to report non-functional device.</p> <p>Should also provide a single tabular view to list all devices along with their availability status in real time.</p> <p>Shall view the environment through geospatial or fixed composite</p>

Sl. No	Functions	Minimum Specifications
		<p>computer-generated (JPEG, BMP, AutoCAD, etc.) map</p> <p>Should allow user to view sensor or system data and related name from the displayed map</p> <p>Should visually display a camera sensor with related camera orientation, camera range and camera field of view angle.</p> <p>Should allow all resources, objects, sensors and elements on the map to be georeferenced such that they have a real world coordinate.</p> <p>Should allow user to choose camera and take live video image snapshot and save to file from any camera</p> <p>Should allow user to choose camera from map to move PTZ cameras</p> <p>Should allow map information “layers” to be displayed/hidden on items such as sensor names, Sensors, sensor range (e.g. camera – orientation, range, field of view angle), Locations and zones, Perimeter ranges, Resource tracking</p> <p>Should provide User Interface to publish messages to multiple devices at the same time</p>
28	Standard Operations Procedures (SOPs)	<p>Solution should provide for authoring and invoking un-limited number of configurable and customizable standard operating procedures through graphical, easy to use tooling interface and support English and Hindi language and optionally Punjabi.</p> <p>Standard Operating Procedures should be established, approved sets of actions considered to be the best practices for responding to a situation or carrying out an operation.</p> <p>The users should be able to edit the SOP, including adding, editing, or deleting the activities.</p> <p>It shall have facility to define more than one SOP for the selected alert category or location</p> <p>The users should be able to also add comments to or stop the SOP (prior to completion).</p>

Sl. No	Functions	Minimum Specifications
		<p>Operations/Actions are automatically logged in audit trail, changes, and commentary for the SOP and its activities, so that an electronic record is available for after-action review.</p> <p>The SOP Tool should have capability to define the following activity types:</p> <ul style="list-style-type: none"> Manual Activity - An activity that is done manually by the owner and provide details in the description field. Automation Activity - An activity that initiates and tracks a particular work order and select a predefined work order from the list. If-Then-Else Activity - A conditional activity that allows branching based on specific criteria. Either enter or select values for Then and Else. Notification Activity - An activity that displays a notification window that contains an email template for the activity owner to complete, and then sends an email and SMS notification. SOP Activity - An activity that launches another standard operating procedure.
29	KPI Display	<p>Solution should be able to facilitate measurement or criteria to assay the condition or performance of departmental processes & policies.</p> <p>Solution should allow defining key performance indicators and provide visualization interface</p>
30	What-if Analysis Tool	<p>The solution should provide the capability to manage the emergencies and in-turn reducing risks, salvaging resources to minimize damages and recovering the assets that can speed up recovery.</p> <p>To take proactive decisions that help minimize risks and damages, the solution should provide Analytical and Simulation systems as part of the Decision Support System.</p> <p>The solution should help simulate what if scenarios.</p>

Sl. No	Functions	Minimum Specifications
		<p>It should help visualize assets/resources at risk due to the pending/ongoing incident, should render impacted region on a GIS/3D map.</p> <p>The solution should help build the list of assets, their properties, location and their interdependence through an easy to use Graphical User Interface.</p> <p>When in What-If Analysis mode the solution should highlight not only the primary asset impacted but also highlight the linked assets which will be impacted.</p> <p>The user should be able to run the What-if Analysis mode for multiple types of emergency events such as Bomb Blast, Weather events, Accidents etc.</p>
31	Reporting Requirements	<p>Solution should provide easy to use user interfaces for operators such as Click to Action, Charting, Hover and Pop Ups, KPIs, Event Filtering, Drill down capability, Event Capture and User Specific Setup</p> <p>The solution should generate Customized reports based on the area, sensor type or periodic or any other customer reports as per choice of the administrators</p>
32	Alarm Display	<p>Should have an ability to display alarm condition through visual display and audible tone</p> <p>Should have an ability to simultaneously handle multiple alarms from multiple workstations</p> <p>Should have an ability to automatically prioritize and display multiple alarms and status conditions according to pre-defined parameters such as alarm type, location, sensor, severity, etc.</p> <p>Should display the highest priority alarm and associated data / video in the queue as default, regardless of the arrival sequence.</p>
33	Historical Alarm Handling	<p>Should have an ability to view historical alarms details even after the alarm has been acknowledged or closed.</p> <p>Should have an ability to sort alarms according to date/time, severity, type, and sensor ID or location.</p>

Sl. No	Functions	Minimum Specifications
34	Alarm Reporting	<p>Should have an ability to generate a full incident report of the alarm being generated.</p> <p>Should have an ability to display report on monitor and print report.</p> <p>Should have details of alarm including severity, time/date, description and location.</p> <p>Captured video image snapshots.</p> <p>Relevant sensor data such as SCADA sensors, Response instructions, Alarm activities, (audit trail).</p> <p>Should have an ability to export alarm report in various formats including pdf, jpeg, html, txt, and mht formats.</p> <p>Should have an ability to generate an alarm incident package including the full incident report and exported sensor data from the incident in a specific folder location.</p>
35	Alarm Policies and Business Logic Administration	<p>The solution should have the following ability to handle the workflow alarms through graphical user interface.</p> <p>Should have an ability to match keywords or text from the alarming subsystem's incident description to raise an alarm using criteria including exact match, exact NOT match, contains match, wildcard match and regularly expression match (such as forced door alarm, denied access, door open too long, etc.)</p> <p>Should have an ability to optionally match alarming subsystem's incident status, incident severity, and sensor type</p> <p>Should have an ability to apply any alarm policy to one or more monitoring area(s) or zone(s) without having to reapplying the policy multiple times.</p> <p>Should have an ability to apply any alarm policy to one or more sensors without having to reapply the policy multiple times.</p> <p>Should have an ability to assign specific actions for each alarm</p> <p>Should have an ability to activate or deactivate alarms as required</p>

Sl. No	Functions	Minimum Specifications
		Should have an ability to create exceptions
		Should Create batch-wise rules and process them
		Should Check and rectify logical errors and contradictory rules
		Should have an ability to schedule execution of rules
		Should Suspend or Terminate the application of rule
		Should archive unused or deactivated rules
36	Collaboration Framework/ Tools	Shall establish a collaborative framework where input from different functional departments of city municipal corporation and other smart city stakeholders such as transport, water, police, e-governance, etc. can be assimilated and analysed on a single platform; consequently resulting in aggregated city level information.
		This aggregated city level information can be converted to actionable intelligence, which would be propagated to relevant stakeholders and citizens.
		Cross collaboration APIs: Enabling contextual information and correlation across domains and verticals (Multiple vendor and Multi-sensor in future) and support security standard like HTTPS over SSL, and key management
		The common operations platform` should have the capability to bring in multiple stake holders automatically into a common collaboration platform like persistent chat rooms and virtual meeting rooms in response to a SOP defined to handle a particular event.
		The stake holders can be on various types of devices like computer, smart phones, tablets or normal phones.
		The operator should also have ability to create these collaboration spaces like virtual meeting rooms or chat groups manually.
		Shall offer the ability to create graphical displays that are representing real-time conditions in a useful, intuitive format.

Sl. No	Functions	Minimum Specifications
37	Communication Requirements	Shall enable the user to look at various operating areas and see, at a glance, <ul style="list-style-type: none"> ▪ What's going on? ▪ What are the current problems? ▪ What things are going well? ▪ Do I need to dispatch maintenance/ emergency response?
		Should provide tools for users to collaborate & communicate in real-time using instant messaging features.
		The solution should adhere to the below mentioned communication requirements.
		Provide the ability to search/locate resources based on name, department, role, geography, skill etc. for rapidly assembling a team, across department, divisions and agency boundaries during emergency
		Provide the capability to invite using information provided during the location of those individuals or roles, invite them to collaborate and to share valuable information.
		Provide a single web based dashboard to send notifications to target audiences using multiple communication methods including voice- based notification on PSTN/Cellular, SMS, Voice mail, E-mail and Social Media
		The solution should provide Dispatch Console integration with various communication channels.
		It should provide rich media support for incidents, giving dispatchers the power to consolidate information relating to an incident and instantly share that information among responder teams.
		It should assess the common operating picture, identify & dispatch mobile resources available nearby the incident location. Augment resources from multiple agencies for coordinated response.

Sl. No	Functions	Minimum Specifications
38	Instant Messaging	Provide ability to converse virtually through the exchange of text, audio, and/or video based information in real time with one or more individuals within the emergency management community.
39	Alert & Mass Notification Requirements	<p>The system should provide the software component for the message broadcast and notification solution that allows authorized personal and/or business processes to send large number of messages to target audience (select-call or global or activation of pre-programmed list) using multiple communication methods including SMS, Voice (PSTN/Cellular), Email and Social Media.</p> <p>Provide a single web based dashboard to send notifications to target audiences using multiple communication methods including voice-based notification on PSTN/Cellular, SMS, Pager, Voice mail, E-mail and Social media</p> <p>Provide function for creating the alert content and disseminating to end users.</p> <p>Provision of alerting external broadcasting organizations like Radio, TV, Cellular, etc., as web-service.</p>
40	Analytics Engine	<p>Analytics Engine can be an artificial intelligence-based smart city analytics platform module to maximize business value through advanced machine learning capabilities. The machine learning capabilities aid in automating policies that result in better asset and infrastructure management.</p> <p>The solution should be flexible to integrate with other city and government software applications.</p> <p>Analytics Engine module should have below intelligence capabilities:</p> <ul style="list-style-type: none"> a) Advanced Predictive Analytics should be part of the solution. b) The solution should be flexible to integrate with other city and government software applications c) The solution should be able to predict insights consuming data from city infrastructure viz., CCTV Surveillance, Traffic, Parking etc.

Sl. No	Functions	Minimum Specifications
		<p>d) The solution should be able to predict and integrate with Smart City solutions helping in driving operational policies creation.</p> <p>e) The solution should be robust, secure and scalable.</p> <p>The solution should have a visualization platform to view historic analytics</p> <p>The application should enable the customers to discover, compare, and correlate data across heterogeneous data sources to unravel the patterns that are previously hidden. At a broader level, when you work with the application, system do the following tasks:</p> <ul style="list-style-type: none"> a) Connect to a variety of data sources b) Analyze the result set c) Visualize the results d) Predict outcomes <p>Analytics Engine should support multiple Data Sources. Min below standard data sources should be supported from day one:</p> <p>CSV, TSV, MS Excel , NoSQL, RDBMS</p> <p>Analytics Engine should provide analysis of data from a selected data source(s).</p> <p>Analysis enables to define arithmetic and aggregation operations that result in the desired output.</p> <p>Analytics engine should provide capability to check analysis with multiple predictive algorithms</p>
41	Analytics Visualizations	<p>Analytics Engine should provide visualizations dashboard.</p> <p>In the visualization workspace it should allow to change visual attributes of a graph.</p> <p>User should not be allowed to alter the graph/visualization definition.</p> <p>In the visualizations workspace, user should able to do the following operations:</p> <ul style="list-style-type: none"> a) Change the graph/visualization type b) Print the graph

Sl. No	Functions	Minimum Specifications
42	Integration with Social Media & Open Source Intelligence	c) Export the graph
		d) Narrow down on the value ranges
		e) Toggle the axis labels
		Integrate with other 3rd party applications seamlessly
		Should support integration of the Incident Management application with the social media.
		Should support analytics based on the social media feed collected from the open source intelligence and collate with the surveillance inputs to alert the responders for immediate action on the ground.
43	Field operator module	Should support notifications to multiple agencies and departments (on mobile) that a new intelligence has been gathered through open source/social media.
		Should be able to identify the critical information and should be able to link it to an existing SOP or a new SOP should be started.
		Should extract messages and display it in an operational dashboard.
44	Summary Dashboard	Should be able to correlate the extracted message from the social media with existing other events and then should be able to initiate an SOP.
		Shall provide a mobile application for field operators bundled together with ICCC platform with at least 50 licenses
		Application shall provide incident management, SOPs and operations platform
44	Summary Dashboard	Operator shall be able to view the ICCC components based on set user permissions
		Shall provide alarm summary of each monitoring zone or monitoring area in graphical chart format
		Shall display the following charts per global area, monitoring zone or monitoring area
		Shall Open Alert Count by Monitoring Zone/Monitoring Area

Sl. No	Functions	Minimum Specifications
		<p>Shall have the capability of New vs. Viewed (Opened Alerts)</p> <p>Shall Open Alert Count by Alert Severity</p> <p>Should have Highest Severity Alert</p> <p>Shall enable Monitoring Zone or Monitoring area default to Summary view dashboard or to a map when the zone or area is selected.</p>

Integration Capabilities:

List of Services	Description
Integration of Intelligent Traffic Management System (Police)	<ul style="list-style-type: none"> ▪ JICCC will be required to integrate with Command Centre of Traffic Management System, to receive real-time feeds of the camera installed by them. ▪ These video feeds will not be saved, but will be utilized in Analytical layer to help administration monitor its assets and do a better urban planning. ▪ JICCC will also be required to send video feeds received from Smart Parking, Smart Pole, PBS in real-time basis to the command centre of Traffic (if required). JICCC should also be able to trigger the commands / alerts (if required) to the respective command centre.
Integration with CCTV Surveillance	<ul style="list-style-type: none"> ▪ JICCC will be required to integrate with CCTV Surveillance System to receive real-time feeds of the camera installed by them. These video feeds will be saved and utilized in Analytical layer to create safe city
Integration of Smart Parking	<ul style="list-style-type: none"> ▪ JICCC will be required to integrate with the command centre of the Smart Parking solution, which is a PAN City initiative. ▪ JICCC will be required to receive feeds on the status of parking across the city which are managed by the Smart Parking command centre.

List of Services	Description
	<ul style="list-style-type: none"> ▪ These feeds will provide information of available, non-available parking slots, functional and non - functional parking slots. ▪ JICCC will also be required get video feeds from the parking areas on real-time basis. ▪ Such video feeds will only be saved for 7 days. All the information received will also be required to be mapped on the GIS map. ▪ All the information received from the smart parking will also go into the Analytical layer which will help city in better planning and running of operations
Integration of Solid Waste Mgmt. Services (Tracking of Solid Waste Vehicles, PCR Vans etc.)	<ul style="list-style-type: none"> ▪ JICCC will be required to integrate with the control room of Solid Waste Vehicle tracking project (Pan City Initiative) to receive feeds on the location of the solid waste vehicles. ▪ JICCC will also get other information which is received in the control room like fuel utilization of Vehicles. ▪ All the information received will also be required to be mapped on the GIS map. ▪ All the information received from the command centre will also go into the Analytical layer which will help city in better planning and running of operations. ▪ JICCC should also be able to trigger the commands / alerts (if required) to the respective command centre.
Integration of Call Centre Services	<ul style="list-style-type: none"> ▪ JICCC will be required to integrate its helpdesk and system with call centre, in case if there is some information or notification is to be sent to ▪ Call centre for doing some action in the field regarding Municipal Corporation work. ▪ All the information received from the command centre will also go into the Analytical layer which will help city in better planning and running of operations. ▪ JICCC will be required to integrate with the backend

List of Services	Description
	<p>system of Jalandhar Municipal Corporation (MCJ).</p> <ul style="list-style-type: none"> ▪ JICCC should be able to integrate with the existing ICT systems and edge / end / mobile devices of various MC departments such as Garden, General Administration Department, Water Supply, Sewerage, Assessment and Collection (Property Tax, Shops and establishment), Fire (Fire Brigade Section), Transport of Heavy Vehicles and Maintenance (Workshop), Audit and License Issue to receive and send information. ▪ JICCC should be able to map the data received from various MC departments on its GIS Platform. ▪ JICCC will be required to send field agents, alerts and notifications for any emergency / incidents / disaster in the city for doing required action. ▪ JICCC system should also be able to get acknowledgement from the receivers.
Integration with Jalandhar GIS Maps	<ul style="list-style-type: none"> ▪ JICCC will be required to use the GIS platform developed by Jalandhar Municipal Corporation for the city. ▪ There will be a requirement for enhancing the existing platform and using it in the JICCC for doing all the necessary actions. ▪ All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations.
Integration with Environmental Sensors	<ul style="list-style-type: none"> ▪ JICCC will be required to integrate with Environmental Sensors to receive real-time feeds from them. ▪ These feeds will be saved and utilized in Analytical layer to help administration monitor its assets and do a better urban planning
Integration with Smart Lights, Water and Sewerage utilities	<ul style="list-style-type: none"> ▪ JICCC will be required to integrate with Municipal components like Street lights, Water and Sewage utilities ▪ All functionalities of the LED lights (existing) should be Geo Tagged on Jalandhar GIS map that provides full

List of Services	Description
	<p>functional and operational features in JICCC dashboard.</p> <ul style="list-style-type: none"> ▪ The Smart light project should be integrated into JICCC Dashboard which should be seamless integration as one component
Property Tax	<p>Property Tax /Land administration platform should seamlessly integrate with field operations and should securely connect to disparate systems to maintain the integrity of survey data. This GIS platform should support in creating and maintaining cadastral data and should streamline work processes and speeds the enrolment of new parcels including - Tax Parcel editing including the tools, workflow, topology, error checking, version management, and historic rollback that make mapping and public records tasks quick and easy. System should be able to identify GIS tax data errors based on set of rules and behaviours that model how points, lines, and polygons share coincident geometry. - Support field data collection to collect data against a map or form-based data and integration with Enterprise cadastral system and track tax payment status per plot</p>
Integration with Project 112	<p>The proposed scheme 112 of Govt. of India will also be linked to the proposed system. (NER)</p>

Video Display Wall - 7 X 3 Cube 50 inch

Sl. No	Minimum Specifications
1	<p>Video display wall content will not be switched frequently and shall be displayed real-time. It shall be rated for 24x7 operations</p>
2	<p>Functionality of centre zone for common viewing, for example map of the city can be enlarged and copied to the centre of the display wall for general reference</p>
3	<p>Option to create multiple layouts shall be present.</p>
4	<p>Ability for all CCTV video, web pages, IoT and all other display content to be routed to the board room</p>
5	<p>Ability to manage the content within the conference room or at the operators' consoles</p>
6	<p>Ability to add content from an JICCC workstation or conference room computer</p>

Sl. No	Minimum Specifications
7	The video display wall product selected shall be durable for optimal use in a 24/7 operational mode.
8	The focus of the design characteristics are ergonomics for the various viewers, quality and stability of the images, uniformity across the whole area, availability of the system, limited maintenance and low disruption of the control room operations
9	Video display wall shall be capable of displaying High Definition (HD) content
10	Gaps between screens shall be negligible to view HD graphics on multi screens
11	Auto calibration feature shall be provided to avoid periodic maintenance
12	There shall be a user interface for all settings and operational parameters

Video Wall Management Software

Sl. No.	Parameter	Minimum Specifications
1	Display & Scaling	Display multiple sources anywhere on display up to any size
2	Input Management	All input sources can be displayed on the video wall in freely resizable and movable windows
3	Scenarios management	Save and load desktop layouts from local or remote machines
4	Layout Management	Support all layout from input sources, Internet Explorer, desktop and remote desktop application
5	Multi View Option	Multiple view of portions or regions of Desktop, multiple application can view from single desktop
6	Other features	SMTP support Remote Control over LAN Alarm management Remote management Multiple concurrent client KVM support
7	Cube Management	Cube Health Monitoring Pop- Up Alert Service Graphical User Interface

Sl. No.	Parameter	Minimum Specifications
8	Remote Viewing	The video wall content will be able to show live on any remote display .Mobile with IE
9	Integration	The video wall software should have tight integration with VMS and JICCC application

Data Centre

Following are the benchmark requirements which should act as guiding factors for the MSI:

There should be dedicated rack space available in the data centre for the Smart City project infrastructure.

1. Access to the Data Centre Space where the Smart City project infrastructure is proposed to be hosted should be demarcated and physical access to the place would be given only to the authorized personnel.
2. Racks to be caged. Smart City Data Centre should be at least a Tier III Data Centre as per Telecommunications Infrastructure Standard for Data Centres and should be 27001 Certified.
3. It should have Access Control System implemented for secured access.
4. Indoor CCTV Cameras would be required to be installed to monitor the physical access of the system from remote location.
5. 90-days Data Backup of the video feeds and the transaction data for min 3 months shall be stored within the Data Centre infrastructure preferable in a cost effective and innovative manner.
6. In case, the data centre services are to go down due to any unforeseen circumstance, the Command Centre should have access to the video feeds of previous 90 days and the transaction data for min 3 months from this data backup facility.
7. Access logs to be stored for the entire duration of contract and handed over to Authority upon termination/expiry of the contract.
8. The availability of data must be guaranteeing to 99.982% availability. Receiving Power: Commercial power substation nearest to DC
9. UPS: UPS system with N+1 redundancy, where N = 1
10. Power Provision: Dual power feed, PDU sources to each rack, Power supply to a rack as per requirement
11. Cooling Features:
 - System: Air-cooling system, Management of temperature and humidity.
 - Blow-out Type: Raised flooring air conditioning system, Down-blow below raised floor and drawn into ceiling.

12. Fire Protection: High Sensitive Smoke Detectors, Fire Suppression System
13. Security: CCTV surveillance cameras, 24*7 on-site security presence, building Access (Photo Id Card must) along with biometric authentication.

Replication / Archival Solution

Replication Solution

Sl. No.	Minimum specifications
1	The proposed architecture should ensure that in event of Disaster at Primary Site, applications can be restarted at DR Site without any data loss.
2	The proposed architecture should focus on not only the data replication, but ensuring application availability
3	The proposed solution must optimize additional infrastructure and storage resources in the architecture.
4	The proposed solution should be a storage agnostic solution. The solution should not only seamlessly integrate with current infrastructure, but also not impose any restriction on storage or platform technology that JSCL may deploy in future.
5	The proposed software must provide comprehensive hardware and platform support. Support for physical and virtual platforms.
6	The proposed software should provide application level availability by ensuring that it not only replicates data within database but also structural changes to databases, application and database binaries etc. without any manual intervention.
7	Application high availability at primary & DR site should not be dependent on Operating system event logs. Solution should be capable to integrate directly with application start, stop and monitor service to avoid outage remedy solution because of Operating system log.
8	The proposed software should support real time tracking of configuration changes being done to Operating system, application binaries, any tuneable added/modified etc. and alert administrators in case of configuration drift between primary and DR site.
9	Shall be able to handle long outages of network without affecting the consistency of data at secondary site. The replication solution should be provisioned for storing data for at least 4 days in case network is down for extended period.

Sl. No.	Minimum specifications
10	The proposed software should provide for an automated fire-drill for testing of DR site. The testing mechanism should automatically validate the application start up at DR site at a pre-defined schedule defined.
11	The proposed software should provide availability across any distance—Builds local metropolitan and wide-area clusters for disaster recovery and local availability.
12	The proposed software should ensure no single point of failure. It has the ability to gracefully move an application to an available server in the event of a failure and coordinate the movement with storage ownership.
13	The proposed software should provide Multi-cluster management and reporting, including applications composed of multiple components running on different physical and virtual tiers, adding resilience to business services. Manages and reports on multiple local and remote clusters from a single unified web-based console.
14	The proposed software should provide seamless integration with all applications/databases used for increased application performance and availability.
15	It should also have the integration capability with replication software/technologies.
16	The proposed software should provide advanced application failover logic to ensure that application uptime is maximized, server resources are efficiently utilized, and detect failures faster than traditional clustering solutions and requires almost no CPU overhead
17	The proposed software should provide advanced clustering support for virtual machine architectures.
18	The proposed software should be simple to install, configure, and maintain. It should provide powerful wizards that enable simple, quick, and error-free setup of advanced, high availability, disaster recovery, and Fire Drill configurations.
19	The proposed software must be able to provide comprehensive insight into the storage environment, enabling improved usage and efficiency across all major operating systems and storage hardware.
20	The proposed software should have deduplication and compression to reduce the primary storage footprint.
21	The proposed software should support automated storage tiring to seamlessly and transparently move data based on business value
22	The proposed software should have the ability to make data compatible between operating systems for simplified OS migration.

Sl. No.	Minimum specifications
23	The proposed software should be able to support physical environment. It should support virtual disks in VMDK/VMFS format, and as well as RDM.
24	The proposed solution should have multi-pathing feature for I/O path availability and performance to efficiently spread I/Os across multiple paths for maximum performance, path failure protection, and fast failover.
25	Host Replication should be certified for performing replication to heterogeneous storage models from different.
26	The Host Replication technology should support different types of data whether structured or unstructured.
27	The proposed host base replication solution should be capable of maintaining data consistency at all times.

Archival Solution

Sl. No.	Minimum specifications
1	The solution must be capable of archiving content from multiple sources like messaging including File Servers , VOIP etc.
2	The proposed solution must have integration with Email solution through SMTP archiving without the need of any additional hardware.
3	The solution should have the capability to archive data from multiple electronic repository to single repository to achieve best single instance across multiple frontend source data.
4	The solution must support a Single unified console to manage archiving from different sources like File server, Mailing solution etc.
5	The solution should provision a web based discovery mechanism to search relevant data across archives from multiple sources like file server, messaging etc. The discovery mechanism should support a guided, hierachal review of searched data with capability to filter, marking and legal hold to prevent deletion/expiry.
6	The solution should facilitate a supervision mechanism for emails to ensure compliance of messaging content. The supervision mechanism should facilitate sampling of messages and subsequent review by authorized personnel
7	The solution should support tagging of messages by message security solutions like anti-spam/anti-virus for efficient retention

8	Proposed solution must support outlook on Windows & MAC machines.
9	Archival solution must have support with IMAP compliant devices to access the emails.
10	Proposed solution should support archiving both at premises and cloud.
11	Proposed solution must have monitoring integration with messaging solution vendor.
12	The solution should support Message Journaling as well as Envelope Journaling, capture data and expansion of distribution lists
13	The solution must support "Agentless" archiving of messages. There should be no need to deploy any agent on the messaging server.
14	The solution must support search for mails based on undisclosed recipients criteria
15	The solution should support seamless access using shortcuts from the native email client as well as browser based client. The solution should support all archiving actions like manually archive, search, restore, retrieve, delete from the native email client and browser based client
16	<p>The solution should support archiving based on either any or a combination of the following criteria:</p> <ul style="list-style-type: none"> · Item Type (message, calendar etc.) · Date · Size · Email Attachment only · User · Organizational Unit
17	Proposed solution must have advance way of archive disk/partition data backup to avoid backup of old partitions which must be possible with or without WORM devices.
18	<p>The solution must allow the administrators to configure the following in shortcuts:</p> <ul style="list-style-type: none"> • Include recipient information in the shortcuts. • Include nothing / original message body / custom message body in shortcuts. • Include "X" number of characters in the shortcut. • Include a custom body defined from a configuration file in the shortcut etc.
19	The solution should leave a shortcut at either the time of archiving or later as well.
20	The solution should allow users to view archived items directly without having the need to restore them to the messaging server to avoid delays and impact on messaging solution. No network connections should be established between archiving server and messaging server at the time of retrieving archived items

21	The solution must support indexing and archiving of minimum 500+ commonly used file types.
22	The solution should support archiving of entire email folders and application of selective archiving policies based upon folders.
23	The solution must support dynamic retention period of archived items i.e. retention of archived items can be increased or decreased on fly.
24	The solution should facilitate "future proofing" of content by facilitating an HTML copy for long term retention and search
25	The solution should support "safety copies" of items to be kept on the mail server. The "safety copy" allows the archiving software to wait for the archived item to be backed up or replicated before the original item is removed from the mail server.
26	Archival solution must have option to set or configure disk property read and read-write access
27	Archival solution must have disk configurable option with High & Low watermark. In case, High watermark reaches, disk should automatically become Read only and other pre-configured disk should get read-write access to store fresh archived items.
28	The solution must have OWA integration in such a fashion that archived item can be browsed directly through archived browser tab instead of browsing through internet explorer (IE). IE can be additional feature.
29	The archival solution must have an integrated e-discovery solution which allows guided Discovery, review and analysis of data from the archives and non-archived data like desktop, file server, Documentum etc. It's required for future proofing.
30	Proposed Archival solution must have seamless and consistent end user search experience across multiple interface like Desktop/Laptop, mobile, tablets etc.

Application Delivery Controller with Web Application Firewall (WAF)

1	General Requirements:
1.1	Web application firewall should be appliance based and provide specialized application threat protection.
1.2	Should protect against application-level attacks targeted at web applications.
1.3	Should provide bi-directional protection against sophisticated threats like SQL injection and cross-site scripting,

1.4	Should provide controls to prevent identity theft, financial fraud and corporate espionage.
1.5	Automatic signature update and install
1.6	Should monitor and enforce government regulations, industry best practices, and internal policies.
2	Performance requirements
2.1	Should support 80,000 HTTP transactions per second & at least 60,000 HTTPs transactions per second
2.2	Device should have Sub Millisecond Latency
2.3	Should support 1 Million HTTP concurrent connections & 400,000 of HTTPs concurrent connections
2.4	Should deliver at least 2 Gbps of WAF throughput on HTTPs
3	Interface and connectivity requirements
3.1	Should support 4 no's of 10/100/1000 GE & 2 x 10G SFP+ SR interfaces with integrated / external hardware bypass
4	Feature specifications.
4.1	The appliance should be able to perform in multiple modes
4.2	Appliance should continuously track the availability of the Servers being protected.
4.3	Should have a Web Vulnerability Scanner to detect existing vulnerabilities in the protected web applications.
4.4	Should have Data Leak Prevention module to analyze all outbound traffic alerting/blocking any credit card leakage and information disclosure
4.5	Provide controls to meet PCI compliance requirements for web application servers.
4.6	Should have controls for Anti Web Defacement and provide ability to check the authorized version of the website content.
4.7	Should enforce strict RFC compliance check to prevent attacks such as encoding attacks, buffer overflows and other application specific attacks.

4.8	Should support automatic signature updates to protect against known and potential application security threats.
4.9	WAF should support fail open in case of hardware failure
4.10	Should have built in policies
4.11	Should support custom signatures
4.12	Provide ability to allow/deny URL access
4.13	Ability to create custom attack signatures or events
4.14	Ability to combine detection and prevention
4.15	Should protect certain hidden form fields.
4.16	Must provide ability to allow or deny a specific URL access.
4.17	A given user must be enforced to follow a sequence of pages while accessing.
4.18	The WAF should support IP Reputation Service and able to provide up to date information about threatening sources.
4.19	Support IPv6 for Reverse Proxy deployments
4.20	Device should able to control BOT traffic and It should able to block known bad bots and fake search engine requests
4.21	It should support antivirus module for scanning of malicious content in uploads along with File upload violations.
4.22	The WAF solution should support integration with the on-premise Anti-APT solution to scan for zero day malwares in future in required
4.23	The solution should support device tracking feature to identify suspected attackers based on the computers they are using
4.24	The solution must prevent against social media password compromise
5	Auto Learn
5.1	Should have the capability to Auto-Learn Security Profiles required to protect the Infrastructure.
5.2	Should provide a statistical view on collected application traffic
5.3	WAF should continue to provide protection even while in learning mode.
6	Brute Force Attack

6.1	Should have controls against Brute force attacks
6.2	should Detect brute force attack (repeated requests for the same resource) against any part of the applications
6.3	Custom brute force attack detection for applications that do not return 401.
6.4	Protection against SYN-flood type of attacks
7	Cookie Protection
7.1	Should be able to protect Cookie Poisoning and Cookie Tampering.
8	Strict Protocol Validation
8.1	Must support multiple HTTP versions such as HTTP/0.9, HTTP/1.0, HTTP1.1
8.2	Should support restricting the methods used.
8.3	Should support restricting the method exceptions.
8.4	Should validate header length, content length, Body length, Parameter length, body line length etc..
9	SSL
9.1	Appliance should be able to terminate SSL
9.2	Should Passively decrypt SSL
9.3	Client certificates should be supported in passive mode and active mode.
9.4	In termination mode, the backend traffic (i.e. the traffic from the WAF to the web server) can be encrypted via SSL
9.5	Are all major cipher suites should be supported by the SSL v3 implementation.
9.6	Should support for hardware-based SSL acceleration or SSL off loading
10	High Availability and load balancing
10.1	Should support High Availability in active mode
10.2	WAF appliance should have application-aware load-balancing engine to distribute traffic and route content across multiple web servers.
10.3	WAF appliance should support Data compression for better response time to users
11	Vulnerability Scanning

11.1	The product must possess a Web Application Vulnerability Scanning capability built in.
11.2	The vulnerability scan should identify vulnerabilities such as XSS, SQL injection, Source code disclosure, Common web server vulnerabilities etc..
11.3	Scan must be able to crawl the Web application
11.4	Must be able to scan the authenticated applications.
11.5	Should support scheduled scanning.
11.6	Should support exclusions in scanning by the administrator.
12	Authentication and Administrative access.
12.1	Should support Secure Administrative Access using HTTPS and SSH
12.2	Should support Role Based Access Control for Management
12.3	Ability to remotely manage boxes
12.4	Management User Interface support for both GUI and CLI access.
12.5	Separate network interface for SSH/HTTPS access.
12.6	Support for trusted hosts
12.7	Role-based management with user authentication.
12.8	Should support and two Factor Authentication

Advance Persistent Threat (APT)

Sl. No	Minimum Specifications
Minimum Specifications of APT	
1	End point Advanced Persistent Threat Solution
2	The solution shall support endpoint based solution to protect systems across all locations from targeted attacks and advanced persistent threats (APTs)
3	The proposed solution shall work independently without depending on any other endpoint or network systems for its functionality
4	The proposed solution shall support detection of all malware types. Necessary subsequent actions to fix malwares shall be supported
5	The proposed solution shall support root cause analysis for security incidents
6	Root cause analysis shall have capabilities of sequential and chronological trace of events

Sl. No	Minimum Specifications
	with details and details on affected files/services
7	Proposed solution shall have capability to quarantine the malicious Application/program/file automatically without quarantining the entire user machine
8	Anti-Advanced Persistent Threat (APT)
9	Anti-APT shall be appliance based and support minimum throughput of 2 Gbps with required ports as per Bidder solution
10	Solution shall be capable of working in inline blocking mode without dependency on other network components
11	Proposed solution's detection rules shall be based on extensible, open language that enables users to create their own rules per requirements
12	Proposed solution shall be capable of gathering active directory user identity information, mapping IP addressed to username and making this information available for event management purposes and access control policy decisions
13	The proposed solution shall be able to whitelist trusted applications from being inspected
14	Solution shall be able to integrate with Firewall / NGFW to support inline blocking mode The solution should support deep packet inspection of SSL encrypted traffic (including HTTPS) for both incoming and outgoing
15	

AAA Specifications (AAA)

Sl. No	Feature	Minimum Specifications
1	Server	Should support approach that combines AAA (Profiling of IOT sensors and ensures only authorized devices get connected to smart city network), NAC (For Employees) and Guest Access (Integrate with Wi-Fi hotspots and SMS gateway for OTP authentication)
		Must have ability to scale up to 5000 devices per appliance. Bidder should offer hardware appliance with redundancy
		Shell protected by CLI providing configuration for base appliance settings
		Appliance must provide disk or file encryption

Sl. No	Feature	Minimum Specifications
		Ability to mix and match virtual and hardware appliances in one deployment. Platform must be deployable in out-of-band model and support for clustering with N+1 active redundancy model Flexibility to operate all features/functions on any appliance in the cluster
2	Functionality	Web-based, interface that includes several productivity tools such as a configuration wizard and preconfigured policy templates
		Support any type of networking equipment (wired, wireless, VPN) and a variety of authentication methods
		Must incorporate a complete set of tools for reporting, analysis, and troubleshooting
		AAA server should have device profiling functionality for 5000 concurrent devices from day 1 to enforce context aware policies
		AAA server must support both functionality RADIUS server for client device authentication and TACACS+ for network device authentication and logging from day 1. Overlay component can be added to achieve both functionality
3	Management	The solution Must be an easy-to-deploy hardware platform that utilizes identity based policies to secure network access and includes an integrated set of capabilities bundled under one policy platform: <ul style="list-style-type: none"> ▪ Built-in guest management and device/user on boarding ▪ Web based management interface with Dashboard ▪ Reporting and analysis with custom data filters ▪ Data repository for user, device, transaction information ▪ Rich policies using identity, device, health, or conditional elements ▪ Deployment and implementation tools.
4	Licensing	Must support flexible licensing model based on required functionality
		Correlation of user, device, and authentication information for easier troubleshooting, tracking etc.

Sl. No	Feature	Minimum Specifications
		<p>AAA framework must allow for the complete separation of Authentication and Authorization sources. For example, authentication against Active Directory but authorize against an external SQL database</p> <p>Should support multiple methods for device identification and profiling such as:</p> <ul style="list-style-type: none"> • Network based, device profiler utilizing collection via SNMP, DHCP, HTTP, AD, ActiveSync/DNS • AAA solution should have an inbuilt Certificate server to generate unique certificates and this need to push to android phones and IOS devices
5	Access	<p>Enforce security policies by blocking, isolating, and repairing noncompliant machines in a quarantine in future</p> <ul style="list-style-type: none"> • Location Based Access • Time Based Access
6	Security	<p>Must support complex PKI deployment where TLS authentication requires validating client certificate from multiple CA trust chain. Must also support AAA server certificate being signed by external CA whilst validating internal PKI signed client certificates</p> <p>AAA server should have licenses to support posture checking which includes antivirus check, firewall check , network connection , USB devices , Peer to Peer applications and auto remediation</p>
7	Reliability / Performance	<p>Appliances have ability to be clustered in any combination via local and remote network connections providing 1 million scale, redundancy, and access load balancing</p> <p>Failure of master node should not impact the ability for backup appliances to continue servicing authentication traffic</p> <p>Must support several deployment modes including centralized, distributed, or mixed</p>
8	Guest Access	Must allow Self registration of Guest with Sponsor approval

Sl. No	Feature	Minimum Specifications
		Should support customizable guest pages to allow the web-developers to create a page for the desired look and feel Access can be restricted based on <ul style="list-style-type: none"> - Time of Day - Number of Devices - Number of Sessions - Amount of Data consumed - Device Type
		Unique delivery of method of 'guest user credentials' <ul style="list-style-type: none"> - SMS - SMS over SMTP
		Solution should support 1000 guest user on boarding - Workflow can be OTP, Sponsor based, receptionist based or social login
		Sponsor approval based on boarding to ensure that no-one can provision a device without an approval

Distributed Denial of Service (DDos)

Sl. No	Minimum Specifications
System Stability and Reliability	
1	The Vendor should guarantee the stability and the reliability of hardware system such as CPU, memory, interface, and software like OS
2	The proposed Equipment must make sure the DDOS mitigation devices can work independently when there is any problem happened in the DDOS detector
3	The proposed Equipment shall be appliance based with fully hardened and secured Operating System (OS)
System Functions and Requirement	
4	The proposed Equipment shall support 10GE SFP+ port and 1 x Console port
5	Mitigation capacity of System should be at least 20Gbps
6	System should support service availability through functions of service monitoring and protection from DDoS traffic
7	System should be stable and not affect service availability even upon any system fault

Sl. No	Minimum Specifications
8	System should support ‘Troubleshooting function’ for each system function
9	System should provide in-line mode and Diversion(off ramping)/Reinjection(on ramping) mode for detecting and protecting DDoS traffic
10	System should detect any DDoS traffic and mitigate any DDoS attack without interrupt legitimate traffic and customer services
11	The Proposed system must be able to detect volumetric DDOS traffic and start mitigate volumetric DDOS traffic within 3 min
12	System should provide IP reputation list protection to filter blacklisted IP.
13	Systems should consists of Detector, Mitigator and Management device
14	System should provide user defined signatures
15	System should support detection and protection of DDoS traffic as below: IP Spoofed/Non-spoofed TCP Syn Flooding IP Spoofed/Non-spoofed TCP Syn-ACK Flooding IP Spoofed/Non-spoofed TCP FIN Flooding IP Spoofed/Non-spoofed UDP Flooding IP Spoofed/Non-spoofed ICMP Flooding HTTP GET Flooding HTTP POST Flooding HTTPS Flooding DNS Query Flooding SIP Flooding DNS amplification NTP amplification SSDP amplification Charge amplification SNMP amplification
16	System should support protection policy for L3 protocol (IP), L4 protocol (TCP, UDP, ICMP) and should support a function of exclusion for specific network.
17	System should support a function ‘protection of Payload pattern’ after analysis of Payload of Web, DNS, HTTP, etc.
18	System should support a DDoS protection function for VoIP(SIP) protocol
19	System should support to protection as a group for several IP addresses
20	System should support IPv4 and IPv6 dual-stack without deteriorating performance

Sl. No	Minimum Specifications
21	In IPv4 and IPv6 dual-stack environment, the application and change operation of individual function should not affect each other
22	The proposed Equipment shall be able to support VLAN traffic reinjection
23	The proposed Equipment shall be able to support MPLS Label traffic reinjection
24	The proposed DDoS device shall be able to support high-availability with: • Device (Anti-DDOS) failure detection • Traffic ReInjection Dead Link, gateway and interface detection
25	The proposed Equipment shall have built-in high availability (HA) features in the following mode: Active-Passive Active-Active
26	The proposed Equipment Ethernet interfaces shall support link aggregation (IEEE 802.3ad) standard
27	The proposed Equipment shall be able to immediately support both IPv4 and IPv6, and implements dual stack architecture
28	The proposed Equipment shall be able to sync with NTP server
29	The proposed Equipment shall be able to support IPv4 & IPv6 routing protocols for traffic mitigation: Static , OSPF & BGPv4
30	The proposed system should be able to be extended it performance using additional modules
31	The proposed system should be able to extend the Anti-DDOS performance and capacity automatically without additionally manual traffic distribution when new modules are added. The proposed system should be able to load share the traffic when new modules are added
32	The propose Equipment shall support policy based routing (PBR) features
33	Time to apply the Anti-DDOS policy should be within 5 minute without any service interruption
34	The proposed Equipment must able to support real-time configuration changes without impact to service
35	The proposed Equipment must be able to integrate with existing management system via SNMP version 3 and SNMP version 2
36	The Vendor must provide the latest Management Information Base (MIB) file for SNMP operation

Sl. No	Minimum Specifications
37	The proposed Equipment log shall contain the following information: Attack logging User Login logging Operation Activity logging Link Status logging Diversion logging System Performance logging HA logging Traffic Alerts logging DDoS Attack logging Syslog
38	The Security System provided shall be able to do remote inventory management capability and software download
39	The NMS shall provide the flexibility of performing configuration via GUI and command base remotely
40	The Vendor must state clearly on the features which are currently supported, to be supported under the road map, and feature that does not support by the equipment
41	Security Equipment proposed by Vendor must be fully compatible with the existing Data Centre network which may have third party equipment's
42	The Vendor shall state the maximum number of devices supported
43	The proposed System shall support secure devices management
44	Able to access managed devices through GUI
45	Able to deploy system OS / firmware patching to managed devices
46	Able to deploy scripts to automate devices system administration
47	The proposed System shall support encrypted communication between management system and device
48	The Vendor shall state the encryption level & algorithm used
49	The proposed System shall be able to execute real-time configuration changes without device service interruption
50	The proposed System shall be able to push global configuration to all or selected devices
51	The proposed System shall support secure web-based access

Sl. No	Minimum Specifications
52	The proposed System shall be able to limit administrator network access
53	The proposed system shall support devices security configuration management
54	Able to deploy single configuration element to all or selected devices
55	Able to store back-up configuration for selected devices
56	The proposed System shall support active monitoring: <ul style="list-style-type: none"> ▪ Able to display devices status ▪ Able to display system alerts ▪ Able to display various traffic data ▪ Able to display security component status & alerts
57	The proposed Equipment shall be able to support authentication schemes but not limited to: Local Password & RADIUS
58	The proposed system should support the HTTP GET FLOOD detection and mitigation. The mitigation devices should support at least 6 algorithms for http attack protection
59	The proposed system should support the extension based on growth of the network and at least support expansion of mitigation devices up to 25 devices
60	The proposed system should support the behaviour based and algorithm based DDOS mitigation
61	The proposed system must provide multi-level Anti-DDOS mitigation infrastructure. The system must support integration of upstream and downstream Anti-DDoS device to mitigate DDoS Attack effectively
62	The proposed system must provide multi-level DDOS + Web application mitigation infrastructure. The upstream Anti-DDoS and downstream WAF can integrate and mitigate layer 1 to layer 7 attack effectively
63	The proposed mitigation device should provide auto packet capture function during DDoS mitigation
64	The proposed system should provide the traffic AUTO learning function for the DDOS traffic monitoring. The auto learning threshold baseline should captured hourly
65	The traffic Auto learning threshold can be apply automatically after auto learning completed
66	The proposed system should provide the multi-level DDOS mitigation policy and different mitigation action based on DDOS traffic type

Sl. No	Minimum Specifications
67	The proposed system should provide the function to monitor the outbound DDOS attack and cooperate with the mitigation platform to block the outbound DDOS attack
68	The proposed system must be able to support netflow v5, netflow v9, sflow v4, sflow v5, netstream v5, ipfix
69	The proposed system must support double diversion feature that can advertise two BGP diversion prefix under single attack to different devices for mitigation
70	The proposed system must support multiple BGP community tagging for different diversion configuration
71	The proposed system must support BGP traffic diversion based on attack size in terms of pps/bps
72	The proposed system must support auto null route based on attack size in terms of pps/bps
Anti – DDoS Reporting System	
73	The proposed System shall support the provisioning of the following reports in detail or in summary
74	Attack reports -top sources, targets, attack type etc
75	System reports -security events triggered
76	User reports -user access activity
77	The proposed system must be able to generate summary attack report of daily/weekly/monthly
78	The proposed system must be able to send schedule summary attack report of daily/weekly/monthly
79	The Vendor shall provide full details regarding the proposed staff required to fulfil the site design and installation service, including an organization chart, job descriptions and staff competency levels.
80	The proposed System shall support report format customization
81	The proposed System shall support remote report view in web HTML
82	The proposed System shall be able to export reports as documents or images
83	The proposed System shall support the export format.
84	The proposed System shall support secure web-based access
85	The proposed system must be able to limit administrator access by IP address

Anti-Virus Solution

The following features are required for centralized anti-virus solution, to protect all computing resources (servers, desktops, other edge level devices, etc.)

1. Ability to scan through all file types and various compression formats. Ability to scan HTML, VBScript Viruses, malicious applets and ActiveX controls.
2. Must update itself over internet for virus definitions, program updates etc. (periodically as well as in push-updates in case of outbreaks)
3. Able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)
4. Shall provide Real-time Product Performance Monitor and Built-in Debug and Diagnostic tools, and context-sensitive help.
5. The solution must provide protection to multiple remote clients
6. Shall provide for virus notification options for Virus Outbreak Alert and other configurable Conditional Notification.
7. Should be capable of providing multiple layers of defence.
8. Shall have facility to clean, delete and quarantine the virus affected files.
9. Should support online update, where by most product updates and patches can be performed without bringing messaging server off-line.

Enterprise Management System (EMS)

Sl. No.	Component	Minimum specifications
1	SLA & Contract Management System	<ul style="list-style-type: none"> ▪ It must be a centralized monitoring solution for all IT assets (including servers, network equipment etc.). ▪ The solution must have integrated dashboard providing view of non performing components/issues with related to service on any active components. The solution must follow governance, compliance and content validations to improve standardization of service level contracts. ▪ Application should be pre-configured so as to allow the users

Sl. No.	Component	Minimum specifications
		<p>to generate timely reports on the SLAs on various parameters.</p> <ul style="list-style-type: none"> ▪ The solution must support Service Level Agreements & Lifecycle Management including Version Control, Status Control, Effectively and audit Trail to ensure accountability for the project. ▪ The solution must have the ability to define and calculate key performance indicators from an End to End Business Service delivery perspective related to JICCC Project under discussion. ▪ The solution should support requirements of the auditors requiring technical audit of the whole system which MSI should allow the auditors to access the system. ▪ The solution must have an integrated dashboard, view of Contract Parties & current SLA delivery levels and view of Services & current SLA performance. ▪ The solution should support SLA Alerts escalation and approval process. Solution should support effective root-cause analysis, support capabilities for investigating the root causes of failed service levels and must make it possible to find the underlying events that cause the service level contract to fail. ▪ Accept Data from a variety of formats. Support for Defining and Calculating Service Credit and Penalty based on clauses in SLAs. ▪ Reporting: <ul style="list-style-type: none"> • Ability to generate reports on penalty and credit due, to check on non-compliance of SLAs for the JICCC project • Monetary penalties to be levied for non-compliance of SLA, thus the system must provide Service Level Performance Report over time, contract, service and more. • The solution should provide historical and concurrent service level reports for the surveillance project in order to ensure accountability of the service provider's performance

Sl. No.	Component	Minimum specifications
		<ul style="list-style-type: none"> • Automatic Report creation, execution and Scheduling, must support variety of export formats including Microsoft Word, Adobe, PDF etc. • The solution must support Templates for report generation, Report Filtering and Consolidation and Context sensitive Drill-down on specific report data to drive standardization and governance of the JICCC project • The solution must support security for drill-down capabilities in dashboard reports ensuring visibility for only relevant personnel of the JICCC project • Support real-time reports (like at-a-glance status) as well as historical analysis reports (like Trend, TopN, Capacity planning reports etc.)
2	Network Monitoring System	<ul style="list-style-type: none"> ▪ The Solution should provide capability to monitor any device based on SNMP v1, v2c & 3 ▪ The Solution should monitor bandwidth utilization. ▪ The solution should monitor utilization based on bandwidth ▪ The Solution must be capable of monitoring the availability, health, and performance of core networking devices including but not limited to CPU, memory, temperature. ▪ The Solution should have the ability to issues pings to check on availability of ports, devices. ▪ The Ping Monitoring should also support collection of packet loss, Latency and Jitters during ICMP Ping Checks ▪ The Port Check for IP Services monitoring should also provide mechanism to define new services and ability to send custom commands during port check mechanism. ▪ The Solution should have the ability to receive SNMP traps and syslog. ▪ The Solution should automatically collect and store historical data so users can view and understand network performance trends. The solution should be capable of monitoring network delay/latency.

Sl. No.	Component	Minimum specifications
		<ul style="list-style-type: none"> ▪ The solution should be capable of monitoring delay variation ▪ The solution should be capable of monitoring packet loss, Packet QOS, Packet Errors on one or more ports ▪ The solution should allow users to access network availability and performance reports via the web or have those delivered via e-mail. ▪ The solution should support auto-discovery of network devices ▪ The solution should have the ability to schedule regular rediscovery of subnets. ▪ The solution should provide the ability to visually represent LAN/WAN links) with displays of related real-time performance data including utilizations. ▪ The system should provide discovery of heterogeneous physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and do mapping of LAN & WAN connectivity. ▪ The System shall support monitoring of Syslog ▪ The solution should provide capability to add an IP device or IP Range or IP subnet with functionality supporting multiple SNMP strings. ▪ The solutions should have real time, detect configuration and asset information changes made across a multi-vendor device network, regardless of how each change is made and also support configuration deployment/rollback and configuration templates.
3	Server Performance Monitoring System	<ul style="list-style-type: none"> ▪ The proposed tool should integrate with network performance management system and support operating system monitoring for various platforms supplied as part of the Surveillance Project. The proposed tool must provide information about availability and performance for target server nodes. The proposed tool should be able to monitor various operating system parameters such as processors,

Sl. No.	Component	Minimum specifications
		<p>memory, files, processes, file systems, etc. where applicable.</p> <ul style="list-style-type: none"> ▪ The solution should provide a unified web based console, which consolidates all aspects of role based access under a single console. Proposed Network Management shall integrate with SLA & Contract Management system in order to supply KPI metrics like availability, utilization, and performance in order to measure central SLA's and calculate penalties
4	Application Performance Management	<ul style="list-style-type: none"> ▪ The solution should measure the end users' experiences based on transactions without the need to install agents on user desktops. ▪ The solution must be able to provide user usage analysis and show how user's success rate, average time and transaction count has changed over a specific period of time such as current week versus previous week. ▪ The solution must be able to provide the ability to detect and alert when users experience HTTP error codes such as 404 errors or errors coming from the web application. ▪ Solution shall be able to monitor customer transaction by end-user name, and thus able to understand exactly which customers were impacted, their location, type of browser used etc. ▪ The solution must simplify complex app topologies through task-relevant views based on attributes such as location, business unit, application component etc. ▪ The solution must speed up the process of triage by showing the impact of change, thus enabling to easily locate where performance problems originate. The solution should provide the flexibility of collecting deep-dive diagnostics data for the transactions that matter for triage as opposed to collecting deep-dive data for every transaction. ▪ The solution must proactively monitor 100% of real user transactions; detect failed transactions; gather evidence

Sl. No.	Component	Minimum specifications
		<p>necessary for triage and diagnosis of problems that affect user experiences and prevent completion of critical business processes.</p> <ul style="list-style-type: none"> ▪ The solution must determine if the root cause of performance issues is inside the monitored application, in connected back-end systems or at the network layer from a single console view. ▪ The solution must provide proactive real-time insights into real user behaviour, trends, log analytics and performance to enhance customer experience across various channels ▪ The solution must provide operational efficiency capabilities that provide insight of app performance by version, geo, OS, network, real-time alerts on threshold violations impacting SLAs and prioritize alerts based on impact to business, revenue and gain end-to-end visibility into the mobile infrastructure. ▪ The solution must provide complete Insights into Application Flows, Heat Maps to enable improving the UI design, understand user interactions, build functionality based on real user data and create product & services differentiation.
5	Asset Management System	<ul style="list-style-type: none"> ▪ Ability to provide inventory of hardware and software applications on end-user desktops, including information on processor, memory, OS, mouse, keyboard, etc. through agents installed on them. ▪ Ability to have reporting capabilities; provide predefined reports and ability to create customized reports on data in the inventory database. Report results could be displayed as lists or graphs. ▪ Ability to provide the facility to collect custom information from desktops. ▪ Ability to provide facility to recognize custom applications on desktops. ▪ Facility for the administrator to register a new application to

Sl. No.	Component	Minimum specifications
		<p>the detectable application list using certain identification criteria. Shall enable the new application to be detected automatically next time the inventory is scanned.</p> <ul style="list-style-type: none"> ▪ Ability to support configuration management functionality using which standardization of configuration can be achieved of all the desktops. ▪ Software metering shall be supported to audit and control software usage. Shall support offline and online metering. ▪ Ability to support dynamic grouping of enabling assets to be grouped dynamically based on some pre-defined criteria e.g. a group shall be able to display how many and which computers has a specific application installed. As and when a new computer gets the new application installed it shall dynamically add to the group. ▪ Ability to use the query tool to identify specific instances of concern like policy violation (presence of prohibited programs / games and old versions, etc.), inventory changes (memory change, etc.) and accordingly it could perform several actions as reply. These actions may be (a) sending a mail, (b) writing to file (c) message to scroll on monitor screen, etc. ▪ Facility to track changes by maintaining history of an asset. ▪ The proposed EMS solution shall provide comprehensive and end -to-end management of all the components for each service including all the hardware devices, Network, Systems and Application infrastructure. <p>Note: It is mandatory that all the modules for the proposed EMS Solution shall provide out-of-the-box and seamless integration capabilities. SI shall provide the specifications and numbers for all necessary Hardware, OS & DB (if any) which is required for an EMS to operate effectively.</p>

Network Management System

1. The NMS should support an open database schema, configuration, administration, monitoring and troubleshooting of Switches, guided workflows based on best practices with built-in configuration templates, the capability to view the network topology, Layer 2 Services and Fault Management
2. It should support rich visibility into end-user connectivity
3. The NMS should automatically discover IP devices, SNMP compliant network devices on the network
4. The NMS should support Inventory management of Network devices, should support Monitoring and troubleshooting of Devices, should support configuration management and reporting.
5. The NMS should support Inventory management of Network devices, should support Monitoring and troubleshooting of Devices, should support configuration management and
6. The NMS should support flexible reporting for inventory, user tracking, compliance, switch port usage and end-of-sale
7. Must show location information of clients, infrastructure Access Points, Rogue Access Points in a map format
8. Must support virtualization
9. The Network Management function must monitor performance across heterogeneous networks from one end of the enterprise to the other.
10. It should proactively analyse problems to improve network performance.
11. The Network Management function should create a graphical display of all discovered resources.
12. The Network Management function should have extensive reporting facility, providing the ability to format and present data in a graphical and tabular display
13. The Network Management function should collect and analyse the data. Once collected, it should automatically store data gathered by the NMS system in a database. This enterprise-wide data should be easily accessed from a central location and used to help with capacity planning, reporting and analysis.
14. The Network Management function should also collect traffic statistics on client/server sessions, which cross the LAN on which it is running
15. The Network Management function should also provide information on performance of Ethernet segments, including capacity utilization and error statistics for the segment and the top contributing hosts, WAN links and routers.

16. Alerts should be shown on the Event Management map when thresholds are exceeded and should subsequently be able to inform network operators and notify concerned authority using different methods such as emails etc.
17. It should be able to automatically generate a notification in the event of a link failure to ensure proper handling of link related issues.

Virtualization software

Sl. No.	Item	Minimum specifications
1	Guest OS Support	Windows client, Windows Server, Linux (at least Red Hat, SUSE, Ubuntu and CentOS, Solaris x86) etc.
2	VM Capability	Create Virtual machines with up to 128 virtual processors, 6 TB virtual RAM and 2 GB Video memory in virtual machines for all the guest operating system supported by the hypervisor.
3	VM Live Migration	Virtual Machine migration between different generations of CPUs in the same cluster and without Virtualization the need for shared storage option and between servers in a cluster, across clusters as well as long distances from one site to another (up to 150 milliseconds round trip time) with no disruption to users or loss of services, eliminating the need to schedule application downtime or business downtime.
4	Storage Live Migration	Live migration of VM disk from one storage array to another without any VM downtime. Support this migration from one storage protocol to another eg: FC, NFS, iSCSI, DAS
5	High Availability	Proactive High availability capability that utilizes server health information and migrates VMs from degraded hosts before problem occurs.
6	Always Available	Zero downtime, zero data loss and continuous availability for the applications running in virtual machines in the event of physical host failure, without the cost and complexity of traditional hardware or software clustering solutions.
7	Resource Addition	Add CPU, Memory & devices to virtual machines on the fly when needed, without disruption or downtime of working VMs for both windows and Linux based VMs.

Sl. No.	Item	Minimum specifications
8	Resource Scheduler	Dynamically allocate and balance computing capacity across collections of hardware resources aggregated into one unified resource pool with optional control over movement of virtual machines like restricting VMs to run on selected physical hosts.
		Create a cluster out of multiple storage data stores and automate load balancing by using storage characteristics to determine the best place for a virtual machine's data to reside, both when it is created and when it is used over time.
9	Security	VM-level encryption with no modifications in guest OS to protects unauthorized data access both at-rest and in-motion and also provides secure boot for protection for both the hypervisor and guest operating system by ensuring images have not been tampered with and preventing loading of unauthorized components.
		Integration of 3rd party endpoint security to secure the virtual machines with offloaded Firewall and HIPS solutions without the need for agents inside the virtual machines from day 1.
10	Storage Support	Support boot from iSCSI, FCoE, and Fibre Channel SAN.
		Integrate with NAS, FC, FCoE and iSCSI SAN and infrastructure from leading vendors leveraging high performance shared storage to centralize virtual machine file storage for greater manageability, flexibility and availability.
		Virtual Volumes which enables abstraction for external storage (SAN and NAS) devices making them Virtualization aware.
		Integration with Storage API's providing integration with supported third-party data protection, multi-pathing and disk array solutions.
11	Virtual Switch	Span across a virtual datacentre and multiple hosts should be able to connect to it. This will simplify and enhance virtual-machine networking in virtualized environments and enables those environments to use third-party distributed virtual switches.

Sl. No.	Item	Minimum specifications
		In-built enhanced host-level packet capture tool which will provide functionalities like SPAN, RSPAN, ERSPAN and will capture traffic at uplink, virtual switch port and virtual NIC level. It should also be able to capture dropped packets and trace the path of a packet with time stamp details.
		“Latency Sensitivity” setting in a VM that can be tuned to help reduce virtual machine latency.
		Link aggregation feature in the virtual switch which will provide choice in hashing algorithms on which link aggregation is decided and this should also provide multiple link aggregation groups to be provided in a single host.
12	VM Based Replication	Efficient array-agnostic replication of virtual machine data over the LAN or WAN. This Replication should simplify management enabling replication at the virtual machine level and enabling RPOs as low as 15 minutes.
13	VM Backup	Simple and cost effective backup and recovery for virtual machines which should allow admins to back up virtual machine data to disk without the need of agents and this backup solution should have built-in variable length de-duplication capability.
14	I/O Control	Prioritize storage access by continuously monitoring I/O load of storage volume and dynamically allocate available I/O resources to virtual machines according to needs. Prioritize network access by continuously monitoring I/O load over network and dynamically allocate available I/O resources to virtual machines according to needs.
15	OEM Support	Direct OEM 24x7x365 days with unlimited incident support and 30mins or less response time including the unlimited upgrades and updates.

Databases

Enterprise class database shall be provided along with license and support and upgrade costs. Database shall be provided as per application requirement and it must be quoted separately in financial bid.

Sl. No.	Minimum specifications
----------------	-------------------------------

Sl. No.	Minimum specifications
General	
1	Database License should be un-restricted, to prevent any non-compliance in an event of customization & integration.
2	Database should provide Unicode (Latest version) capability with Indian language support
3	Databases shall support multi hardware and Operating System platform.
4	Database shall provide standard access Tool for administering the database. The tool should be able to monitor, maintain and manage the database instance, objects, and packages.
5	Database shall have built-in backup and recovery tool, which can support the online backup.
6	Database shall be able to provide database level storage management mechanism, which should enable the availability by means of creating redundancy, automatically balance the data files across the available disks, i/o balancing across the available disks for the database for performance, availability and management.
7	Should be an enterprise class database with the ability to support connection pooling, load sharing and load balancing when the load on the application increases.
8	Database shall provide native functionality to store XML, within the database and support search, query functionalities.
9	Database shall have built-in DR solution to replicate the changes happening in the database across DR site with an option to run real-time reports from the DR site without stopping the recovery mechanism
10	Database shall have Active-Passive failover clustering with objectives of scalability and high availability.
11	Database shall provide mechanism to recover rows, tables when accidentally deleted. The mechanism should provide ways and means of recovering the database.
12	Database shall provide functionality to replicate / propagate the data across different databases.
13	The RDBMS should support partitioning feature in table level object.
14	Database shall provide native functionality to store XML, Images, Text, Medical Images, CAD images within the database and support search, query functionalities.
15	Database shall include tools for enterprise class high availability solution like monitoring performance, diagnose and alert for problems, tuning bottlenecks, resource monitoring and automatic resource allocation capabilities.

Sl. No.	Minimum specifications
16	RDBMS must support the SQL queries.
17	Database shall provide security mechanism at foundation level of the database, so that the options and additions to the database confirm the security policy of the organization without changing the application code. Shall confirm to security evaluations and conformance to common criteria.
18	Database shall provide control data access down to the row-level so that multiple users with varying access privileges can share the data within the same physical database.
19	Database shall support for enhanced authentication by integrating tokens and biometric technologies.
20	Database shall provide functionality for classifying data and mediating access to data based on its classification for multi-level security and mandatory access control, manage access to data on a "need to know" basis.
21	Database shall be having native auditing capabilities for the database. Should support optional Audit Capability to store the audit records in separate audit store with monitoring & reporting for multiple databases to detect any security breaches.
22	Database shall be having built-in provision to Administer database / database clusters, Monitor performance, Maintain database, Backup and recovery, Recovery management, Disaster recovery management.
23	The Management tool should provide advisory-based performance tuning tool which help to tune the queries or objects, SQL analysis, SQL access.
24	The enterprise database should provide single web-based console for management of the database.
Restart and Recovery	
25	Availability of recovery/restart facilities of the DBMS.
26	Automated recovery/restart features provided that do not require programmer involvement or system reruns.
27	Program restart should be provided from the point of failure.
28	Ability to manage recovery/restart facilities to reduce system overhead.
29	Provides extra utilities to back up the databases by faster means than record by record retrieval.
30	Provides clear error reporting, recovery and logging.
31	Describe recovery strategies that needs to be in place.

Sl. No.	Minimum specifications
32	System should support mirroring for DRP.
Backup Procedures	
33	Describe Backup Procedures you plan to deploy.
34	Describe backup application(s) your proposed solution use.
35	Provide details of data backup and restore processes and procedures for all data elements.
36	Provide details of automated archiving procedures to copy active data to storage media when archive 'age' is reached.
Error Handling	
37	<p>Ability to trap a transaction failure through:</p> <ul style="list-style-type: none"> • Application Software • DBMS • Availability of manual containing all system error messages and correction procedures
System Control	
38	Provide details of the 'Audit trail' facility for your proposed solution.
39	Should provide adequate auditing trail facility.
40	System should record the date and time stamp for all records.
41	Ability to track terminals from where the system is accessed.

Video Conferencing System

Video Conferencing System – General Requirements		
Sl. No.	Component	Minimum Specifications
1	System Features	Conferencing System should have minimum 20 ports at HD/ 1080p, 25fps or better on IP in continuous presence mode with H.264 resolution or better and encryption
		Multi-point video Conferencing Solution should be capable of offering a High Definition/1080p, 25fps or better in real-time for at least 15 number of concurrent ports/systems in single call or multiple multi-party sessions in continuous presence and voice activation mode
		It should as well provide network flexibility for a reliable distributed architecture and cost-effective scalability for future requirements.
		Conferencing System should be deployed in High Availability and should

Video Conferencing System – General Requirements		
Sl. No.	Component	Minimum Specifications
		<p>be redundant (1:1)</p> <p>It should provide flexibility to the users, where users can join the video conference call using PC, laptop, Smart phones, PSTN but not limited to. Video conferencing system shall support various browsers installed in PC, Laptop, Smartphones etc. This facility should be available from day one.</p> <p>The systems should support document sharing (PC images, etc.).</p>
2	Video Standards and Resolutions	<p>It should support WebRTC latest industry standards for video compression.</p>
3	Content Standards and Resolutions	<p>Content sharing should be possible at 1080p 25fps</p> <p>It should support H.239 and encryption in SIP & H.323 modes</p>
4	Audio Standards and Features	<p>It should support G.711, G.722, G.722.1</p> <p>It shall support aspect ratio of 16:9 and 4:3.</p> <p>It shall support a mix of resolutions in both Voice-activated mode and Continuous Presence. Each endpoint shall receive at the maximum of its capacity without reducing the capacity of another.</p> <p>Dynamic CP layout adjustment (it will choose the best video layout according to the number of participants in the conference).</p> <p>It should support distributed architecture with intelligent and automatic call routing. It must support load balancing such that in case there are two instances, conference participants can get distributed across these two instances based on their locations and still join into the same conference.</p>
5	Network and security features	<p>It shall support encryption of 128 bit for every participant without affecting any other feature, functionality or port count.</p>
6	Interoperability	<p>Apart from Integrated video systems, video IP phones, normal IP phones also should be able to join the conference seamlessly</p>
Management & Scheduling		
Sl. No.	Component	Specifications

Video Conferencing System – General Requirements		
Sl. No.	Component	Minimum Specifications
7	System	The central management solution should be able to schedule the meeting quickly and easily manage conference infrastructure device configuration and provision of the endpoints.
8	System Capacity	The Central management server must support 10 devices capacity from day one and must be scalable.
9	Provisioning	The administration should be able to configure individual end points or group of endpoints using user policy from single management console.
		It should be possible for the endpoint to automatically pull the device and site provisioning information from the system while start up
10	Software Update	It should support automatic and scheduled mechanism to upgrade the software on one or more endpoints with a standard software.
11	Scheduling	The system should support schedule video conference meetings.
12	Directory Services	Should support integration with the corporate Active Directory for scheduling the video conference calls.
		The system should store video dialling information.
Voice and Video Call Control		
Sl. No.	Component	Specifications
13	System	The Call control solution should be able to register Integrated VC room system, Video IP phones, normal IP phones natively.
		The system should be a converged communication System with ability to run TDM and IP on the same platform.
		It should be possible to deploy Servers / Call Servers in an active-active/active or active/hot-standby hot-standby configuration over the distributed IP infrastructure (LAN/WAN).
		The communication feature server and gateway should support IP V6 from day one so as to be future proof
		The offered solution must provide a standard based mechanism for QoS implementation
		Should support AD & LDAP integration for directory synchronization & user authentication
14	Support for	Should support signalling standards/Protocols – SIP, MGCP, H.323, Q.Sig

Video Conferencing System – General Requirements		
Sl. No.	Component	Minimum Specifications
	call-processing and call-control	Voice Codec support - G.711, G.729, G.729ab, g.722. Video codecs: H.261, H.263, H.264 or better and Wideband Video Codec
		Video telephony support
		System should be supplied with 50 endpoint license
15	Security	The protection of signalling connections over IP by means of authentication, Integrity and encryption should be carried out using TLS
		System should support MLPP feature
		Proposed system should support SRTP for media encryption and signalling encryption by TLS
		Secure HTTP support for Call Server Administration, Serviceability, User Pages, and Call Detail Record Analysis and Reporting Tool. Should support Secure Sockets Layer (SSL) for directory
Fully Integrated Single Room System		
Sl. No.	Component	Specifications
16	Protocols	Should support H.323 (LAN Video Conferencing) standards. The system should be able to call any H.323 and SIP endpoint directly or indirectly.
		It should be possible to share content via BFCP and H.239
		Endpoint should support the latest video coding standard either H.263, H.264, H.265 or better
		It should support Audio coding G.722, G.722.1, G.711
17	Network	Endpoint should support bit rate up to 8 Mbps or more on IP (H.323 and SIP)
		Minimum 1 X Gigabit Ethernet: Should support 10/100/1000 BASET
18	Main Video Resolution	Shall support high definition video resolution/1080p, 25fps or better for live video for both Transmit and receive

Video Conferencing System – General Requirements		
Sl. No.	Component	Minimum Specifications
19	Camera	Inbuilt in the Integrated system with 1 cameras
		Zoom: Minimum 10x (optical) or better
20	Video Inputs	Minimum 2 HDMI inputs and 1 input for connecting PC / laptop
21	Video Outputs	Minimum 2 x HDMI or similar or better to connect two displays. Additional Outputs are desirable.
22	Audio Inputs	Omnidirectional / Directional Microphones. 2 microphones to be supplied from day one with the system.
23	Encryption	AES 128 bit or more, TLS, SRTP, HTTPS or similar or better
24	User Interface	Intuitive touch panel to operate the entire system
Video device		
Sl. No.	Component	Specifications
25	System	Should be an integrated system with at least 50-inch LCD/TFT screen, 1080P resolution (16:9), HD camera and speakers for wideband audio output. The Codec should be a part of the unit.
		The LCD/TFT screen should be remote control operable.
		Video Standards:
		<ul style="list-style-type: none"> • Minimum H.264 and above
		<ul style="list-style-type: none"> • The system should support SIP protocol
		<ul style="list-style-type: none"> • Must support desktop sharing SIP calls
		Video Frame Rate: Must support 1080p 25 fps
		Video Input: Should have HDMI or DVI (Digital Video Interface) input to connect PC/Laptop directly to the Video conferencing system and display a resolution of XGA/SXGA. The user must be able to toggle between the Laptop/PC mode and the Video conferencing mode at a push of button/icon.
		Video Output: Must have an HD output via an HDMI/DVI output port to

Video Conferencing System – General Requirements		
Sl. No.	Component	Minimum Specifications
		display the VC screen onto an external display Should have inbuilt microphone & speaker system.
26	Security	Security - Password protected system menu
27	Camera	Should be HD at least 6-megapixel camera, with privacy shutter Must support 1080p resolution. Should support Wide formats. Must support 1920 X 1080 resolution The VC unit must allow the camera to be used as a document camera to capture hard copies and transmit it to the far end site

EPABX

Operational Requirements:

1. The control room shall be equipped with **EPABX comprising** of 1 PRI line hunting - single telephone number to a group of 10 lines.
2. The Control room shall have seating capacity of minimum of 10 operators. Citizen can dial the telephone no. for any complaints related with police/ambulance/fire. The system shall have capability to display name, address and find the geographical position of the caller at the time of receiving call in call centre.
3. All phone calls shall be recorded for future references. The phone calls of at least the last 6 months shall be stored.
4. The operators shall be able to receive call, dispatch calls, use GIS maps and can send the alerts to the nearby free patrolling vehicles / fire engines / ambulances and also inform the nearest Police Station about the event.
5. The operator shall be able to view the nearest Fire Station, Hospital, Blood Bank for providing additional assistance at the site of incident.
6. A web-based incident analytic software shall be made available that will help the Police / Ambulance / Fire / Municipal Corporation to do detailed analysis and analytics so that the response can be made proactive and also the effectiveness of the service improved.
7. After the Call has been logged in by the call taker, the system shall send a SMS to the Caller stating the CFS/Tracking Number along with a password as acknowledgement to the call made to the control room. The caller can use this number on department website to access the event progress details such as Action Taken Reports (ATR), file attachments, remarks, or other information's as per the prevailing departmental policy for data sharing.
8. Security and Audit - The platform needs to be audited with STQC certification by CERT-IN empanelled agency.

9. Multi-Language & Differently abled person Support - Should have support for local Indian languages to be able to reach masses. Shall provide support for English and Hindi, standard local languages (Punjabi) across various channels (SMS, IVR, Smart Client, Mobile Web etc.) for services across service categories as required by individual integrating departments.
- Policies for retention of records including voice recording, screen recording, case details etc.
 - Records would be deleted in consultation with the department.

Technical Specifications:

Video Wall

Sl. No.	Parameter	Minimum Specifications
1	Size	JICCC Screen unit size- 50" in 7 * 3 array arrangement DLP screen Viewing Centre – 50" single DLP screen
2	Resolution	Full high definition (1920 x 1080); 16:9 Widescreen
3	Contrast ratio	1400:1 or better
4	Brightness	Minimum 250 nits or better and should be adjustable for lower or even higher brightness requirements Uniformity: $\geq 90\%$
5	Viewing angle	178 degree/178 degree or better (H/V)
6	Screen to screen gap	< 1 mm or better
7	Light Source Type	Best in class LED light source with redundancies for DLP LEDs.
8	Dust Prevention	Should be designed to avoid dust / Dust tight and resistant / Follow standards as prescribed by Government
9	Response time	8ms
10	Input	HDMI/DVI
11	Control	· On Screen Display (OSD) · IR remote control or IP based control or any other medium
12	Operations	24 x 7 basis
13	Power Consumption	Less than 250 watts per cube or more
13	Colour and Brightness	All cubes should have uniform brightness and colour. The colour calibration should be automatic and continuous operations.

Video Wall Controller

S. No.	Parameter	Minimum Specifications
1.	Controller	Controller to control Video wall in a matrix arrangement as per requirement along with software
2.	Chassis	19" Rack mount
3.	Processor	Latest Generation 64 bit x86 Quad Core processor (3.4 Ghz) or better
4.	Operating System	Pre-loaded 64-bit Operating System Windows / Linux / Equivalent, with recovery disc
5.	RAM	32 GB or more
6.	HDD	500 GB (7200 RPM) or more
7.	Networking	Dual-port Gigabit Ethernet Controller with RJ-45 ports
8.	RAID	RAID 0, 1 or better
9.	Power Supply	Redundant
10.	Input/ Output support	DVI/HDMI/USB/ LAN/ VGA/SATA port
11.	Accessories	104 key Keyboard and Optical USB mouse
12.	USB Ports	Minimum 4 USB Ports
13.	Redundancy support	Power Supply, HDD, LAN port & Controller
14.	Scalability	Display multiple source windows in any size, anywhere on the wall
15.	Control functions	Brightness/ Contrast/ Saturation/ Hue/ Filtering/ Crop/ Rotate
16.	Inputs	To connect to minimum 2 sources through HDMI
17.	Output	To connect to minimum 16 Displays through HDMI
18.	Operating Temperature	-10°C to 35°C, 90 % humidity
19.	Cable & Connections	Successful bidder should provide all the necessary cables and connectors, so as to connect Controller with LED Display units
20.	Architecture	The controller should be based on distributed architecture. The controller should be used to decode the IP camera on the video wall

Workstation

The workstations to be provided for Emergency Response System shall have three monitors. For details please refer Emergency Response system. CCTV surveillance desktops shall have two monitors.

Sl. No.	Parameter	Minimum Specifications
1	Processor	Latest generation 64bit X86 Quad core processor(3Ghz) or better
2	Chipset	Latest series 64bit Chipset
3	Motherboard	OEM Motherboard
4	RAM	Minimum 8 GB DDR3 ECC Memory @ 1600 Mhz. Slots should be free for future upgrade. Minimum 4 DIMM slots, supporting up to 32GB ECC
5	Graphics card	Minimum Graphics card with 2 GB video memory (non- shared)
6	HDD	2 TB SATA-3 Hard drive @7200 rpm with Flash Cache of 64GB SSD. Provision for installing 4 more drives.
7	Media Drive	No CD / DVD Drive
8	Network interface	10/100/1000 Mbps autosensing on board integrated RJ-45 Ethernet port.
9	Audio	Line/Mic IN, Line-out/Spr Out (3.5 mm)
10	Ports	Minimum 6 USB ports (out of that 2 in front)
11	Keyboard	104 keys minimum OEM keyboard
12	Mouse	2 button optical scroll mouse (USB)
13	PTZ joystick controller (with 2 of the workstations in JICCC)	<ul style="list-style-type: none"> • PTZ speed dome control for IP cameras • Minimum 10 programmable buttons • Multi-camera operations • Compatible with all the camera models offered in the solution • Compatible with VMS /Monitoring software offered
14	Monitor	22" TFT LED monitor, Minimum 1920 x1080 resolution, 5 ms or better response time, TCO 05 (or higher) certified
15	Certification	Energy star 5.0/BEE star certified
16	Operating System	64 bit pre-loaded OS with recovery disc
17	Security	BIOS controlled electro-mechanical internal chassis lock for the system.

Sl. No.	Parameter	Minimum Specifications
18	Antivirus feature	Advanced antivirus, antispyware, desktop firewall, intrusion prevention (comprising of a single, deployable agent) which can be managed by a central server. (Support, updates, patches and errata for the entire contract/ project period)
19	Power supply	SMPS; Minimum 400-watt Continuous Power Supply with Full ranging input and APFC. Power supply should be 90% efficient with EPEAT Gold certification for the system.
20	USB Ports	Minimum 4 USB ports (out of that 2 must be in front)
21	Certification for Desktop	Energy Star 5.0 or above / BEE star certified

Laptops

Sl. No.	Item	Minimum Specifications
1	Processor	Latest generation Intel Core i5 (3 Ghz) or higher
2	Display	Minimum 14" Diagonal TFT Widescreen with Minimum 1366 x 768 resolution (16:9 ratio)
3	Memory	8 GB DDR3 RAM @ must be free for future upgrade
4	Hard Disk Drive	Minimum 500 GB SATA HDD @ 5400 rpm
5	Ports	3 USB Ports; 1- Gigabit LAN (RJ 45); 1- HDMI/Display port; 1- VGA; 1- headphone/Microphone
6	Web Camera	Built in web cam
7	Wireless Connectivity	Wireless LAN - 802.11b/g/n/ Bluetooth 3.0
8	Audio	Built-in Speakers
9	Battery backup	Minimum 4 lithium ion or lithium polymer battery with a backup of minimum 4 hours
10	Keyboard and Mouse	84 Keys Windows Compatible keyboard, Integrated Touch Pad.

Sl. No.	Item	Minimum Specifications
11	Operating System	Pre-loaded Windows 10 (or latest) Professional 64 bit or equivalent and Office suite or equivalent, licensed copy with certificate of authenticity (or equivalent authenticity information) and all necessary and latest patches and updates. All Utilities and driver software, bundled in CD/DVD/Pen-drive media.
12	Certification	Energy Star 5.0 or above / BEE star certified
13	Weight	Laptop with battery (without DVD) should not weigh more than 3 Kg
14	Accessories	Laptop carrying Back-pack. It must be from same OEM as laptop
15	Other pre-loaded software (open source/ free)	Latest version of Adobe Acrobat Reader, Scanning Software (as per scanner offered). These software shall be preloaded (at the facility of OEM or any other location) before shipment to Authority offices/locations.

IP Phone

Sl. No.	Parameter	Minimum Specifications
1	Display	2 line or more, Monochrome display for viewing features like messages, directory
2	Integral switch	10/100 mbps for a direct connection to a 10/100 BASE-T network or better.
3	Speaker Phone	Yes
4	Headset	Wired, Cushion Padded Dual Ear- Speaker, Noise Cancelling headset with mouthpiece microphone, port compatibility with IP Phone
5	VoIP Protocol	SIP V2
6	POE/POE+	IEEE 802.3af or better and AC Power Adapter (Option)
7	Supported Protocols	SNMP, DHCP, DNS
8	Codecs	G.711, G.722, G.729 including handset and speakerphone
9	Speaker Phone	Full duplex speaker phone with echo cancellation Speaker on/off button, microphone mute
10	Volume control	Easy decibel level adjustment for speaker phone, handset and

Sl. No.	Parameter	Minimum Specifications
		ringer
11	Phonebook/Address book	Minimum 100 contacts
12	Call Logs	Access to missed, received, and placed calls. (Minimum 20 overall)
13	Clock	Time and Date on display
14	Ringer	Selectable Ringer tone
15	Directory Access	LDAP standard directory

IP PBX

Sl. No.	Minimum specifications
1	The IP telephony system should be a converged communication System with ability to run analog and IP on the same platform using same software load based on server and Gateway architecture
2	The single IP PBX system should be scalable to support up to 500 stations (any mix/percentage of Analog/IP) to achieve the future capacity
3	The system should be based on server gateway architecture with external server running on Linux OS. No. of card based processor systems should be quoted.
4	The voice network architecture and call control functionality should be based on SIP
5	The call control system should be fully redundant solution with no single point of failure & should provide 1:1 redundancy.
6	The communication server and gateway should support IP V6 from day one so as to be future proof
7	The entire solution (IP PBX, its hardware, IP Phones, Voice Gateway) should be from a single OEM
Support for call-processing and call-control	
8	Should support signalling standards/Protocols – SIP, MGCP, H.323, Q.Sig
9	Voice Codec support - G.711, G.729, G.729ab, g.722
10	The System should have GUI support web based management console
Security	

Sl. No.	Minimum specifications
11	The protection of signalling connections over IP by means of authentication, Integrity and encryption should be carried out using TLS
12	System should support MLPP feature
13	Proposed system should support SRTP for media encryption and signalling encryption by TLS
14	Secure HTTP support for Call Server Administration, Serviceability, User Pages, and Call Detail Record Analysis and Reporting Tool. Should support Secure Sockets Layer (SSL) for directory
15	The administrator logging on to the call control server needs to authenticate by suitable mechanism such as User Login Information and Passwords/ Radius Server
16	Voice gateway to be provided with 1 PRI card scalable to 3 PRI in future for PSTN (PRI) line termination.

Multi-Function Laser Printer

Sl. No.	Parameter	Minimum Specifications
1	Technology	Laser
2	Monthly duty cycle/RMPV (pages)	200,000/5K-20K
3	Print speed – simplex (A4)	Up to 41 ppm
4	Scan speed – Black/Colour simplex	Up to 50/30 ipm
5	Scan speed – Black/Colour duplex	Up to 19/14 ipm
6	Scan-to destinations	Email, Network folder, USB
7	Processor (MHz)	600
8	Memory (MB)	1024
9	Hard disk drive (HDD)/Capacity (GB)	Yes/240
10	Connectivity	2 Hi-Speed USB 2.0; 1 Gigabit Ethernet 10/100/1000T network
11	Print resolution – Max/Best print quality (dpi)	Up to 1200x1200
12	Input capacity – Std/Max (sheets)	600/4,600
13	Output size – Min/ Max (mm)	76.2 x127/312x469.9
14	Automatic duplex	Yes

Sl. No.	Parameter	Minimum Specifications
15	Energy Efficiency	BEE or Energy Star certified
16	Control panel display	20 m touchscreen

Laser Printer

Sl. No.	Parameter	Minimum Specifications
1	Print speed black (normal, A4)	Up to 25 ppm
2	Print quality black (best)	Up to 1200 x 1200 dpi
3	Print technology	Monochrome Laser
4	Duty cycle (monthly, A4)	Up to 15,000 pages
5	Recommended monthly page	volume 250 to 2000
6	Standard memory	Minimum 128 MB
7	Processor speed	Minimum 700 MHz
8	Paper handling standard/input	Up to 250-sheet input tray
9	Paper handling standard/output	Up to 150-sheet output bin
10	Media sizes supported	A4, A5, A6, B5, postcard
11	Media types supported	Paper, transparencies, postcards, envelopes, labels
12	Standard connectivity	Hi-Speed USB 2.0 port with USB data cable, Ethernet with RJ45 connectivity
13	Duplex printing	Automatic (standard)
14	Compatible operating systems	Microsoft Windows 7 Professional(64bit), Windows 8 Pro(64 bit), Windows 8.1, Windows 10, Server 2008 R2, Server 2012 R2, MAC OS 9.0, MAC OS X, Linux
15	Power requirements:	Input voltage 220 to 240 VAC (+/- 10%), 50 Hz (+/- 2 Hz);
16	Power consumption during printing	Less than 500W
17	Energy Efficiency	BEE or Energy Star certified

Sl. No.	Parameter	Minimum Specifications
18	Front operating Panel	Graphical LCD display

Projector

Sl. No.	Item	Minimum Specifications
1	Display Technology	Poly-silicon TFT LCD
2	Resolution	HD 1080p
3	Colours	16.7 million Colours
4	Brightness	2500 or more ANSI lumens (in Normal Mode)
5	Contrast Ratio	2000:1 or more
6	Video Input	One computer (D-Sub, Standard 15 pin VGA connector), One S-Video, One HDMI
7	Audio	Internal speaker
8	Output ports	External Computer Monitor port, audio ports
9	Remote Operations	Full function Infrared Remote Control
10	Other features	Auto source detect, Auto-synchronization, Keystone Correction

WAN Router

Sl. No.	Item	Minimum Specifications
1	Architecture	Router should have redundant control plane/routing engine and should support state full switchover, non-stop forwarding, Non-stop routing and Graceful restart.
		Router shall support sync any configurations from previous modules to new modules with hot-swap event occurred
		The router shall support following type of interfaces – 10GE, 1GE interfaces, 10G, Ch STM1
		Field replacement of port or card should not require to bring down the chassis.
2	Performance	Router shall support non-blocking capacity of 64 Gbps full duplex
		Router shall support 60 Mbps forwarding performance for IPv4 & IPv6 performance

		The router should support 20Gbps per slot throughput. Router shall support 16000 Mac addresses Router shall support 18000 IPv4/IPv6 routes Router shall support 4000 queues and 128 MPLS VPN's Router shall support aggregation of links. Minimum 8 links should be supported as part of single aggregation Router shall support IPSLA or equivalent and Y.1731 for performance monitoring
3	High Availability	Router should support Redundant Power Supply and should also support Online insertion and removal of same.
		Fan tray should be a Field Replaceable Unit (FRU). The node can run indefinitely with a single fan failure.
		Router shall support MPLS-TE with FRR for sub 50 msec protection.
		Router must support Traffic Engineering for node and link protection.
4	Protocol Support	Router should support following routing protocols: IPV4 and IPV6, IGMP V2/V3, MLD, IGMP V1,V2,V3 and PIM, 6PE, BGP, Policy Routing, OSPF V2 and V3
		Router should support high availability for all BFD,BGP ,OSPF and IS-IS and no packet loss during controller switch over.
		Router should support RFC 3107 of Carrying Label Information in BGP-4
		The Router should support Point to Point and Point to Multipoint LSP for Unicast and Multicast traffic.
		Router shall support layer3 and layer2 MPLS VPN.
5	QoS Features	Router shall support HQOS on all kind of interface in both ingress and egress direction. Similar QOS shall be supported for all type of interface including Bundled interfaces.
		Shall 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
		Shall support Strict Priority Queuing or Low Latency Queuing to support real-time application like Voice and Video with minimum delay and jitter.
		Congestion Management: WRED, Priority queuing, Class-based weighted fair queuing
6	Security & Management	Support Access Control List to filter traffic based on Source & Destination IP Subnet, Source & Destination Port, Protocol Type (IP, UDP, TCP, ICMP etc.) and Port Range etc. Should Support per-user Authentication, Authorization, and Accounting through RADIUS or TACACS and SNMPv1/v2/V3
7	Operating Environmental Requirements	0°C to 40°C operating temperature and 10 to 90%, non-condensing
8	Interface	The proposed router should support the following from day1: - 2x10G SFP+ ports supplied with 1x10G single mode transceiver, 1x10G multi-mode transceiver, 8x1G SFP ports supplied with 4x1G single mode transceiver, 4x1G multi-mode transceiver & 32 no's of 10/100/1000 Base-T ports.
9	Certifications/ OEM	The router should be IPv6 ready from day-1.

Internet and Aggregation Router

Sl. No	Minimum Specifications
1	Router should be chassis based device with minimum 10 Gbps of throughput scalable up to 20 Gbps. It should have minimum 4 GB of RAM/ DRAM
2	Router supports management protocol: SNMP v1/v2/v3, CLI (Telnet/Console), TFTP update and configured file management
3	Router must have inbuilt state full firewall, zone-based firewall and 3 DES capability technologies to support the access controller strategy based source and destination IP

	protocol port and time parameters
4	Router should have tunnelling protocols like IPsec VPN, GET VPN or equivalent, Multi Point VPN and encryption mechanisms like DES, 3DES, AES (128 and 256Bit).It should support minimum 300 IPsec tunnels from day one.
5	Router has support for the following routing /WAN protocols
6	PPP/MLPPP, HDLC
7	Router should be modular chassis based device and should accommodate a combination of high-density 10G, Gigabit Ethernet, Fast Ethernet
8	Router should support protocols like RIP, OSPF, BGP, VRRP/HSRP, 802.1q, GRE, ACL's and NAT MPLS, traffic engineering, EoMPLS or VPLS or equivalent, L2 VPN from day one
9	
10	Shall support the RIPng & BGP for IPv6, OSPFv3, MPLS, BGP from day one.
11	The router supports state full packet inspection supporting H.323, SIP and other application level gateway support
12	The state full firewall supports IPsec pass through
13	System shall support to provide the ability to filter and gather application information in a flexible manner from day one
14	Router should support QoS Classification and marking policy based routing, IP precedence, DSCP
15	QoS -congestion management WRED/RED, Priority queuing, class-based weighted for fair queuing
16	IP Access list to limit Telnet SNMP access to router
17	Multiple privilege level authentication for console and telnet access
18	Time-based ACL for controlled forwarding based on time of day for offices
20	Provides QoS features like traffic prioritization, differentiated services, and committed, and committed access rate, QoS Support, RSVP/WFQ/MRED. Router should be able to take pre-configured action on these events like changing routes, changing routing metric
21	Router supports for QoS Features for defining the QoS policies. Support for low latency queuing, Layer 2 and Layer 3 CoS/DSCP

22	Router should have multicast routing protocols support: IGMPv1, v2 (RFC2236) PIM-SM (RFC2362) and PIM-DM/ Multicast VLAN Registration
23	The following interface required from Day-1: 2x 10G SFP+ based ports loaded with single mode transceiver, 3*1GE & 3*1G SFP-based transceiver.
24	The router should be IPv6 ready

SAN Storage

Sl. No.	Parameter	Minimum Specifications
1	RAID Level	RAID Array supporting Raid Levels 0, 1, 5,0+1 / 10 or equivalent
2	Availability and Required Cache	Cache should be mirrored between Active-Active controllers on dedicated, redundant paths / links between the controllers. In case of power failure, the SAN array must be provided with cache protection mechanism to ensure no loss of data in cache by de-staging to disks, irrespective of duration of power outage. The Proposed SAN Array should be configured with at least 16 GB usable data cache or higher or as per proposed solution for storage
3	Reliability	The proposed SAN Array should be configured with No Single Point of Failure Architecture with Dual Controllers for redundancy and should support hot plug and hot swap of components online (including controllers, disks, power supplies, cooling fans etc.). Should have continuous system monitoring and shall support remote diagnostics / error reporting feature. It should also allow the recovery of data in transit in the event of failure
4	Drive interface	
5	Other Features	<ul style="list-style-type: none"> ▪ Box should be compatible of SAN environment ▪ The SAN Array should support intermixing of SAS / FC & NL-SAS / FATA/SATA-II Disks of various capacities and speeds ▪ Storage subsystem shall support 300GB/ 400 GB/ 600 GB or higher with 10K / 15 K RPM Fibre channel/ SAS drives or as per proposed backup solution & 600GB/750GB /1TB or higher SATA/FATA or equivalent disk drives in the same device array ▪ The storage array proposed should have an upgrade path

Sl. No.	Parameter	Minimum Specifications
		<ul style="list-style-type: none"> ▪ All the necessary software to configure and manage the storage space, RAID configuration, logical drives allocation, virtualization, snapshots (including snap clones and snap mirrors) for entire capacity etc. should be included. ▪ Must have redundant power supplies, batteries, cooling fans and data path and storage controller. ▪ Should support Non-disruptive component replacement of controllers, disk drives, cache, power supply, fan subsystem etc. ▪ Load balancing shall be able to be controlled by system management software tools. ▪ Should support the supplied storage and operating systems ▪ The storage system should be scalable from 2 PB. ▪ The storage array should support block level replication across storage arrays ▪ The storage array should support all the Operating System Platforms & Clustering ▪ Any software or license required to enable connectivity to these OS should be included ▪ Storage should support non-disruptive online firmware upgrade for both Controllers and disk drives. ▪ The storage array should support hardware based data replication at the Block level across all models of the offered family. ▪ The storage should provide automatic rerouting of I/O traffic from the host in case of primary path failure. ▪ Should provide for LUN masking, fiber zoning and SAN security ▪ Should support storage virtualization, i.e. Easy logical drive expansion. ▪ Storage should be supplied with virtualization license as per solution requirement ▪ Should support hot-swappable physical drive raid array expansion with the addition of extra hard disks ▪ Should be able to support clustered and individual servers at the same time.

Sl. No.	Parameter	Minimum Specifications
		<ul style="list-style-type: none"> ▪ Should be able to take "snapshots" of the stored data to another logical drive on a different Disk/RAID Group for backup purposes ▪ Should be configured with "snapshots and clone" ▪ The vendor must provide the functionality of proactive monitoring of Disk drive and Storage system for all possible hard or soft disk failure. Vendor should also offer storage performance monitoring and management software. ▪ The storage system shall be configured with GUI based management software as below: <ul style="list-style-type: none"> ▪ Monitor and manage the storage array Configuration ▪ Remote Storage base replication ▪ Storage front end port monitoring ▪ Disk Monitoring ▪ LUN management. ▪ Storage Component replacement, etc.
6	Note	All specifications stated are minimum required. Proposed system may have features over and above the minimum specification stated. Bidder should ensure that the performance of storage is not negatively affected

SAN Switch

Sl. No.	Minimum Specifications
1	The fibre channel switch must be rack-mountable. Thereafter, all reference to the 'switch' shall pertain to the 'fibre channel switch'
2	The switch to be configured with minimum of 96 ports 16 Gbps FC configuration backward compatible to 4/8
3	All 96 x FC ports for device connectivity should be 4/8/16 Gbps auto-sensing Fibre Channel ports
4	The switch must have redundant power supply & fan module without resetting the switch, or affecting the operations of the switch
5	The switch must be able to support non-disruptive software upgrade.
6	The switch must be able to support state full process restart

Sl. No.	Minimum Specifications
7	The switch must be capable of creating multiple hardware-based isolated Virtual Fabric (ANSI T11) instances. Each Virtual Fabric instance within the switch should be capable of being zoned like a typical SAN and maintains its own fabric services, zoning database, Name Servers and FSPF processes etc. for added scalability and resilience
8	The switch must support up to 32 Virtual Fabric Instances
9	The switch must be capable of supporting hardware-based routing between Virtual Fabric instances
10	The switch must support graceful process restart and shutdown of a Virtual Fabric instance without impacting the operations of other Virtual Fabric instances
11	The switch shall support Small Form Factor Pluggable (SFP) LC typed transceivers
12	The switch must support hardware ACL-based Port Security, Virtual SANs (VSANs)/ Virtual Fabric and Port Zoning
13	The Switch must support default zoning, port/WWN zoning, broadcast zoning
14	Should support features to automated configuration deployment and fabric configuration services
15	Inter-switch links must support the transport of multiple Virtual Fabrics between switches, whilst preserving the security between Virtual Fabrics
16	The switch must support routing between Virtual Fabric instance in hardware
17	The switch shall support FC-SP for host-to-switch and switch-to-switch authentication.
18	The switch must be able to load balance traffic through an aggregated link with Source ID and Destination ID. The support for load balancing utilizing the Exchange ID must also be supported
19	The switch must be equipped with congestion control mechanisms such that it is able to throttle back traffic away from a congested link
20	The switch must be capable of discovering neighbouring switches and identify the neighbouring Fibre Channel or Ethernet switches
21	The switch should support IPv6. It should support native switch based REST APIs
22	The bidder must provide at least 2 of these switches
23	The interface requirement mentioned here is the minimum. If the solution requires more number of interfaces (considering 100% redundancy) then the same should be quoted by the bidder

Rack

Sl. No.	Parameter	Minimum Specifications
1	Type	<ul style="list-style-type: none"> ▪ 19" 42U racks mounted on the floor ▪ Floor Standing Server Rack - 42U with Heavy Duty Extruded Aluminium Frame for rigidity. ▪ Two pairs of 19" mounting angles with 'U' marking ▪ Heavy Duty Top and Bottom frame of MS. ▪ Should be capable of carrying maximum load of 500 Kg. ▪ All racks must be lockable on all sides with unique key for each rack ▪ Shelf, Stationery 4 Sets per Rack
2	Power Distribution Units	<ul style="list-style-type: none"> ▪ 2 per rack ▪ Vertically Mounted, 32AMPs with 25 Power Outputs. (20 Power outs of IEC 320 C13 Sockets & 5 Power outs of 5/13Amp Sockets), Electronically controlled circuits for Surge & Spike protection, LED readout for the total current being drawn from the channel, 32AMPS MCB, 3KVAC isolated input to Ground & Output to Ground (2 No per Rack). Each power distribution unit should be with built in mechanism of trip in case of short circuit
3	Doors	Fully perforated front & rear mesh doors
4	Fans and Fan Tray	<ul style="list-style-type: none"> ▪ Fan 4 Nos. per Rack ▪ The Fans should switch on based on the Temperature within the rack. This unit should also include - Humidity & temperature sensor

Rack Server

Sl. No.	Parameter	Minimum Specifications

Sl. No.	Parameter	Minimum Specifications
1	Chipset	Intel C621 or equivalent or higher
2	Form Factor	Max. 2U rack mounted with sliding rails
3	CPU	Latest series/ generation of 64 bit x86 processors E5- 2640 or higher with Ten or higher Cores. Processor speed should be minimum 2.5 GHz. 2 processors per each physical server. Scalable up to up to 28 cores per processor
4	Memory Slots	24 DDR4 DIMM slots RDIMMS& LR DIMMS supporting speeds up to 2666MT/s. Optionally support up to 12 DIMM & 12 NVDIMM
5	Memory configured	Minimum 128 GB RAM, scalable to 1.5 TB
6	RAID Controller	12 Gbps PCIe 3.0 with RAID 1, 5, 6,10, 50
7	Disks configured	Minimum 8 x 2.5" SAS/SATA/SSD or 4 x 3.5" SAS/SATA
8	I/O slots	Up to 8x PCIe Gen3 Slots
9	GPU Support	Up to 3 DW and 6 SW GPU cards
10	Ethernet ports	4 x 1G RJ45 LOM
11	Certification and compliances	Microsoft Windows Server, Hyper-V, VMWare, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES) or as per solution
12	Power Supply	Redundant Power Supply
13	SD Modules slots	Dual SD Module slots supporting redundant configuration
14	Management integration	Support for integration with systems such as Microsoft System Centre, VMware vCentre, BMC Software et
15	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure

Sl. No.	Parameter	Minimum Specifications
16	Configuration & management	Real-time out-of-band hardware performance monitoring & alerting, Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of FC, HBA & CNA & system health Out-of-band hardware & firmware inventory Zero-touch auto configuration to auto deploy a baseline server configuration profile. Automated hardware configuration and Operating System deployment to multiple servers Zero-touch repository manager and self-updating firmware system, Virtual IO management / stateless computing, Support for Redfish API for simple and secure management of scalable platform hardware
17	HTML5 support	To Support HTML/ Java based KVM
18	Server security	<p>Should have a cyber-resilient architecture for a hardened server design for protection, detection & recovery from cyber attacks</p> <p>Should protect against firmware which executes before the OS boots</p> <ul style="list-style-type: none"> ▪ Should provide effective protection, reliable detection & rapid recovery using: ▪ Silicon-based Hardware Root of Trust ▪ Signed firmware updates ▪ Secure default passwords ▪ Configuration and firmware drift detection ▪ Persistent event logging including user activity ▪ Secure alerting § Automatic BIOS recovery ▪ Rapid OS recovery § System erase
19	Upgrades	Configuration upgrades should be only with cryptographically signed firmware and software
20	System lockdown	Should provide system lockdown feature to prevent change (or “drift”) in system firmware image(s) & prevent malicious modification of server firmware
21	Intrusion alert	Intrusion alert in case chassis cover being opened

Sl. No.	Parameter	Minimum Specifications
22	Warranty	3 years On-site comprehensive warranty with 24x7x365 remote hardware support. Post installation, 3-year product warranty should reflect in the support web site of the OEM

KVM Switch

Sl. No.	Parameter	Minimum Specifications
1	KVM Requirement	Keyboard, Video Display Unit and Mouse Unit (KVM) for the IT Infrastructure Management at Data Centre
2	Form Factor	19" rack mountable
3	Ports	Minimum 8 ports
4	Server Connections	USB or KVM over IP
5	Auto-Scan	It should be capable to auto scan servers
6	Rack Access	It should support local user port for rack access
7	SNMP	The KVM switch should be SNMP enabled. It should be operable from remote locations
8	OS Support	It should support multiple operating system
9	Power Supply	It should have dual power with failover and built-in surge protection
10	Multi-User support	It should support multi-user access and collaboration
11	Power Specification	200-240V, 50-60 Hz
12	Operating temperature range	0° to 45° C
13	Operating Relative Humidity range (non-condensing)	20 to 90% relative humidity
14	Total no. of ports on the proposed switch	24
15	Throughput of each FC port	8/16Gbps
16	Support for 4/8/16 Gb/s HBAs	YES

Sl. No.	Parameter	Minimum Specifications
17	Interface	Support for 4/8/16 Gb/s HBAs
18	Security	RADIUS, SSH, SNMP
19	Availability	No single point of failure Redundant Power supply

Backup Appliance

Sl. No.	Minimum Specifications
1	Appliance should support Inline deduplication and compression with up to 20:1 of data reduction ratio or higher
2	System should be configured with minimum 20 TB of physical usable capacity (non-dedupe) or higher
3	Should have minimum 3 TB/hr of transfer rate (data ingest speed) or higher
4	Should support CIFS & NFS protocol
5	Should have minimum 4 x 1 GbE ports, 2x 10GbE ports
6	System should be able to support loss of up to 3 disks at the same time
7	Should be compatible with all industry standard backup applications and must be supplied with required software
8	System should have inbuilt capability and configured with data replication to central location
9	System should support one to one, many to one, bidirectional replication topologies
10	Should support WORM feature for data protection & regulatory compliance
11	System should be configured with GUI for remote management & monitoring purpose
12	Should have a remote management port to manage the system in case system is down
13	System should support SNMP v1, v2c or higher and IPMI v2.0 Support
14	Should be able to generate Email alerts in case of any information, Warning & Error
15	Should be able to send system reports and logs via emails
16	Should have redundant fans and Hot-Swap redundant power supplies.
17	Form Factor : 2U rack mountable or better

Switching Fabric Architecture

Sl. No.	Parameter	Minimum Specifications
1	Fabric Definition	<ul style="list-style-type: none"> ▪ Fabric is the Clos Architecture defined using Spine, Leaf and VXLAN + ISIS or VXLAN + EVPN Protocol. ▪ Fabric should have following functionalities to be achieved: <ul style="list-style-type: none"> ▪ Flexibility: allows workload mobility anywhere in the DC. ▪ Robustness: while dynamic mobility is allowed on any authorized location of the DC, the failure domain is contained to its smallest zone. ▪ Performance: full cross sectional bandwidth (any-to-any) – all possible equal paths between two endpoints are active. ▪ Deterministic Latency: fix and predictable latency between two endpoints with same hop count between any two endpoints, independently of scale. ▪ Scalability: add as many Leaf as needed to achieve desired scale in terms of number of servers while maintaining the same oversubscription ratio everywhere inside the fabric.
2	Optics	Fabric should have Switch and Optics from same OEM/different OEM.
3	Fabric Features	<ul style="list-style-type: none"> ▪ Fabric must support various Hypervisor encapsulation without any additional hardware/software or design change. ▪ Fabric must auto discover all the hardware and auto provision the fabric based on the policy. ▪ The fabric architecture must be based on hardware VXLAN overlays to provide logical topologies that are abstracted from the physical infrastructure with no performance degradation. Fabric must support VXLAN

Sl. No.	Parameter	Minimum Specifications
		<p>Switching/Bridging and VXLAN Routing.</p> <ul style="list-style-type: none"> ▪ Fabric must provide open programmable interface using python SDK, Jason SDK, XMLS or COBRA etc. from the Central Management appliance / SDN Controller for programming/configuring the entire fabric. ▪ Fabric must provide open scripting interface using Bash, PowerShell, NetConf, YANG from the central management appliance / SDN Controller for configuring the entire fabric. ▪ Fabric must support Role Based Access Control in order to support Multi - Tenant environment. ▪ Fabric must integrate with different virtual machine manager and manage virtualise networking from the single pane of Glass - Fabric Controller/SDN Controller. ▪ Fabric must integrate with best of breed L4 - L7 Physical and virtual appliances and manage using single pane of glass - Fabric Controller / SDN Controller. ▪ Fabric must provide deeper visibility into the fabric in terms of latency and packet drop between VM to VM, VM to Physical server and vice versa, Leaf to another leaf etc. ▪ Fabric must act as single distributed layer 2 switch, Layer 3 router and Stateless distributed firewall etc. ▪ Fabric must provide REST APIs from the Central management appliance/SDN Controller in order to integrate with best of breed Management, Monitoring, Hypervisor and Cloud automation & Orchestration software.
4	Fabric Layer 2, Layer 3 and Misc. Features	<ul style="list-style-type: none"> ▪ Fabric must support Layer 2 features like LACP, STP /RSTP /MSTP, VLAN Trunking, LLDP etc. ▪ Fabric must support multi chassis ether channel/MLAG i.e. Host connects to two different Leaf switches and form ether channel using LACP/NIC Teaming on Host. ▪ Fabric must support Jumbo Frame up to 9K Bytes on

Sl. No.	Parameter	Minimum Specifications
		<p>1G/10G/25G/40G/100G ports.</p> <ul style="list-style-type: none"> ▪ Fabric must support Layer 2 Multicast i.e. IGMP v1, v2 and v3. ▪ Fabric must support IP v4 and IP v6 FHRP using HSRP or VRRP. ▪ Fabric must support IP v4 and IP v6 Layer 3 routing protocol OSPF and BGP. ▪ Fabric must support IP v6 dual stack. ▪ Fabric must support traffic redistribution between different routing protocols. ▪ Fabric must support IP v4 and IP v6 management tools like - Ping, Traceroute, VTY, SSH, TFTP and DNS Lookup. ▪ Fabric must support IP v4 and IP v6 SNMP V1 / V2 / V3. ▪ Fabric must support RMON/RMON-II for monitoring. ▪ Fabric must support integration with the centralised Syslog server for monitoring and audit trail. ▪ Fabric must support NTP.
5	Fabric Features	<p>Security</p> <ul style="list-style-type: none"> ▪ Fabric must have zero trust policy model for connected systems or hosts to help in protecting against any kind of attacks like Unauthorized Access, Man - in - the - middle - attack, Replay Attack, Data Disclosure, Denial of Service. ▪ Fabric must provide RBAC policies and support AAA using Local User authentication, External RADIUS, External TACACS+, External LDAP, External AD. ▪ Fabric must support VM attribute based zoning and policy. ▪ Fabric must support Micro Segmentation for the Virtualize and Non - Virtualize environment. ▪ Fabric must support true multi tenancy. ▪ Fabric must be accessible using CLI over SSH and GUI

Sl. No.	Parameter	Minimum Specifications
		<p>using HTTP/HTTPS</p> <ul style="list-style-type: none"> ▪ Fabric must support SNMP v2/3 with HMAC-MD5 or HMAC-SHA authentication and DES encryption. ▪ Fabric must act as a State-less distributed firewall with the logging capability.
6	Fabric Service Features	<ul style="list-style-type: none"> ▪ Fabric must be capable to provide services of L 4 - L7 services using physical or virtual appliances i.e. Firewall, ADC, IPS etc. ▪ Fabric must have zero trust policy model for connected systems or hosts to help in protecting against any kind of attacks like Unauthorized Access, Man - in - the - middle - attack, Replay Attack, Data Disclosure, Denial of Service.
7	Fabric Scale and Performance	<ul style="list-style-type: none"> ▪ Fabric should support scale up and scale out without any service disruption. ▪ Fabric must scale from 100 Tenant to 500 Tenant without any additional component or upgrade or design change. ▪ Fabric must integrate with minimum 3 Virtual Machine Manager (i.e. vCentre, SCVMM, OpenStack etc.) of different Hypervisors simultaneously and scalable to 5 in future with or without common orchestrator. ▪ Fabric must be capable of connecting 2500 physical servers and scale to 5000 physical servers. ▪ Fabric must be capable of integrating minimum of 8 nos. of L 4 - L7 services physical or virtual appliances (i.e. Firewall, ADC, IPS etc.) and scale up to 16 no's of L4 - L7 Services appliances. ▪ Fabric must support minimum of 4 Leaf switches and scale up to 250 Leaf switches without any design change. ▪ Fabric must support minimum of 2 Spine Switches and scale up to 6 Spine switches without any design change. ▪ Spine Switches must have adequate number of line rate 40/100G ports to support desired Leaf Scale.

Sl. No.	Parameter	Minimum Specifications
		<ul style="list-style-type: none"> ▪ Each Leaf connects to Each Spine using minimum 1 x 40/100 G ports connectivity i.e. Each Spine must have 128 nos. of line rate 40G/100G ports with consideration of leaf to SPINE over subscription ration of 4:1. ▪ Fabric must support 20K IPv4 and 10K IPv6 routes scalable to 30K IPv4 and 15K IPv6 routes. ▪ Fabric must support 4K multicast groups scalable to 8K multicast groups. ▪ Fabric must support 256 nos. of MLAG/VPC scalable to 384 nos. Each MLAG/VPC must support maximum 8-member links. ▪ Fabric must support 256 nos. of Port Channel scalable to 384 nos. Each Port Channel must support maximum of 8 member links.
8	Fabric Management	<ul style="list-style-type: none"> ▪ Fabric must provide Centralised Management Appliance or SDN Controller - Single pane of Glass for managing, monitoring and provisioning the entire Fabric. ▪ Fabric must Auto discover all the Spine and Leaf switches and auto provision them based on the Fabric policy using Centralised Management appliance or SDN Controller. ▪ Centralised management appliance or SDN Controller must manage and provision L4 - L7 Services physical or virtual appliance as well as integrate with Virtual Machine manager. ▪ Centralised management appliance or SDN Controller should not participate in Data plane and control plane path of the fabric. ▪ Centralised management appliance or SDN Controller must provide necessary report for compliance and audit. ▪ Centralised management appliance or SDN Controller must communicate to south bound devices using open standard protocol i.e. OPFLEX, OPENFLOW, OVSDB etc. or using Device APIs.

Sl. No.	Parameter	Minimum Specifications
		<ul style="list-style-type: none"> ▪ Centralised management appliance or SDN Controller communication with the south bound devices must be encrypted ▪ Centralised management appliance or SDN Controller must communicate with the south bound devices using more than one path i.e. in-path connectivity and out of band management connectivity ▪ Centralised management appliance or SDN Controller provide dynamic device inventory of the Fabric as well as current network topology of the fabric. It must also validate the cabling connectivity and generate alarms in case of wrong or faulty connectivity. ▪ Centralised management appliance or SDN Controller must run in "N + 1 or N + 2" redundancy to provide availability as well as function during the split brain scenario.

Spine Switch

Sl. No.	Parameter	Minimum Specifications
1	Solution Requirement	Minimum 2 number of Spine switches should be provided. If the solution requires more number of spine switches, the same shall be provided by the bidder.
2	General Requirement	<p>The core/spine layer switches should have hardware level redundancy (1+1) in terms of data plane and control plane. Issues with any of the plane should not impact the functioning of the switch. All the switches should be from same OEM.</p> <p>The switch should have redundant CPUs working in active-active or active-standby mode. CPU fail over/change over should not disrupt/impact/degrade the functioning the switch.</p> <p>The Switch should support non-blocking Layer 2 switching and</p>

Sl. No.	Parameter	Minimum Specifications
		Layer 3 routing The switch should not have any single point of failure like power supplies and fans etc. should have 1:1/N+1 level of redundancy Switch should support in line hot insertion and removal of different parts like modules/power supplies/fan tray etc. This should not require rebooting of the switch or create disruption in the working/functionality of the switch Switch should support the complete STACK of IP V4 and IP V6 services. Switch with different modules should function line rate and should not have any port with oversubscription ratio applied Switch should support upgradation of the operating systems of the switch without disturbing the traffic flow. There should not be any impact on the performance in the event of the software upgrade/downgrade. It should support in service patching of selected process/processes only without impacting other running processes Switch should support non-blocking, wire speed performance per line card
3	Hardware and Interface Requirement	Switch should have the following interfaces: 48 nos. of line rate and Non - Blocking 40/100G ports Switch should have min 60 MB buffer Switch should have console port for local management Switch should have management interface for Out of Band Management Switch should be rack mountable and support side rails, if required Switch should have adequate power supplies for the complete system usage with all slots populated and used, providing N+1 redundancy Switch should have hardware health monitoring capabilities and should provide different parameters through SNMP

Sl. No.	Parameter	Minimum Specifications
4	Performance Requirement	Switch should support VLAN tagging (IEEE 802.1q)
		Switch should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy
		Switch should have the capability of holding multiple OS images to support resilience & easy rollbacks during the version upgrades etc and should support in service software upgrade including:
		<ul style="list-style-type: none"> • Multiple System image • Multiple system configuration • Option of Configuration roll-back
		Switch should support for different logical interface types like loopback, VLAN, Port Channel, multi chassis port channel/Link Aggregation Group (LAG) etc.
		The switch should support at least 60,000 IPv4 and IPv6 or more routes entries in the routing table with multicast routes. The Bidder may propose best specification as per the proposed solution and city requirements.
		Switch should support Graceful Restart for OSPF, BGP etc.
		.
		The switch should support forwarding operation for OSPF, BGP etc. routing protocols to ensure high-availability during primary controller failure
		The switch should support hardware based load-balancing at wire speed using LACP and multi chassis ether channel/LAG
		Switch should support total aggregate minimum 3.2 Tbps minimum of switching capacity including the services: <ul style="list-style-type: none"> • Switching • IP Routing (Static/Dynamic) • IP Forwarding • Policy Based Routing • QoS • ACL and Other IP Services

Sl. No.	Parameter	Minimum Specifications
		<ul style="list-style-type: none"> IP V.6 host and IP V.6 routing
5	Virtualization Features	Switch should support Network Virtualisation using Virtual Over Lay Network using VXLAN (RFC 7348)/NVGRE as per RFC 2890
		Switch should support VXLAN (RFC7348) and EVPN or equivalent for supporting Spine - Leaf architecture to optimise the east - west traffic flow inside the data centre
		Switch should support Open Flow/Open Day light/Open Stack controller
		Switch should support Data Centre Bridging
		Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically
6	Layer2 Features	Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S)
		Switch should support VLAN Trunking (802.1q) and should support 4096 VLAN
		Switch should support basic Multicast IGMP v1, v2, v3
		Switch should support minimum 160,000 no. of MAC addresses
		Switch should support 16 Nos. of link or more per Port channel (using LACP) and support 48 port channels or more per switch
		Switch should support Industry Standard Port/Link Aggregation for All Ports across any module or any port.
		Switch should support multi chassis Link Aggregation for All Ports across any module or any port of the switch and Link aggregation should support 802.3ad LACP protocol for communication with downlink/uplink any third party switch or server. Spine to spine -minimum 16 port Multi Chassis ether channel/LAG should be provided.
		Switch should support Jumbo Frames up to 9K Bytes on 1G/10G Ports
		Support for broadcast, multicast and unknown unicast storm

Sl. No.	Parameter	Minimum Specifications
		<p>control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities</p> <p>Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures</p>
		<p>Switch should support all physical ports to use either in Layer2 or Layer 3 mode and also should support layer 3 VLAN Interface and Loopback port Interface</p> <p>Switch should support basic routing feature i.e. IP Classless, default routing and Inter VLAN routing</p>
		<p>Switch should support static and dynamic routing using:</p> <ul style="list-style-type: none"> • Static routing • OSPF V.2 using MD5 Authentication • ISIS using MD5 Authentication • BGP V.4 using MD5 Authentication • Should support route redistribution between these protocols • Should be compliant to RFC 4760 Multiprotocol • Extensions for BGP-4 (Desirable)
7	Layer3 Features	<p>Switch should re-converge all dynamic routing protocol at the time of routing update changes i.e. Non-Stop forwarding for fast re-convergence of routing protocols</p> <p>Switch should support MPLS routing</p> <p>Switch should be capable to work as DHCP server and DHCP relay</p> <p>Switch should provide multicast traffic reachable using:</p> <ul style="list-style-type: none"> • PIM-SM • PIM-SSM • Bi-Directional PIM • Support RFC 3618 Multicast Source Discovery Protocol (MSDP) • IGMP V.1, V.2 and V.3

Sl. No.	Parameter	Minimum Specifications
		Switch should support Multicast routing ECMP
8	Availability	Switch should have provisioning for connecting to 1:1/N+1 power supply for usage and redundancy
		Switch should provide gateway level of redundancy in IP V.4 and IP V.6 using HSRP/VRRP
		Switch should support for BFD For Fast Failure Detection
9	Quality of Service	Switch system should support 802.1P classification and marking of packet using: <ul style="list-style-type: none"> • CoS (Class of Service) • DSCP (Differentiated Services Code Point) • Source physical interfaces • Source/destination IP subnet • Protocol types (IP/TCP/UDP) • Source/destination TCP/UDP ports
		Switch should support methods for identifying different types of traffic for better management and resilience
		Switch should support for different type of QoS features for real time traffic differential treatment using: <ul style="list-style-type: none"> • Weighted Random Early Detection • Strict Priority Queuing
		Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy
		Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic as per IEEE 802.3x or should support nextgen flow control using VoQ.
10	Security	Switch should support for deploying different security for each logical and physical interface using Port Based access control lists of Layer-2 to Layer-4 in IP V.4 and IP V.6 and logging for fault finding and audit trail
		Switch should support control plane i.e. processor and memory Protection from unnecessary or DoS traffic by control plane

Sl. No.	Parameter	Minimum Specifications
		protection policy
		Time based ACL
		Switch should support for external database for AAA using: <ul style="list-style-type: none"> • TACACS+ • RADIUS
		Switch should support MAC Address Notification on host join into the network for Audit trails and logging
		Switch should support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding
		Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined
		Switch should support to prevent edge devices in the network not administrator's controlled from becoming Spanning Tree Protocol root nodes
		Switch should support unicast and/or multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port
		Switch should support Spanning tree BPDU protection
11	Manageability	Switch should support for embedded RMON/RMON-II for central NMS management and monitoring
		Switch should support for sending logs to multiple centralised syslog server for monitoring and audit trail
		Switch should provide remote login for administration using: <ul style="list-style-type: none"> ▪ Telnet ▪ SSH V.2
		Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures

Sl. No.	Parameter	Minimum Specifications
12	IPv6 features	<p>Switch should support for management and monitoring status using different type of Industry standard NMS using:</p> <ul style="list-style-type: none"> ▪ SNMP V1 and V.2 ▪ SNMP V.3 with encryption ▪ Filtration of SNMP using Access list ▪ SNMP MIB support for QoS
		<p>Switch should support for basic administrative tools like:</p> <ul style="list-style-type: none"> ▪ Ping ▪ Traceroute
		<p>Switch should support central time server synchronisation</p>
		<p>Switch should support for providing granular MIB support for different statistics of the physical and logical interfaces</p>
		<p>Switch should support for predefined and customized execution of script for device mange for automatic and scheduled system status update for monitoring and management</p>
		<p>Switch should provide different privilege for login in to the system for monitoring and management</p>
		<p>Switch should support Real time Packet Capture using Wireshark in real time for traffic analysis and fault finding</p>
12	IPv6 features	<p>Switch should support for IP V.6 connectivity and routing required for network reachability using different routing protocols such as:</p> <ul style="list-style-type: none"> • OSPF V.3 • BGP with IP V.6 • IP V.6 Policy based routing • IP V.6 Dual Stack etc • IP V.6 Static Route • IP V.6 Default route • Should support route redistribution between these protocols
		<p>Switch should support multicast routing in IP V.6 network using PIMv2 Sparse Mode/MLD/Equivalent</p>

Sl. No.	Parameter	Minimum Specifications
		Switch should support for QoS in IP V.6 network connectivity
		Switch should support for monitoring and management using different versions of SNMP in IP V.6 environment such as: <ul style="list-style-type: none"> • SNMPv1, SNMPv2c, SNMPv3 • SNMP over IP V.6 with encryption support for SNMP Version 3
		Switch should support syslog for sending system log messages to centralised log server in IP V.6 environment
		Switch should support NTP to provide an accurate and consistent timestamp over IPv6 to synchronize log collection and events

Leaf (Fiber) Switch:

Sl. No.	Parameter	Minimum Specifications
1	Solution Requirement	Minimum 4 number of switches should be provided. If the solution requires more number of spine switches, the same shall be provided by the bidder as per requirement.
2	General Requirement	<p>The Switch should support non-blocking Layer 2 switching and Layer 3 routing.</p> <p>There switch should not have any single point of failure like power supplies and fans etc. should have 1:1/N+1 level of redundancy</p> <p>Switch support in-line hot insertion and removal of different parts without disrupting the functionality of the system.</p> <p>Switch should support the complete STACK of IP V4 and IP V6 services</p> <p>The Switch and different modules used should function in line rate and should not have any port with oversubscription ratio applied.</p>
3	Hardware and Interface Requirement	<p>Switch should have the following interfaces:</p> <p>a. 48 x10G/25G Multi Mode Fiber Interface</p> <p>b. 6 x 40/100GbE QSFP ports</p> <p>Switch should have minimum 15 MB buffer or should have 8 hardware queues</p>

Sl. No.	Parameter	Minimum Specifications
		<p>Switch should have console port</p> <p>Switch should have management interface for Out of Band Management</p> <p>Switch should be rack mountable and support side rails if required</p> <p>Switch should have hardware health monitoring capabilities and should provide different parameters through SNMP</p> <p>Switch should support VLAN tagging (IEEE 802.1q)</p> <p>Switch should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy</p> <p>Switch should support Configuration roll-back and check point</p> <p>Switch should support for different logical interface types like loopback, VLAN, Port Channel, multi chassis port channel/LAG etc.</p>
		<p>The switch should support 1,00,000 IPv4 and 50,000 IPv6 routes entries in the routing table with multicast routes</p> <p>Switch should support Graceful Restart for OSPF, BGP etc.</p>
4	Performance Requirement	<p>The switch should support hardware based load balancing at wire speed using LACP and multi chassis ether channel/LAG</p> <p>Switch should support total aggregate minimum 2.4 Tbps minimum of switching capacity including the services:</p> <ul style="list-style-type: none"> a. Switching b. IP Routing (Static/Dynamic) c. IP Forwarding d. Policy Based Routing e. QoS f. ACL and Other IP Services g. IP V.6 host and IP V.6 routing <p>The Bidder may propose best specification as per the proposed</p>

Sl. No.	Parameter	Minimum Specifications
		solution and city requirements.
		Each leaf should have connectivity to all spine switches and the over subscription should not be less than 4:1
5	Advance Features	Switch should support Network Virtualisation using Virtual Over Lay Network using VXLAN (RFC 7348)/NVGRE as per RFC 2890
		Switch should support VXLAN (RFC7348) and EVPN or equivalent for supporting Spine - Leaf architecture to optimise the east - west traffic flow inside the data centre
		Switch should support Open Flow/Open Day light/Open Stack controller
		Switch should support Data Centre Bridging
		Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically
6	Layer2 Features	Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S)
		Switch should support VLAN Trunking (802.1q) and should support 4096 VLAN
		Switch should support basic Multicast IGMP v1, v2, v3
		Switch should support minimum 90,000 no. of MAC addresses. The Bidder may propose best specification as per the proposed solution and city requirements
		Switch should support 16 Nos. of link or more per Port channel (using LACP) and support 48 port channels or more per switch
		Switch should support Industry Standard Port/Link Aggregation for

Sl. No.	Parameter	Minimum Specifications
		All Ports across any module or any port.
		Switch should support multi chassis Link Aggregation for All Ports across any module or any port of the switch and Link aggregation should support 802.3ad LACP protocol for communication with downlink/uplink any third party switch or server. Spine to spine - minimum 16 port Multi Chassis ether channel/LAG should be provided.
		Switch should support Jumbo Frames up to 9K Bytes on 1G/10G Ports
		Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities
		Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures
7	Layer3 Features	Switch should support all physical ports to use either in Layer2 or Layer 3 mode and also should support layer 3 VLAN Interface and Loopback port Interface
		Switch should support basic routing feature i.e. IP Classless, default routing and Inter VLAN routing
		Switch should support static and dynamic routing using: a. Static routing b. OSPF V.2 using MD5 Authentication c. ISIS using MD5 Authentication d. BGP V.4 using MD5 Authentication e. Should support route redistribution between these protocols f. Should be compliant to RFC 4760 Multiprotocol Extensions for BGP-4 (Desirable)

Sl. No.	Parameter	Minimum Specifications
		<p>Switch should support MPLS routing</p> <p>Switch should be capable to work as DHCP server and DHCP relay</p> <p>Switch should provide multicast traffic reachable using:</p> <ul style="list-style-type: none"> a. PIM-SM b. PIM-SSM c. Bi-Directional PIM d. Support RFC 3618 Multicast Source Discovery Protocol (MSDP) e. IGMP V.1, V.2 and V.3 <p>Switch should support Multicast routing ECMP</p>
8	Availability	<p>Switch should have provisioning for connecting to 1:1/N+1 power supply for usage and redundancy</p> <p>Switch should provide gateway level of redundancy in IP V.4 and IP V.6 using HSRP/VRRP</p> <p>Switch should support for BFD For Fast Failure Detection.</p>
9	Quality of Service	<p>Switch system should support 802.1P classification and marking of packet using:</p> <ul style="list-style-type: none"> a. CoS (Class of Service) b. DSCP (Differentiated Services Code Point) c. Source physical interfaces d. Source/destination IP subnet e. Protocol types (IP/TCP/UDP) f. Source/destination TCP/UDP ports <p>Switch should support methods for identifying different types of traffic for better management and resilience</p> <p>Switch should support for different type of QoS features for real time traffic differential treatment using</p> <ul style="list-style-type: none"> a. Weighted Random Early Detection b. Strict Priority Queuing

Sl. No.	Parameter	Minimum Specifications
10	Security	Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy
		Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic.
		Switch should support for deploying different security for each logical and physical interface using Port Based access control lists of Layer-2 to Layer-4 in IP V.4 and IP V.6 and logging for fault finding and audit trail
		Switch should support control plane i.e. processor and memory Protection from unnecessary or DoS traffic by control plane protection policy
		Time based ACL
		Switch should support for external database for AAA using: a. TACACS+ b. RADIUS
		Switch should support MAC Address Notification on host join into the network for Audit trails and logging
		Switch should support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding
		Switch should support to prevent edge devices in the network not administrator's controlled from becoming Spanning Tree Protocol root nodes
		Switch should support unicast and multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port
		Switch should support Spanning tree BPDU protection
11	Manageability	Switch should support for embedded RMON/RMON-II for central NMS management and monitoring

Sl. No.	Parameter	Minimum Specifications
		Switch should support for sending logs to multiple centralised syslog server for monitoring and audit trail
		Switch should provide remote login for administration using: a. Telnet b. SSH V.2
		Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures
		Switch should support for management and monitoring status using different type of Industry standard NMS using: a. SNMP V1 and V.2 b. SNMP V.3 with encryption c. Filtration of SNMP using Access list d. SNMP MIB support for QoS
		Switch should support for basic administrative tools like: a. Ping b. Traceroute
		Switch should support central time server synchronisation
		Switch should support for providing granular MIB support for different statistics of the physical and logical interfaces
		Switch should support for predefined and customized execution of script for device mange for automatic and scheduled system status update for monitoring and management
		Switch should provide different privilege for login in to the system for monitoring and management
		Switch should support Real time Packet Capture using Wireshark in real time for traffic analysis and fault finding

Sl. No.	Parameter	Minimum Specifications
12	IPv6 features	<p>Switch should support for IP V.6 connectivity and routing required for network reachability using different routing protocols such as:</p> <ul style="list-style-type: none"> a. OSPF V.3 b. BGP with IP V.6 c. IP V.6 Policy based routing d. IP V.6 Dual Stack etc. e. IP V.6 Static Route f. IP V.6 Default route g. Should support route redistribution between these protocols
		Switch should support multicast routing in IP V.6 network using PIMv2 Sparse Mode/ MLD/Equivalent
		Switch should support for QoS in IP V.6 network connectivity
		Switch should support for monitoring and management using different versions of SNMP in IP V.6 environment such as:
		<ul style="list-style-type: none"> a. SNMPv1, SNMPv2c, SNMPv3 b. SNMP over IP V.6 with encryption support for SNMP Version 3
		Switch should support syslog for sending system log messages to centralised log server in IP V.6 environment
		Switch should support NTP to provide an accurate and consistent timestamp over IPv6 to synchronize log collection and events
		Switch should support for IP V.6 different types of tools for administration and management such as:
		<ul style="list-style-type: none"> a. Ping b. Trace route c. VTY d. SSH e. DNS lookup

Web Security Appliance:

Sl. No.	Parameter	Minimum Specifications
1	Appliance Requirement and Functionality	The solution should be a hardened Web Proxy, Caching, Web based Reputation filtering, URL filtering, Antivirus and Anti-malware appliance. All the functionalities should be in a single appliance only.
2	Hardware	Minimum of 1 * 6-core CPUs, 2.4 TB storage, RAID 10, 32 GB or more DRAM, hot-swappable hard drive
3	Operating System	The appliance based Solution shall provide hardened Operating System.
4	Operating System Performance	The underlying operating system and hardware should be capable of supporting at least 2000 users from day with licenses & scalable up to 5000 users.
5	Operating System Security	The operating system should be secure from vulnerabilities and hardened for web proxy and caching functionality.
6	IP V6 Support	Should have the ability to proxy, monitor, and manage IPv6 traffic.
7	Forward proxy mode	The solution should support explicit forward proxy mode deployment in which client applications like browsers are pointed towards the proxy for web traffic.
8	Proxy support	The proposed solution should be a Fast Web Proxy and should support HTTP, FTP and HTTPS proxy.
9	HTTPS Decryption	The solution should support HTTPS decryption
10	HTTPS decrypted traffic scanning	The solution should support scanning of the https decrypted traffic by the on-board anti-malware and/or anti-virus engines.
11	HTTPS decryption policy	HTTPS decryption should provide flexibility to have multiple decryption policies and should not be just a Global action

Sl. No.	Parameter	Minimum Specifications
12	Proxy Chaining	The solution should support proxy configuration in a Chain. The Lower end proxies at spoke locations should be able to forward the request to an Higher end proxies at Hub Location forming a Chain of Proxies
13	DNS Splitting	The solution should support configuration to use Split DNS. It should be able to refer to different DNS for Different Domains e.g. (root dns for all external domains and internal DNS for organization domain
14	IP Spoofing support in transparent mode deployments	The solution should have facility to do IP spoofing. When enabled, requests originating from a client should retain the client's source address and appear to originate from the client instead of the appliance. This is useful in scenarios where policies are based on original IP and logging/reporting is required to track activity of individual IP basis.
15	Transparent mode	The solution should also support transparent mode deployment using WCCP v2 and L4 switches/PBR (Policy-based Routing)
16	Pac File support	The appliance should support hosting proxy auto-config files that defines how web browsers can automatically choose the appropriate web proxy for fetching a URL.
17	Support multiple deployment options	The solution should allow to deploy the appliance in explicit proxy as well as transparent mode together.
18	Remote support	The remote support from principal company should be available via India Toll Free and Email. The Support Portal access should be provided for Case management, knowledgebase, new version information, tools etc.
19	Secure Remote Access	The Support Engineers should be able to login to appliance using secure tunnelling methods such as SSH for troubleshooting purposes
20	High Availability	Provision of active/active High Availability is required

Sl. No.	Parameter	Minimum Specifications
21	Application and Protocol Control	The solution should support granular application control over web eg. Facebook controls like block file upload, block posting text, enforcing bandwidth limits on application types.
22	File download and size restrictions	The solution should be capable of blocking specific files downloads and based on size and per user group basis. It should also provide option to block object using MIME File types.
23	IP based Access Control	The solution should allow administrator to define access to internet based on IP addresses, range of IP addresses, subnet and CIDR basis. It should also support to be forced for Authentication from Specific IP addresses, Subnet or CIDR's
24	User based Access Control	The solution should support integration with active directory and/or LDAP. This should allow administrator to define user or group based access policies to Internet
25	Multiple Authentication Server Support	The solution should support Multiple Auth Servers / Auth Failover using Multi Scheme Auth (NTLM and LDAP). It should also support authentication exemption.
26	Layer 4 Traffic Monitoring	Should detect Phone Home attempts occurring from the entire Network. It should support actions to allow traffic to & from known malware addresses & should support from known allowed & unlisted addresses & block traffic to & monitoring suspected malware addresses.
27	Bandwidth restrictions	The solution should support providing bandwidth limit/cap for streaming media application traffic. This should be possible at the Global level as well as at a per policy level.

Sl. No.	Parameter	Minimum Specifications
28	Anti-Malware	The appliance should support at least 2 industry known Anti Malware/Anti-Virus engine that can scan HTTP, HTTPS and adware, browser hijackers, phishing and pharming attacks to FTP traffic for web based threats, that can range from more malicious threats such as rootkits, Trojans, worms, system monitors and Key loggers and as defined by the organizations policy. Please mention the antimalware engine.
29	Malware Protection	With dual AV/Anti-Malware engine scanning when a URL causes different verdicts from the scanning engine the appliance should perform the most restrictive action.
30	Web Reputation	The solution should provide Web Reputation Filters that examine every request made by the browser (from the initial HTML request to all subsequent data requests) – including live data, which may be fed from different domains to assign a web based score to determine the likelihood that it contains url-based malware.
31	Customizable Web Reputation	The Appliance should have customizable setting in the Web Based Reputation Services, like Allow, Scan and Block based on the scoring settings by the Administrator.
32	Incoming/Outgoing Traffic scanning	The solution should scan for Incoming and outgoing traffic.
33	Outbound connection control on all ports and protocols	The solution shall provide option to scan all ports at wire speed, detecting and blocking spyware activity trying to connect to the outside Internet. By tracking all 65,535 network ports and all protocols, the solution shall effectively mitigate malware that attempts to bypass Port 80
34	Custom URL filtering	The solution should support creation of custom URL categories for allowing/blocking specific destinations as required by the Organisation.

Sl. No.	Parameter	Minimum Specifications
35	URL Filtering Options	The web Proxy should support following actions like allow, monitor, block, time-based access. Should also support displaying a warning page but allows the user to continue clicking a hypertext link in the warning page.
36	URL check & submission	Support portal should give facility to end user to check URL category and submit new URL for categorization
37	Dynamic Categorization	Provision should be available to enable Real Time Dynamic categorization that shall classify in real time in case the URL the user is visiting is not already under the pre-defined or custom categories database.
38	Reporting MIS-categorization	The solution should have facility for End User to report Mis-categorisation in URL Category.
39	Filtering Content	Solution should support filtering adult content from web searches & websites on search engines like Google.
40	Signature based application control	The solution should support signature based application control.
41	End User Notification	Solution should support following end user notification functionalities. The proxy should support the functionality to display a custom message to the end user to specify the reason the web request is blocked.
		When the website is blocked due to suspected malware or URL-Filters it should allow the end user to report that the webpage has been wrongly misclassified.
		The solution should support the functionality of redirecting all notification pages to a custom URL to display a different block page for different reasons.
		Should support the functionality to force users to explicitly agree to the terms and conditions for browsing the World Wide Web from the organization's network to let the user know that the Organisation is monitoring their web activity.

Sl. No.	Parameter	Minimum Specifications
42	Diagnostic Tools	The appliance should have diagnostic network utilities like telnet, traceroute, nslookup and tcpdump/packet capture.
43	Updates and Upgrades	The appliance should provide seamless version upgrades and updates.
44	Secure Web Based management	The appliance should be manageable via HTTP or HTTPS
45	CLI based management	The appliance should be manageable via command line using SSH
46	Serial Console access	For emergency, the appliance should have serial console access
47	Ethernet Management	Should have provision for separate Ethernet for managing the appliance
48	Web Logs	The Proxy Log should be scalable. The log formats shall include Apache, Squid and W3C.
49	Retention Period	The retention period should be customizable. Options should be provided to transfer the logs to an FTP using FTP or SCP.
50	User Reports	Informative and exhaustive set of reports on User Activity and URL filtering activities (GUI to report past activity, top usage users and top malware threat)
51	Bandwidth Reports	Reports on Bandwidth Consumed / Bandwidth Saved
52	Detailed logging	Product to maintain detailed proxy access logs that can be searched via filters, for easy location of any desired access of the user and to see how the product dealt with it
53	Blocked by reputation & malware reports	It should support reporting web requests blocked due to web reputation & blocked by malware
54	Report Formats	Solution should support generating a printer-friendly formatted pdf version of any of the report pages. Should also support exporting reports as CSV files.
55	Scheduling of Reports	Solution should support to schedule reports to run on a daily, weekly, or monthly basis.

Sl. No.	Parameter	Minimum Specifications
56	System Reports	Should support system reports to show CPU usage, RAM usage, percentage of disk space used for reporting & logging.
57	Updates and Upgrades	Support should cover all upgrades for the time period the licenses and support purchased from principal vendor

HSM:

Sr No.	Specifications
Functional Capabilities	
(a)	Must support cryptographic offloading and acceleration
(b)	Should provide Authenticated multi-level access control
(c)	Must have strong separation of administration and operator roles
(d)	Capability to support hardened and hardware based client authentication mechanism with HSM
(e)	Must have secure key wrapping, backup, replication and recovery
(f)	Must support unlimited protected key storage
(g)	Must support clustering and load balancing
(h)	Should support unlimited Logical cryptographic separation of application keys
Application Program Interfaces (APIs)	
(a)	PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI and CNG
Host connectivity.	
(a)	Dual Gigabit Ethernet ports
Cryptography	
(a)	Asymmetric public key algorithms: RSA, Diffie-Hellman, DSA, KCDSA, ECDSA, ECDH
(b)	Symmetric algorithms: AES, ARIA, DES, Triple DES, SEED
(c)	Hash/message digest: SHA-1, SHA-2
Security compliance	
(a)	FIPS 140-Level 3
Safety and environmental compliance	
(a)	Compliance to UL, CE, ULL, C-TICK
(b)	Compliance to RoHS2, WEEE
(c)	IPv6 compliant
Management and monitoring	

(a)	Support Remote Administration
(b)	Syslog diagnostics support
(c)	Command line interface (CLI)/graphical user interface (GUI)
(d)	Support SNMP monitoring agent
Physical characteristics	
(a)	Standard 1U 19" Rack Mount
Performance	
(a)	RSA 2048 Signing performance - upto 5000 RSA 2048 Key generation performance - 15
Custom Application	
(a)	Should enable secure execution of custom security
Key Generation and Protection	
(a)	Ability to generate RSA keys (2048) and shall be secured by high security module in accordance with FIPS 140-2 level 3 recommendations for Cryptographic Modules Validation.
Key back up and restoration	
(a)	The proposed solution must include the software/hardware to - securely store the keys at DC, at DR and at one remote location and restore them in case of necessity
No. of Keys to be protected	
(a)	The HSM must secure a minimum of 1 lakh keys in accordance with FIPS 140-2 level 3 standards. The licensing and HSM hardware must have no restriction on the number of keys to be protected
Performance upgrade of HSM	
(a)	The performance of HSM should be upgradable on field.
Logical partitions	
(a)	Unlimited logical/cryptographic separation of application keys.

Anti-APT

Sl. No.	Minimum Specifications
1.	Anti-APT solution should be appliance based and should offer a minimum throughput of 2 Gbps
2.	Appliance should support at least 8*1Gbps ports
3.	Appliance shall provide a separate management port and should also provide a web-based GUI management
4.	Appliance should provide at least 1 Million concurrent sessions or 1000 concurrent users

Sl. No.	Minimum Specifications
5.	Appliance should have redundant power supplies
6.	Solution should be capable of blocking call backs to CnC Servers
7.	Solution should be capable of blocking threats based on both signatures and behaviour
8.	Proposed solution's detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.
9.	Proposed solution should be capable of blocking threats on the following protocols: HTTP, HTTPS
10.	The solution should be capable of executing MS Office Documents, Portable Documents, Archive Files, Multimedia Files and executable binaries in a virtual sandbox environment
11.	The solution should be capable of exempting specific hosts from specific compliance rules and suppressing corresponding compliance events and alerts.
12.	<p>The solution should be capable of gathering Active Directory user identity information, mapping IP addresses to username and passively gathering information about network devices including but not limited to:</p> <ul style="list-style-type: none"> • Network protocols used, e.g. IPv6, IPv4 • Network services provided, e.g. HTTPS, SSH • Open ports, e.g. TCP:80 • Client applications installed and type, e.g. Chrome - web browser • Web applications access, e.g. Facebook, Gmail • Risk and relevance ratings should be available for all applications • Potential vulnerabilities • Current User • Device type, e.g. Bridge, Mobile device • Files transferred by this device/user
13.	The solution should be capable of whitelisting trusted applications from being inspected to avoid business applications from being affected & in turn productivity
14.	The solution should be capable of blocking traffic based on geo locations to reduce the attack landscape and to protect communication to unwanted destinations based on geography
15.	The sandbox should be appliance based with the ability to run multiple versions of Operating Systems
16.	All the devices shall be managed centrally and should be capable of

Sl. No.	Minimum Specifications
	<ul style="list-style-type: none"> ▪ Centralized, life cycle management for all sensors ▪ Aggregating all events and centralized, real-time monitoring and forensic analysis of detected events ▪ Must provide a highly customizable dashboard
17.	The sandbox should be appliance based with the ability to run multiple versions of Windows within the same environment
18.	The Sandbox should be a proprietary custom-built malware analysis solution and not open source or generic sandbox
19.	<p>The Sandbox should be a proprietary custom-built malware analysis solution and not open source or generic sandbox and should provide:</p> <ul style="list-style-type: none"> - analysis reports - threat score of the sample - ability to queue samples, - impact analysis - Global Threat Intelligence - Sandbox shall be able to detect memory residing malware
20.	The proposed solution shall have the capability to continuously track a file's disposition based on global intelligence and do a retrospective block and alert if the file has exhibited malicious traits globally even if the file hasn't started behaving maliciously locally
21.	The solution should include protection against desktop and server & should support all the Operating Systems.

Firewall with IPS & URL Filtering

Sl. No.	Minimum Specifications
1	Hardware Architecture
	The appliance-based security platform should be capable of providing firewall, application visibility, and IPS functionality in a single appliance
	The appliance should support at least 2 * 10G ports scalable up to 8x10G, the firewall should be modular in nature so that it can be scalable

	The appliance hardware should be a multicore CPU architecture with a hardened 64-bit operating system to support higher memory
	Proposed Firewall should be open architecture based on multi-core CPU's to protect & scale against dynamic latest security threats.
2	Performance & Scalability
	Should support at least 10 Gbps of production performance / multiprotocol combined firewall & IPS throughput
	Firewall should support at least 20 Million concurrent sessions
	Firewall should support at least 200,000 connections per second
	Firewall should support at least 1000 VLANs
3	Firewall Features
	Firewall should provide application detection for DNS, FTP, HTTP, SMTP,ESMTP, LDAP, MGCP, RTSP, SIP, SCCP, SQLNET, TFTP, H.323, SNMP
	Firewall should support creating access rules with IPv4 & IPv6 objects simultaneously
	Firewall should support operating in routed & transparent mode
	Should support Static, RIP, OSPF, OSPFv3 and BGP
	Optionally, Firewall should support manual NAT (Network Address Translation) and Auto-NAT, static nat, dynamic nat, dynamic pat
	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality
	Firewall should support Multicast protocols like IGMP, PIM, etc.
	Should support security policies based on security group names in source or destination fields or both
	Should support capability to limit bandwidth on basis of apps/groups, Networks / Geo, Ports, etc.
4	High-Availability Features

	Firewall should support Active/Standby failover
	Firewall should support ether channel or equivalent functionality for the failover control & date interfaces for providing additional level of redundancy
	Firewall should support redundant interfaces to provide interface level redundancy before device failover
	Firewall should support 802.3ad Ether channel or equivalent functionality to increase the bandwidth for a segment.
	Firewall should have redundant power supply.
5	Next Generation IPS
	Should have the capability of passively gathering information about virtual machine traffic, network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.
	Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.
	Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.
	Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.
	Should be capable of detecting and blocking IPv6 attacks.
	Should support the capability to quarantine end point
	The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reputation of IP addresses determined by the proposed security vendor
	The solution must support IP reputation intelligence feeds and custom lists of IP addresses including a global blacklist.
	Should must support URL and DNS threat feeds to protect against threats

	Should support reputation and category based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies in more than 75 categories.
	The solution must be capable of passively gathering details unique to mobile devices traffic to identify a wide variety of mobile operating systems, mobile applications and associated mobile device hardware.
	Should support more than 2500 application layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.
	Must be capable of providing network-based detection of malware by checking the disposition of known files in the cloud using the SHA-256 file-hash as they transit the network and capability to do dynamic analysis on-premise (if required in future) on purpose built appliance
	The Appliance OEM must have its own threat intelligence analysis centre and should use the global footprint of security deployments for more comprehensive network protection.
	The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).
	Should be able to identify attacks based on Geolocation and define policy to block on the basis of Geo-location
	The detection engine should support the capability of detecting variants of known threats, as well as new threats
	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioural anomaly detection techniques. Identify and explain each type of detection mechanism supported.
	Should support access to community resources and ability to easily customize security to address new and specific threats and applications quickly
	The integrated solution should also provide URL filtering functionality for up to 200 million URL's, up to 60 different categories for URL

6	Management
	The management platform must be accessible via a web-based interface and ideally with no need for additional client software
	The management platform must provide a highly customizable dashboard.
	The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows
	The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.
	Should support REST API for monitoring and config programmability
	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.
	The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).
	The management platform must provide robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.
	The management platform must risk reports like advanced malware, attacks and network
	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications.

L2 PoE/PoE+ Switch

Sl. No.	Minimum Specifications
1	19" Rack Mountable stackable switch with min 24 Nos. 10/100/1000 POE ports with redundant power supply/ equivalent or higher

Sl. No.	Minimum Specifications
2	Switch should support for minimum 56 Gbps of forwarding throughput & minimum 70 mbps forwarding rate
3	The switch should support dedicated stacking port separate from uplink ports with 40 Gbps of stacking bandwidth to put minimum 8 switches into a single stack group.
4	Switch should have static, default IP routing enabled from day one.
5	Switch shall have IEEE 802.3ad Link Aggregation Control Protocol (LACP) with up to 8 links (ports) per trunk.
6	It shall have IEEE 802.1s Multiple Spanning Tree Protocol and provide legacy support for IEEE 802.1d STP and IEEE 802.1w RSTP or equivalent technology and static routes.
7	Switch should have feature to protect access ports using port security, TACACS/TACACS+, Radius, storm control, Access Control List both port, VLAN based.
8	Switch should have queuing as per IEEE 802.1P standard on all ports with mechanism for traffic shaping and rate limiting features for specified Host, network, Applications etc.
9	Should have Power supply 230 Volt 50Hz input
10	The switch should support IPv6 Guard, IPv6 RA-Guard, IPv6 DHCP- Guard, Source-Guard features
11	Switch should support automated image installation, configuration & automatic configuration of per port QoS to reduce switch provisioning time & effort.
12	Must have SNMP v1, v2, v3 from day one
13	Should have CLI and GUI based management console port.
14	The switch should support IEEE 802.3az from day-1
15	The switch should be IPv6 ready

Fixed Camera with Outdoor Housing and Lens – 2MP - JICCC

Sl. No.	Parameter	Minimum Specifications
1	Image sensor	1/2.7"Progressive Scan CMOS or better
2	Lens	CS Mount: 5-50mm, DC-Iris, Megapixel IR corrected Lens
3	True Day and Night	Yes

Sl. No.	Parameter	Minimum Specifications
4	Minimum Illumination / Light Sensitivity	Color: 0.01 lux color/ B/W: 0.001 lux F1.4 or Better
5	IR Filter	Automatic Built in IR Cut filter
6	Shutter Speed	1/25s to 1/15000
7	Video Compression	H.264 or H.265 High, Main, Base profile and MJPEG
8	Resolutions and frame rates	1920 x 1080
9	Video Streams	Minimum 3 Streams @ 1920x1080, H265, 25 fps
10	Power Supply	Power over Ethernet (PoE/PoE+) IEEE 802.3af Class 2
11	Digital I/O (Alarms)	DI x 1 DO x 1
12	Local storage	SD Card Slot with 128GB Support
13	Image Settings	Color, Brightness, Sharpness, Contrast, White balance, Image Mirroring, Text and image overlay, Privacy mask, Rotation: 0°, 90°, 180°, 270°, Exposure control, Exposure zones, Fine tuning of behaviour at low light, Mirror Image
14	Supported Protocol	IPv4 & v6, HTTP, HTTPS, SSL/TLS, QoS Layer 3 DiffServ, FTP, SMTP, UPnP ,SNMPv1/v2c/v3(MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SSH
15	Security	IEEE 802.1x, IP Address Filter, Password Protection, Digest Authentication
16	ONVIF	Profile S
17	API	The interface shall be available for integration with 3rd party analytics and applications in public domain free of cost
18	Operating Conditions	- 10°C to 50°C, Humidity 10–90 % RH
19	Privacy Mask	Required with Minimum 2 Zones
20	Image Configuration	The camera allows include/ exclude area in any shape in order to reduce false alarms and bandwidth/ storage

Sl. No.	Parameter	Minimum Specifications
21	GOV Length	It is possible to vary the GOV length in the camera setting for better control on bandwidth
22	Wide Dynamic Range	Minimum 100 dB True or Better
23	Event Triggers	Motion Detection, Edge storage events, External Input, Time Scheduled, Camera Tampering, Software alarms.
		The camera shall be able to send and received trigger directly from any other camera without interface of VMS.
24	Event Actions	FTP or HTTP or network share, EMAIL, Notification via HTTP to other camera or device, Pre and post alarm video buffering, External Output Trigger, PTZ Pre-set, Guard Tour
25	Firmware Upgrade	The firmware upgrade shall be done through web interface, The firmware is available free of cost
26	Embedded Applications	The camera shall provide a platform allowing the upload of third party applications into the camera
28	Housing	IP 66 Rated IK 8/10 rated for outdoor use or better
29	Certifications	CE, FCC, IEC, EN, UL
30	Warranty	3 years OEM warranty

High Definition PTZ Dome Camera (JICCC building)

Sl. No.	Parameter	Minimum Specifications
1	Image Sensor	1/2.8" Progressive Scan CMOS or better
2	Operating Frequency	Min 50 Hz
3	Day/ Night Operation	Automatic with IR Cut Filter
4	Minimum Illumination	Colour: 0.05 Lux
		B/W": 0 Lux or better
5	high-speed pan-tilt functionality	360° endless pan range and a 180° tilt range or better
6	Optical Zoom	30x Minimum & 12x Digital Zoom, Total 360x Zoom or better
7	Lens	4.5-129 mm or better
8	Pan, tilt, manual and	Auto 360° endless pan range and a 160° tilt range or better

Sl. No.	Parameter	Minimum Specifications
	preset speed	Manual Pan: 0.5°/s - 240°/s; Manual Tilt: 0.5°/s - 120°/s; preset speed: 240 °/s or better
	The speed shall be applicable for Manual, Tour and Pre-set Mode	
9	Image Resolution	1920 x 1080 or better
10	Compression	H.264/H.265 Baseline, Main and High Profiles, Motion JPEG
11	Frame Rate and Bit Rate	25 FPS at all resolutions with Controllable Bit Rate/ Bandwidth and Frame Rate. In CBR Priority to be defined for Video quality or frame rate and the bandwidth upper limit shall not exceed the defined limit
12	GOP/ GOV	Ability to change the GOP/GOV Length to optimize the bandwidth and storage
13	Video Streams	Minimum 3 Streams @ 1920x1080, H265, 25 fps
14	Motion Detection	Yes built in with multiple configurable areas in the video stream
15	Electronic Shutter	1/10000 s to 1 s or better
16	Electronic Exposure & Control	Automatic/ Manual
17	Wide Dynamic Range	100 dB or Better
18	Backlight Compensation	Required
19	Electronic Image Stabilization	Required
20	Image Freeze on PTZ	Required
21	Privacy Masks	Minimum 8 configurable 3D zones or better
22	Pre-set Positions	Minimum 256 or better
23	Image Flip	Yes Automatic
24	Guard Tour	Minimum 2 Nos
25	Built In Heater & FAN	Required
26	Temperature Control	Required
27	Audio	Two Way
28	Alarm	Min 2 Alarm input/ Output ports or better

Sl. No.	Parameter	Minimum Specifications
29	On-screen directional indicator	Required
30	Compression	<p>The camera shall support H.264/H.265 implementation support scene adaptive bitrate control, in order to lower bandwidth and storage requirements.</p> <p>The camera shall support automatic dynamic GOP for optimal bitrate utilization. The camera shall support automatic dynamic ROI to reduce bitrate in un-prioritized regions.</p>
31	Event Triggers	<p>The camera shall be able to send and receive trigger directly from any other camera without interface of VMS.</p> <p>Live Stream Accessed, Motion Detection, Shock</p> <p>Detection, Audio Detection, Network, Temperature, Manual Trigger, Virtual Inputs, Alarm Inputs, PTZ: Error, Moving, Preset Reached, Ready, Storage Disruption, Storage Recording, System Ready, User schedule</p>
32	Event Actions	<p>File upload via FTP, SFTP, HTTP and email</p> <p>Notification via email, HTTP and TCP</p> <p>Pre- and post-alarm video buffering, External output activation, PTZ present, guard tour, Video recording to edge storage, Day/night</p> <p>mode, Overlay text</p>
33	Pixel Counter	Built in
34	Edge Storage	Built in SD card slot with support up to 128 GB with Class 10 speed
35	Storage	The Cameras shall have the feature to directly record the videos/images onto storage without any Software
36	Protocols	At least IP, HTTP, HTTPS, SSL/TLS, TCP, ICMP, SNMPv1/v2c/v3 (MIB-II), RTSP, RTP, UDP, IGMP, RTCP, SMTP, FTP, DHCP, UPnP, ARP, DNS, DynDNS, NTP, IPv4 & IPv6
37	Text Overlay	Date & time, and a customer-specific text, camera name, graphical image etc.

Sl. No.	Parameter	Minimum Specifications
38	Security	Password protection, IP address filtering, HTTPS encryption,
		IEEE 802.1Xa network access control, Digest authentication, User access log
39	Firmware Upgrade	The firmware upgrade shall be done through web interface, The firmware shall be available free of cost
40	Logs	The camera shall provide minimum 200 logs of latest connections, access attempts, users connected, changes in the cameras etc.
41	Interface	RJ 45, 100 Base TX
42	Enclosure	Die Cast Aluminium, IK10 rated, IP66 rated, polycarbonate clear dome and sunshield, PVC free complying to WEEE Standards
43	Mount	Wall / Pole Mount
44	Power requirements	Power over Ethernet (PoE/PoE+) IEEE 802.3at Type 2 Class 4, max. 24 W, Typical 9W; 24 V DC max. 30 W
		24 V AC, max. 40 VA or better
45	Operating Temperature	-20 °C to 55 °C or better
46	Operating Humidity	20–90% RH) or better
47	Certification	UL, CE, FCC
48	Embedded Applications	The camera shall provide a platform allowing the upload of third party applications into the camera
49	Application Programmers Interface	The interface shall be available for integration with 3rd party analytics and applications in public domain free of cost
50	Onvif	S required
51	Warranty	Min 3 Years OEM warranty

Online UPS

Sl. No.	Parameter	Minimum Specifications
1	Capacity	Adequate capacity to cover all above IT Components at respective location. Indicative capacity JICCC – 50 KVA, Viewing centre – 10 KVA, Traffic Signals – 1KVA

Sl. No.	Parameter	Minimum Specifications
2	Output Wave Form	Pure Sine wave
3	Input Power Factor at Full Load	>0.90
4	Input	Three Phase 3 Wire for over 5 KVA
5	Input Voltage Range	305-475VAC at Full Load
6	Input Frequency	50Hz +/- 3 Hz
7	Output Voltage	400V AC, Three Phase for over 5 KVA UPS
8	Output Frequency	50Hz +/- 0.5% (Free running); +/- 3% (Sync. Mode)
9	Inverter efficiency	>90%
10	Over All AC-AC Efficiency	>85%
11	Technology	<ul style="list-style-type: none"> · True Online Double Conversion · IGBT technology · PWM inverter switching technology
12	UPS shutdown	UPS should shutdown with an alarm and indication on following conditions 1) Output over voltage 2) Output under voltage 3) Battery low 4) Inverter overload 5) Over temperature 6) Output short
13	Battery Backup	60 minutes in full load
14	Battery	VRLA (Valve Regulated Lead Acid)
15	Indicators & Metering	Indicators for AC Mains, Load on Battery, Fault, Load Level, Battery Low Warning, Inverter On, UPS on Bypass, Overload, etc.
		Metering for Input Voltage, Output Voltage and frequency, battery voltage, output current etc.
16	Audio Alarm	Battery low, Mains Failure, Over temperature, Inverter overload, Fault etc.
17	Cabinet	Rack / Tower type, 75KW/ 150KW/ 200KW configurations
18	Operating Temperature	0 to 60 degrees centigrade

Diesel Genset

Sl. No.	Item	Minimum Specifications
1	General Specifications	<ul style="list-style-type: none"> • Auto Starting DG Set mounted on a common base frame with AVM (Anti-Vibration) pads, residential silencer with exhaust piping, complete conforming to ISO 8528 specifications and CPCB certified for emissions. • KVA rating as per the requirement to provide the supply for JICCC
2	Engine	Radiator cooled/air cooled/Water cooled, multi cylinder, 1500 RPM/3000 RPM diesel engine, with electronic/manual governor and electrical starting arrangement complete with battery, conforming to BS 5514/ ISO 3046/ IS 10002
3	Fuel	High Speed Diesel (HSD)
4	Alternator	Self-exciting, self-regulating type alternator rated at 0.8 PF or better, 415 Volts, 3 Phase, 4 wires, 50 cycles/sec, 1500 RPM, conforming to IS 4722/ BS 5000, Windings of 100% Copper, class H insulation, Protection as per IP 23.
5	AMF (Auto Main Failure) Panel	<p>AMF Panel fitted inside the enclosure, with the following: It should have the following meters/indicators:</p> <ul style="list-style-type: none"> • Incoming and outgoing voltage • Current in all phases • Frequency • KVA and power factor • Time indication for hours/minutes of operation • Fuel Level in fuel tank, low fuel indication • Emergency Stop button • Auto/Manual/Test selector switch • MCCB/Circuit breaker for short-circuit and overload protection • Control Fuses • Earth Terminal • Any other switch, instrument, relay etc. essential for Automatic functioning of DG set with AMF panel

Sl. No.	Item	Minimum Specifications
6	Acoustic Enclosure	The DG set shall be provided with acoustic enclosure / canopy to reduce the sound level and to house the entire DG set (Engine & Alternator set) assembly outside (open-air). The enclosure must be weather resistant powder coated, with insulation designed to meet latest MOEF/CPCB norms for DG sets, capable to withstand climate. The enclosure must have ventilation system, doors for easy access for maintenance, secure locking arrangements etc.
7	Fuel Tank Capacity	It should be sufficient and suitable for containing fuel for minimum 12 hours continuous operation, Complete with level indicator, fuel inlet and outlet, air vent, drain plug, inlet arrangement for direct filling and set of fuel hoses for inlet and return.

Disaster Recovery (DR)

- a) The MSI is required to provision for a Disaster Recovery (DR) Site on cloud same as of main Data Centre (DC) capacity & standard for Smart City Solution.
- b) The DR site should not be in the same seismic zone and should be at least 250 km from Main DC site.
- c) DR site shall provision to cater to 100% load of the smart city system.
- d) MSI shall propose to host Applications and storage on cloud for complete Data Recovery (DR) operations.
- e) MSI should select the Cloud Service Provider from who adheres the guidelines of MeITY or preferred to be empanelled vendors of MeITY.
- f) The MSI shall establish dedicated connectivity between the DC and DR Site for replication & failover.
- g) For CCTV surveillance, selected video feeds from police shall only be replicated to DR site

Below are the key factors to be considered for cloud hosting:

- i. The MSI is required to prepare and submit along with their technical proposal, the details of methodologies and computations for sizing and capacity of storage, compute, backup, network and security.
- ii. There should be physical and logical separation (of space, servers, storage, network infrastructure and networks) to protect data, applications and servers.

- iii. The system will be hosted in the site identified by the MSI and as agreed by the Authority for DR.
- iv. There should be sufficient capacity (compute, network and storage capacity offered) available for near real time provisioning (as per the SLA requirement of the Authority) during any unanticipated spikes in the user load.
- v. DR site will be located in India only.
- vi. Ensure redundancy at each level
- vii. Both DC and DR site shall work in active-passive mode
- viii. DR should have 50% computing power for the mentioned smart city applications in RFP and 2% of video feeds for 10 years should be available in DR
- ix. RPO and RTO will be designed and configured as under: DC Infrastructure and applications being commissioned through this project - RPO 4 hours and RTO 30 minutes
- x. MSI shall provide interoperability support with regards to available APIs, data portability etc. for the JSCL to utilize in case of Change of cloud service provider, migration back to in-house infrastructure, burst to a different cloud service provider for a short duration or availing backup or DR services from a different service provider.
- xi. The MSI is fully responsible for tech refreshes, patch management and other operations of infrastructure that is in the scope of the MSI.
- xii. JSCL retains ownership of all virtual machines, templates, clones, and scripts/applications created for the JSCL's application. JSCL retains the right to request (or should be able to retrieve) full copies of these virtual machines at any time.
- xiii. Provide a robust, fault tolerant infrastructure with enterprise grade SLAs with an assured uptime of 99.5%, SLA measured at the VM Level & SLA measured at the Storage Levels
- xiv. Cloud services should be accessible via internet and MPLS.
- xv. Required Support to be provided to the JSCL in migration of the VMs, data, content and any other assets to the new environment created by the Authority or any Agency (on behalf of the JSCL) on alternate cloud service provider's offerings to enable successful deployment and running of the Smart city solution on the new infrastructure.
- xvi. The MSI should configure, schedule and manage backups of all the data including but not limited to files, folders, images, system state, databases and enterprise applications
 - Perform and store data and file backups consisting of an initial full back up with daily incremental backups for files;
 - For the files, perform weekly backups;

- For the databases, perform a twice weekly full database backup, with a three times daily backup of database log files
 - Encryption of all backup files and data and management of encryption keys as a service that can be enabled for Government Departments that require such a service.
 - Retain database backups for thirty (30) days
 - Videos selected by police shall never be deleted
- xvii. The MSI should offer dashboard to provide visibility into service via dashboard.
- xviii. MSI shall not delete any data at the end of the agreement (for a maximum of 45 days beyond the expiry of the Agreement) without the express approval of the Authority.

Preparation of Disaster Recovery Operational Plan The bidder should provide detailed operating procedures for each application during the following scenarios. These will be mutually agreed upon with Authority during the project kick off.

- **Business as usual:** The primary site is functioning as required, procedures for ensuring consistency of data availability at secondary site.
- **Disaster:** Declaration of disaster, making the DR site live for production, ensuring availability of users to the secondary site.
- **Operations from DR site:** Ensuring secondary site is addressing the functionality as desired
Configure proposed solution for usage

The service provider shall provide DR Management Solution to Authority meeting following specifications:

1. The proposed solution must offer a workflow based management & monitoring and reporting capability for the real time monitoring of a DR solution parameter like RPO (at DB level), RTO, replication status and should provide alerts (including SMS and e-mail alerts) on any deviations. The proposed solution should be able to conduct DR Drills from a centralized location.
2. The proposed solution should provide a single dashboard to track DR Readiness status of all the applications under DR
3. The proposed solution should be capable of reporting important health parameters like disk space, password changes, file addition/deletion etc. to ensure DR readiness
4. The proposed solution should have inbuilt ready to use library of recovery automation action for heterogeneous databases and replication environment. This must significantly reduce custom development of scripts and speedy deployment of DR solutions

5. The proposed solution should facilitate out-of-the-box, workflow based switchover and switchback for DR drills for standard applications based on industry best practices
6. The proposed solution should facilitate workflows for bringing up the applications and all the components it depends on at DR while it is up at primary site without pausing/stopping the replication
7. The proposed solution should be able to manage hosts by either deploying agents or without deploying any agent and should not require any change in the existing environment
8. The proposed solution must support all major platforms including Linux, Windows, Solaris, HP-UX, and AIX with native high availability options. It must support both physical and virtual platforms
9. The proposed solution should facilitate workflow based, single-click recovery mechanism for single or multiple applications
10. The proposed DRM solution should integrate seamlessly with the existing setup without the need to reconfigure or remove existing application setup including clusters
11. The proposed solution should cover all the functionalities mentioned in the specifications and all the required licenses should be provisioned

Periodic Disaster Recovery Plan

The service provider shall be responsible for –

- Devising and documenting the DR policy discussed and approved by Authority.
- Providing data storage mechanism with from the Go-Live date till the date of contract expiry for the purpose of compliance and audit.

4.2 CCTV City Surveillance

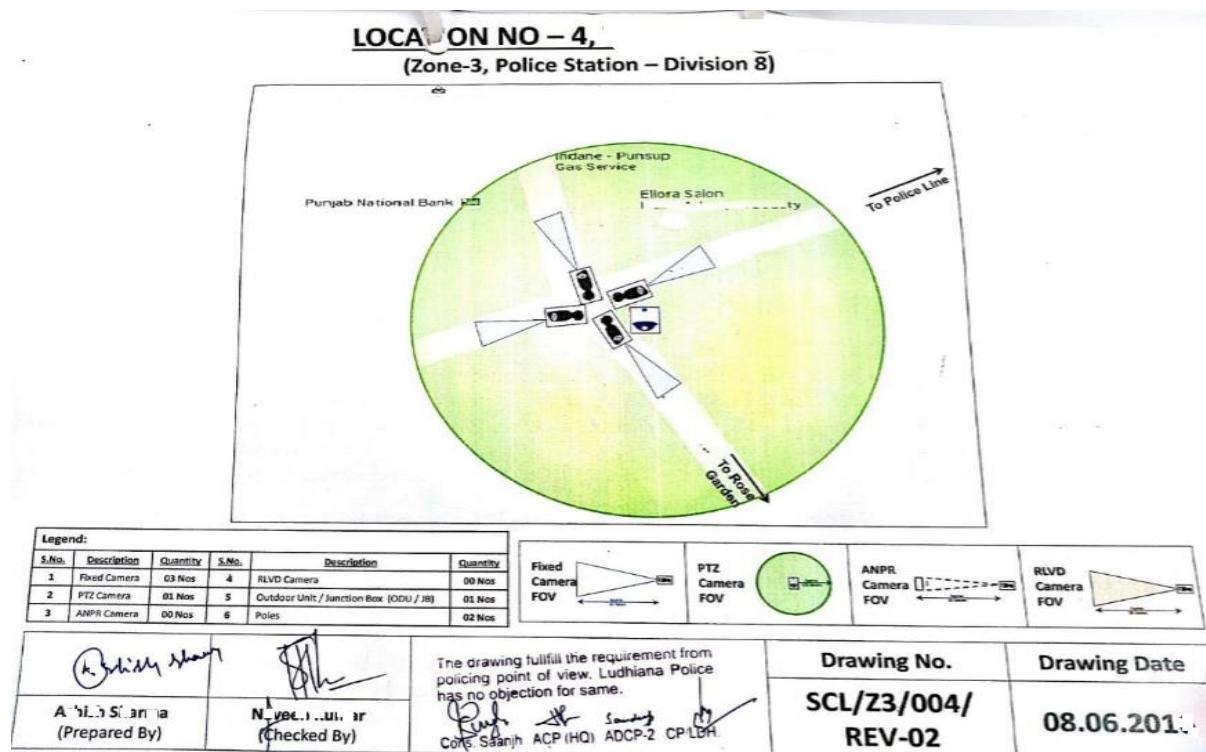
This Component covers planning & implementation of the Surveillance system comprising cameras and other field equipment at identified locations. Actual placement of pole & number of cameras at each location, type of cameras, fixation of height & angle for the cameras to ensure maximum coverage shall be done in consultation with Jalandhar Police Department.

A detailed survey shall be conducted, by the MSI along with Jalandhar police, at each of the strategic locations for placement of junction boxes and cameras. This survey shall finalize the position of all field equipment's and the orientation/ field of view of the cameras. Appropriate field of view snapshot shall be taken by a handheld camera for future reference at the time of survey.

MSI along with Jalandhar police shall talk to nearby private/public property owners and get permissions to place the junction boxes. These junction boxes may be placed on terrace or underground parking spaces or mounted on wall/ceiling in the identified property.

The surveyors shall also finalize the approximate location of foundation for junction box and camera poles. The route for all the underground cable laying shall be finalized during this survey (wherever required). Every detail, finalized during the survey, shall be demarcated on an AutoCAD drawing by the MSI and submitted to JSCL or designated agency and Jalandhar police in the form of a detailed site survey report along with other details for its approval in the format below

Sample of AutoCAD diagram is as follows:



System shall provide inter-operability of hardware, operating system, software, networking, printing, database connectivity, reporting, and communication protocols. MSI shall prepare the detailed report for field level requirements e.g. Cameras (types & numbers), Camera Mounting requirements, Power Requirements, Connectivity Requirements etc. for perusal of JSCL and designated agency. MSI shall also study the process requirements of police to configure and customize the system and implement the processes over a period of 6 months' post go live.

Various components of CCTC City Surveillance

The CCTV City Surveillance shall comprise the following:

- PTZ cameras & Fixed box cameras
- Video Management Server & Video Analytics
- Establish Network Connectivity to transfer the data from field devices to the Data Centre & Integrated Command Control Centre (JICCC)
- Set up City Surveillance Operations at JICCC with required software platform capability to aggregate incoming data streams onto a single platform, provide analytics results in real time
- IT infrastructure including hardware and software at JICCC and DC for the management of the edge devices, command centre.
- Develop strategies and system processes to assist in city surveillance with video analytics and implement Standard Operating Procedures.
- Develop a consolidated database of incidents
- Develop a data analytics infrastructure and team

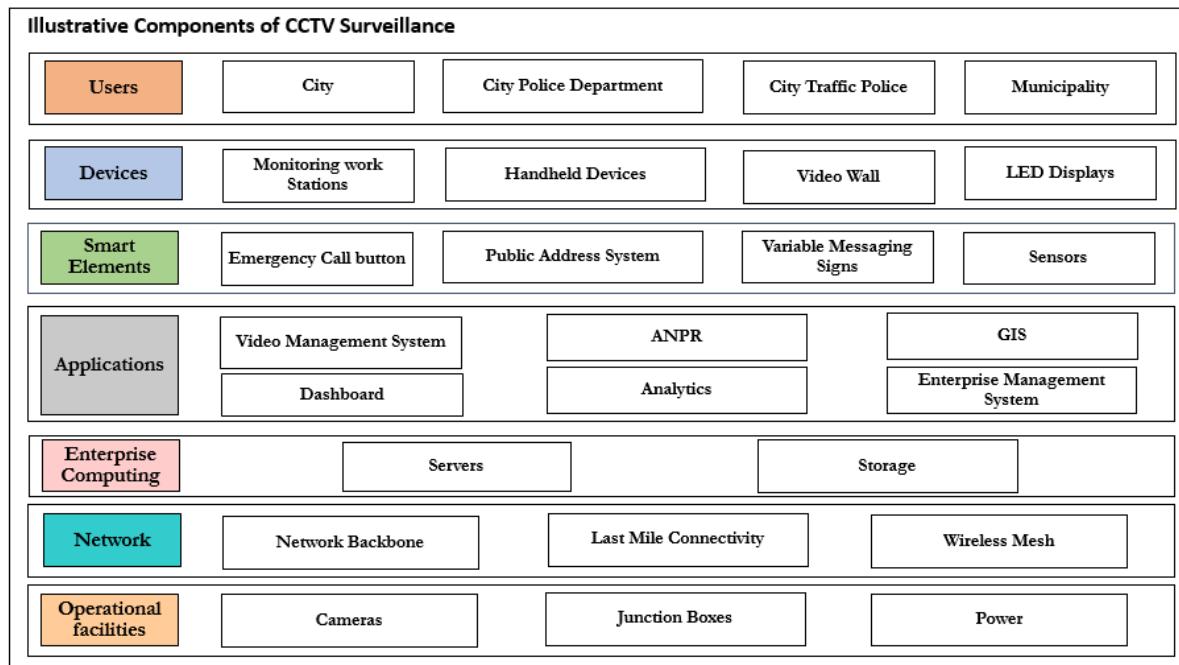


Figure: Illustrative components of CCTV Surveillance

Field Level Hardware

An Indicative list of the field level hardware to be provided by MSI is as follows:

1. Cameras (Fixed Box Cameras, PTZ Cameras, Dome cameras etc.) with external IR, Wipers and bird spikes
2. Local processing unit for ANPR / RLVD / SVDS/FRS cameras
3. Face recognition System
4. Switches
5. Outdoor Cabinets
6. Pole for cameras / Mast
7. Junction box
8. UPS
9. Networking and power cables and other related infrastructure

Key Performance Indicators

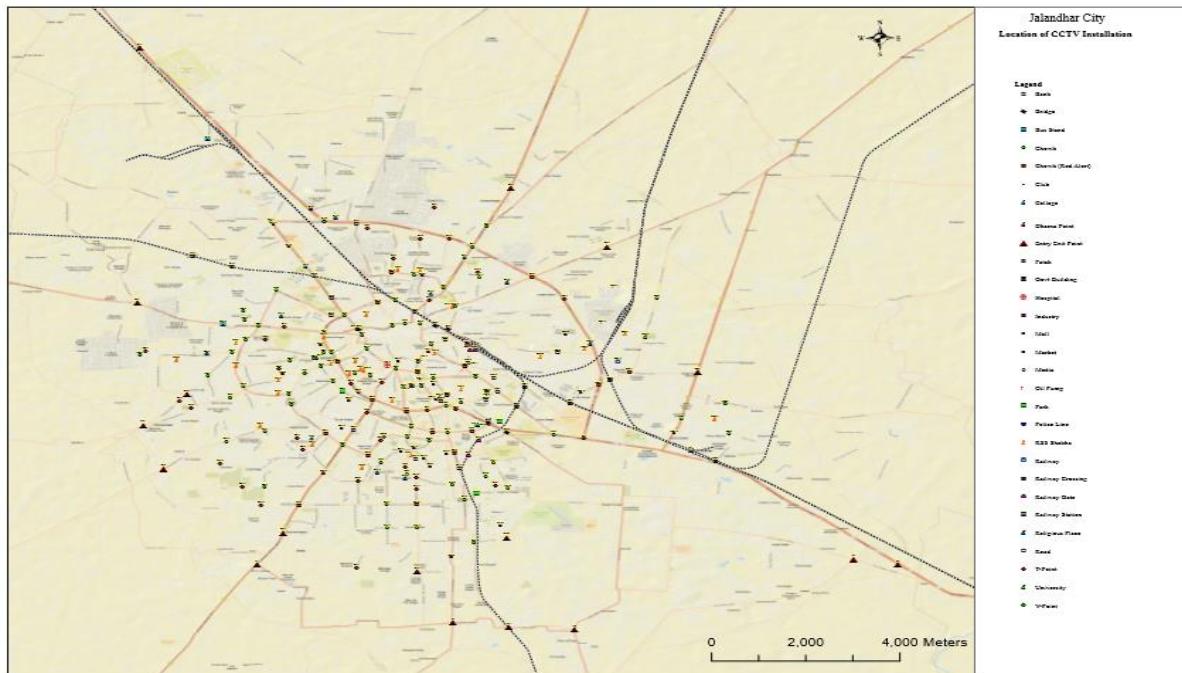
The KPIs for CCTV Surveillance shall be the following:

- a. City Surveillance should cater to an effective Monitoring and Management with appropriate decision support mechanisms.
- b. City surveillance must ensure a pro-active 24*7 monitoring of PAN city parameter that capture video footages of all junctions across the road network of Jalandhar and project the feeds to the proposed Command and Control centre without time lag on real time basis.
- c. City Surveillance System must ensure and provide a secure and safe environment for the citizens with intelligent and effective use of video analytics and integrated platform for all concerned departments.
- d. The surveillance prime equipment i.e. High Definition Camera units which includes Fixed box, and PAN-Tilt-Zoom, must be located at a suitable position wherein the required area is properly captured. The intensity of captured footage should be enough to sustain the clarity as per the required zooming levels. Industry leading practices must be adopted during the implementation phase w.r.t positioning and mounting the cameras, poles and junction boxes.
- e. The surveillance system shall be to provide proactive security as opposed to reactive security on PAN city basis with a clear defined objective of each HD camera unit.
- f. The surveillance System shall provide inter-operability of hardware, operating system, software, networking, printing, database connectivity, reporting, and communication protocols.
- g. It has to be ensured that the pole is well placed for vibration resistance adhering to the road safety norms. Also, the poles erected to mount cameras are good, both qualitatively and aesthetically.

- h. Appropriate branding / colour coding of junction boxes should be done, to warn mischief mongers against tampering with the equipment at the junction with the needful operational equipment. Cameras needs to be protected from the on field challenges of weather, physical damage and theft.
- i. This City Surveillance software should have the capability to provide various alarms & triggers. The required analytics and related triggers should include Parking Violation, Wrong Direction, People loitering, Camera Tampering (In case this is an inherent feature of the camera, this may not be provided as a separate line item), Unattended Object, Crowd detection, Traffic flow/Congestion, Traffic Volume estimation and statistical counts, Video Content Analytics Requirement, People tracking.
- j. Video Management System must allow users to view a count of analytics events on the video pane while video is being displayed.
- k. Each intersection should be fitted with outdoor cabinets dimensioned to host all equipment necessary to operate enforcement systems and traffic surveillance systems
- l. The data retention of minimum 90 days has to be maintained at JICCC for city surveillance.
- m. The city surveillance system must ensure real time and event base monitoring of the city, situation/ rule based alerts including early warnings for prevention and avoidance of unwanted incidents like riots, flooding, etc.
- n. The system should support automated response based on events including communication of alerts to relevant authorities like Fire, Hospitals, etc. for swift response in case of emergencies.
- o. The system should have access to historic video data for investigative purposes.
- p. IP based Public Address System shall also be used as part of the information dissemination system at various locations in the city. These systems shall be deployed at identified junctions to make public interest announcements.
- q. The feed from video shall be accessed from multiple locations as mentioned in list of viewing centres.
- r. Wipers and bird spikes shall be installed for all the cameras

Geographic Locations

The 154 locations identified by Jalandhar Police for installation of CCTV City Surveillance system are mapped as below



Geographic locations:

Sl. No	Location	Long_DMS	Lat_DMS	Long_DD	Lat_DD
1	Issa Nagar	75° 32' 24.454" E	31° 22' 46.455" N	75.54012601	31.37957081
2	Verka Milk Plant	75° 33' 35.532" E	31° 21' 47.952" N	75.55987	31.36332
3	Sanjay Gandhi Nehar Pulli	75° 34' 6.728" E	31° 21' 36.313" N	75.56853569	31.36008708
4	Hardev Nagar	75° 33' 17.028" E	31° 20' 9.636" N	75.55473	31.33601
5	Gaji Gulla Chowk	75° 34' 21.288" E	31° 20' 29.400" N	75.57258	31.3415
6	Y-Point Bhagat Singh Colony	75° 33' 44.646" E	31° 21' 38.076" N	75.56240175	31.36057679
7	Sehnai Palace Chowk	75° 33' 50.718" E	31° 19' 23.379" N	75.56408821	31.32316082
8	Sabji Mandi Chowk	75° 34' 10.373" E	31° 20' 2.512" N	75.56954799	31.33403119
9	Gulab Devi Road	75° 33' 49.328" E	31° 20' 18.620" N	75.56370218	31.33850557

Sl. No	Location	Long_DMS	Lat_DMS	Long_DD	Lat_DD
10	OBC Kapurthla Chowk	75° 33' 44.413" E	31° 20' 0.891" N	75.56233696	31.3335809
11	Shakti Nagar Park	75° 34' 6.120" E	31° 19' 41.012" N	75.56836657	31.32805881
12	Adarsh Nagar Near Gita Mandir	75° 33' 49.376" E	31° 19' 38.486" N	75.56371562	31.32735714
13	ShaheedUdam Singh Nagar	75° 34' 11.720" E	31° 19' 33.126" N	75.56992225	31.32586844
14	Shetla Mata Mandir Chowk	75° 34' 31.889" E	31° 20' 10.500" N	75.57552462	31.3362499
15	Doaba Chowk	75° 35' 6.994" E	31° 20' 40.771" N	75.58527624	31.34465874
16	Bhaghat Singh Chowk	75° 34' 58.263" E	31° 19' 54.208" N	75.58285087	31.33172455
17	Damoria Pull under Bridge	75° 34' 8.569" E	31° 20' 6.993" N	75.56904704	31.33527589
18	Damoria Pull over Bridge	75° 35' 9.863" E	31° 20' 7.308" N	75.58607309	31.33536344
19	Adda Tanda Road Phatak	75° 34' 46.891" E	31° 20' 21.967" N	75.57969196	31.33943537
20	Adda Hoshiarpur Chowk	75° 34' 51.300" E	31° 20' 11.305" N	75.58091678	31.33647353
21	Phagwara Gate Market	75° 34' 56.263" E	31° 19' 48.808" N	75.58229531	31.33022455
22	Park Corporation Office	75° 34' 50.563" E	31° 19' 42.308" N	75.58071198	31.32841899
23	Milap Chowk	75° 34' 49.020" E	31° 19' 40.200" N	75.58028333	31.32783333
24	Sikka Chowk	75° 34' 16.320" E	31° 19' 28.200" N	75.5712	31.3245
25	Circuit House	75° 34' 44.760" E	31° 19' 19.380" N	75.5791	31.32205
26	TV Centre	75° 34' 7.980" E	31° 19' 14.340" N	75.56888333	31.32065
27	Civil Hospital Jalandhar	75° 34' 28.164" E	31° 19' 37.214" N	75.57448993	31.32700389
28	Desh Bhagat Yadgar Hall Near BMC Chowk	75° 34' 1.440" E	31° 19' 7.860" N	75.56706667	31.31885

Sl. No	Location	Long_DMS	Lat_DMS	Long_DD	Lat_DD
29	Ali Baba Mobile Centre Turn towards SUS Nagar	75° 34' 24.306" E	31° 19' 22.746" N	75.57341845	31.32298503
30	SBI Main Branch Civil Line Jal	75° 34' 44.640" E	31° 19' 20.340" N	75.57906667	31.32231667
31	Park Near Loins Club Lajpat Nagar Jal	75° 34' 31.440" E	31° 19' 7.320" N	75.5754	31.3187
32	Shakti Nagar Park	75° 34' 1.920" E	31° 19' 30.180" N	75.5672	31.32505
33	Rock Garden	75° 34' 9.540" E	31° 19' 33.960" N	75.56931667	31.3261
34	Gujral Nagar Market	75° 34' 59.820" E	31° 19' 21.540" N	75.58328333	31.32265
35	Gakhal Puli (City Ceiling)	75° 31' 40.192" E	31° 18' 46.651" N	75.52783104	31.31295851
36	Kot Sadiq Nehar Puli Kala Sangia Road	75° 31' 54.083" E	31° 18' 9.785" N	75.53168981	31.30271797
37	Babrik Chowk	75° 33' 20.295" E	31° 19' 12.982" N	75.5556374	31.32027283
38	Kari Chowk Basti Danishmandा	75° 32' 39.966" E	31° 19' 10.076" N	75.54443509	31.3194656
39	Adda Basti Shiekh	75° 33' 22.155" E	31° 19' 4.076" N	75.55615417	31.31779894
40	Peer Chowk Jhandiya Wala	75° 33' 42.460" E	31° 19' 36.234" N	75.56179453	31.32673178
41	Y-Point Evening College Basti Nau	75° 33' 31.283" E	31° 19' 30.725" N	75.55868981	31.3252013
42	T-Point St Soldier College Basti Danishmandा	75° 32' 13.078" E	31° 19' 1.299" N	75.53696609	31.31702748
43	Guru Nanak Colony Wala Chowk	75° 32' 37.489" E	31° 18' 33.208" N	75.54374696	31.3092244
44	Ghas Mandi Chowk	75° 33' 3.986" E	31° 18' 41.326" N	75.55110726	31.31147951
45	Dusehra Ground Kala Sanghia Road	75° 33' 0.572" E	31° 18' 46.340" N	75.55015899	31.31287214
46	Nahal Pulli	75° 32' 10.237" E	31° 19' 12.655" N	75.53617695	31.32018192

Sl. No	Location	Long_DMS	Lat_DMS	Long_DD	Lat_DD
47	Geeta Colony	75° 32' 32.987" E	31° 18' 14.748" N	75.5424965	31.30409654
48	T-Point Near Entry/Exit BMC Flyover Opposite HDFC Bank near Narinder cinema	75° 35' 15.000" E	31° 19' 0.000" N	75.5875	31.31666667
49	T-Point Link Road Near Khalsa School	75° 34' 14.000" E	31° 18' 58.000" N	75.57055556	31.31611111
50	Chowk Gol Market	75° 34' 41.514" E	31° 18' 5.951" N	75.57819832	31.30165301
51	T-Point Near No-Exit Model Town	75° 34' 40.308" E	31° 18' 11.694" N	75.57786344	31.30324829
52	Diaryan Chowk	75° 34' 23.685" E	31° 18' 15.617" N	75.57324591	31.30433799
53	Liberty Chowk	75° 35' 14.223" E	31° 18' 23.822" N	75.58728409	31.30661732
54	Chowk near KFC Model Town	75° 34' 37.385" E	31° 18' 25.007" N	75.57705152	31.30694625
55	HDFC Currency Chest Cool Road	75° 35' 17.385" E	31° 18' 10.949" N	75.58816263	31.30304128
56	Shivani Sharma Park Model Town market	75° 34' 44.334" E	31° 18' 21.773" N	75.57898169	31.3060481
57	Mata Gujri Park GTB Nagar	75° 34' 10.651" E	31° 18' 11.234" N	75.56962528	31.30312042
58	Mata Rani Chowk Model Town	75° 34' 57.475" E	31° 18' 12.234" N	75.58263195	31.30339843
59	Abadpura T-Point Mall Road	75° 34' 25.332" E	31° 18' 37.177" N	75.57370342	31.31032703
60	Taramount Hotel	75° 34' 23.371" E	31° 18' 34.248" N	75.57315852	31.30951325
61	T-Point Gill Farm Mithapur	75° 34' 6.787" E	31° 16' 46.976" N	75.56855183	31.27971548
62	Mithapur Chowk Near School	75° 34' 48.452" E	31° 16' 43.702" N	75.58012549	31.27880623
63	Chowk Subhana Near Ganda Nala	75° 35' 27.460" E	31° 17' 8.428" N	75.59096111	31.28567453
64	Under Brigde Defence Colony	75° 35' 50.106" E	31° 18' 40.477" N	75.59725168	31.31124355

Sl. No	Location	Long_DMS	Lat_DMS	Long_DD	Lat_DD
65	Railway Phatak near Cambridge School	75° 35' 23.499" E	31° 18' 21.673" N	75.58986075	31.30602017
66	Railway Phatak Defence Colony	75° 35' 30.612" E	31° 18' 34.336" N	75.59183675	31.30953786
67	Dayanand Chowk Garha	75° 35' 50.965" E	31° 17' 53.775" N	75.59749038	31.29827095
68	Choti Baradari Chowk	75° 35' 41.099" E	31° 18' 15.210" N	75.59474986	31.30422493
69	T-Point PPR Market	75° 34' 48.053" E	31° 17' 53.473" N	75.5800148	31.29818705
70	Sangha Chowk	75° 34' 27.642" E	31° 17' 40.173" N	75.57434513	31.29449242
71	Cheema Chowk	75° 34' 48.156" E	31° 17' 40.199" N	75.58004344	31.29449977
72	Kukki Dhab Chowk	75° 34' 27.899" E	31° 17' 20.328" N	75.57441651	31.28897993
73	Inter State Bus Stand Jalndhar	75° 35' 29.959" E	31° 18' 46.405" N	75.59165539	31.31289023
74	Chapatti Market	75° 35' 45.726" E	31° 17' 22.434" N	75.59603507	31.2895649
75	Baba Sweetshop Phase-I	75° 35' 42.386" E	31° 17' 56.102" N	75.59510711	31.29891718
76	Sweety Park	75° 35' 29.315" E	31° 17' 49.043" N	75.59147631	31.29695634
77	Golden Avenue Chowk	75° 35' 35.649" E	31° 18' 4.063" N	75.59323579	31.30112874
78	Andh Vidyalay Phase-II	75° 35' 12.702" E	31° 17' 57.004" N	75.58686172	31.29916786
79	Subhana Chowk Cantt Road	75° 35' 49.982" E	31° 17' 12.238" N	75.59721714	31.2867328
80	Gulshan Hotel	75° 35' 36.420" E	31° 21' 34.148" N	75.59345009	31.35948554
81	Hoshiarpur Road Near Gulmarg City Mor	75° 36' 58.927" E	31° 21' 16.387" N	75.61636857	31.35455187
82	Kali Mata Mandir T-point	75° 34' 32.182" E	31° 21' 6.814" N	75.57560605	31.35189274
83	Transport Nagar T-Point Near Police station	75° 35' 0.240" E	31° 21' 49.644" N	75.5834	31.36379

Sl. No	Location	Long_DMS	Lat_DMS	Long_DD	Lat_DD
84	Sanjay Gandhi Nagar T-Point Nehalpuli	75° 34' 14.196" E	31° 21' 32.328" N	75.57061	31.35898
85	Gujja Peer Chownk	75° 34' 50.664" E	31° 21' 23.004" N	75.58074	31.35639
86	Dargah Peer Baba Nimboo Shah ji	75° 35' 50.352" E	31° 20' 46.968" N	75.59732	31.34638
87	Aman Nagar Road near GP Tower T-Point	75° 35' 10.619" E	31° 21' 23.533" N	75.58628292	31.35653692
88	Aman Nagar Morh Near KMV college	75° 35' 21.156" E	31° 21' 7.560" N	75.58921	31.3521
89	T-Point Angoora Dia Bela Santokhpura	75° 35' 30.228" E	31° 20' 55.248" N	75.59173	31.34868
90	Nimbuawali Gali	75° 35' 31.308" E	31° 20' 50.640" N	75.59203	31.3474
91	Sodal Chowk	75° 34' 30.864" E	31° 20' 54.852" N	75.57524	31.34857
92	Devi Talab Mandir	75° 34' 57.901" E	31° 20' 36.995" N	75.58275026	31.34360964
93	Thapra Bagichi	75° 34' 35.220" E	31° 20' 57.516" N	75.57645	31.34931
94	KalishNagar Near Mandir	75° 34' 50.484" E	31° 20' 56.832" N	75.58069	31.34912
95	Court Road Chowk	75° 35' 18.780" E	31° 19' 6.180" N	75.58855	31.31838333
96	Madan Flour Mill Chowk	75° 35' 21.360" E	31° 19' 36.000" N	75.58926667	31.32666667
97	Kamal Palace Chowk	75° 35' 9.060" E	31° 19' 11.760" N	75.58585	31.31993333
98	Alaska Chowk	75° 35' 28.800" E	31° 19' 27.540" N	75.59133333	31.32431667
99	Railway Crossing Guru Nanak Pura West	75° 36' 33.600" E	31° 19' 5.340" N	75.60933333	31.31815
100	Railway Crossing Sant Nagar Fatak	75° 36' 2.460" E	31° 19' 19.140" N	75.60068333	31.32198333
101	Railway Crossing Ladowali Road	75° 35' 56.940" E	31° 19' 2.640" N	75.59915	31.3174

Sl. No	Location	Long_DMS	Lat_DMS	Long_DD	Lat_DD
102	Front of Police Line	75° 35' 37.440" E	31° 18' 51.180" N	75.59373333	31.31421667
103	Puda Ground opp DC Office	75° 35' 36.385" E	31° 19' 10.911" N	75.59344041	31.31969752
104	Bank of Badodha Railway Road Currency Chest	75° 35' 23.580" E	31° 19' 39.240" N	75.58988333	31.32756667
105	SBI Shastari Market Currency Chest	75° 35' 41.160" E	31° 19' 26.460" N	75.59476667	31.32401667
106	SBI Mandi Fanttan Ganjh Railway Road Currency Chest	75° 35' 23.396" E	31° 19' 38.805" N	75.58983215	31.3274459
107	Neta Ji Park Master Tara Singh Nagar	75° 35' 18.720" E	31° 19' 17.220" N	75.58853333	31.32145
108	Rly Stn Gate No 1	75° 35' 28.300" E	31° 19' 50.200" N	75.59119444	31.33061111
109	Rly Stn Gate No 2	75° 35' 24.800" E	31° 19' 50.200" N	75.59022222	31.33061111
110	Rly Stn Gate No 3	75° 35' 23.000" E	31° 19' 54.600" N	75.58972222	31.33183333
111	Nangal Shama Chowk	75° 38' 1.320" E	31° 19' 31.140" N	75.6337	31.32531667
112	Suchi Pind Pulli	75° 37' 33.420" E	31° 20' 33.000" N	75.62595	31.3425
113	Dhillwan Chowk	75° 37' 56.131" E	31° 19' 12.557" N	75.63225849	31.32015475
114	Batha Road	75° 36' 25.020" E	31° 19' 47.760" N	75.60695	31.32993333
115	Dakoha Railway Crossing Choke Point	75° 38' 13.740" E	31° 18' 16.380" N	75.63715	31.30455
116	Chugitti Railway Crossing Choke Point	75° 37' 1.080" E	31° 19' 24.300" N	75.61696667	31.32341667
117	Partap Palace Chowk	75° 37' 14.460" E	31° 19' 31.260" N	75.62068333	31.32535
118	Under Brij Chugitti	75° 36' 53.340" E	31° 19' 20.340" N	75.61481667	31.32231667

Sl. No	Location	Long_DMS	Lat_DMS	Long_DD	Lat_DD
119	Guru Nanak Dev University Campus Ladowali Road	75° 37' 25.320" E	31° 20' 1.080" N	75.6237	31.33363333
120	Rama Mandi Main Market	75° 37' 45.060" E	31° 18' 39.840" N	75.62918333	31.31106667
121	Guru Nanak Pura Main Market	75° 36' 41.040" E	31° 19' 13.920" N	75.6114	31.32053333
122	Sainik Vihar	75° 38' 13.020" E	31° 18' 52.200" N	75.63695	31.3145
123	Kamal Vihar	75° 36' 13.020" E	31° 19' 44.340" N	75.60361667	31.32898333
124	Wadala Chowk	75° 33' 27.213" E	31° 17' 39.582" N	75.55755923	31.29432846
125	Rejant Park Avtar Nagar	75° 33' 57.000" E	31° 19' 14.940" N	75.56583333	31.32081667
126	Sethi Battery T-Point Model House	75° 33' 25.980" E	31° 18' 35.880" N	75.55721667	31.30996667
127	Udey Nagar Chowk	75° 33' 3.617" E	31° 17' 55.200" N	75.55100477	31.29866677
128	Chara Mandi Butta Mandi	75° 33' 44.022" E	31° 18' 7.064" N	75.56222846	31.30196235
129	Mata Rani Chowk	75° 33' 45.626" E	31° 18' 39.834" N	75.56267388	31.31106494
130	Park near Gurdwara Singh Saba Model House Road	75° 33' 36.497" E	31° 18' 30.921" N	75.56013813	31.30858927
131	Wadala Road Phase-II	75° 33' 1.130" E	31° 17' 39.431" N	75.55031395	31.29428632
132	T-Point Nakhawala Bagh	75° 32' 48.324" E	31° 17' 54.932" N	75.54675665	31.29859215
133	Waryana Morh	75° 31' 36.112" E	31° 20' 29.091" N	75.5266977	31.34141425
134	T-Point Leather Complex	75° 31' 41.685" E	31° 19' 49.411" N	75.52824591	31.33039199
135	T-Point Shashtri Nagar	75° 33' 13.471" E	31° 19' 33.957" N	75.55374198	31.32609921
136	T-Point Basti(Near Khana)	Mithu Patwar 75° 33' 4.000" E	31° 19' 59.000" N	75.55111111	31.33305556

Sl. No	Location	Long_DMS	Lat_DMS	Long_DD	Lat_DD
137	Pull Nehar KPT Road	75° 32' 59.463" E	31° 20' 9.893" N	75.54985071	31.33608132
138	Pull Nehar S.B.L.S Nagar	75° 33' 11.739" E	31° 20' 39.838" N	75.55326077	31.34439955
139	Jaggiwan Ram chowk	75° 32' 49.000" E	31° 19' 19.000" N	75.54694444	31.32194444
140	Sher Singh Pull Nehar	75° 32' 24.684" E	31° 19' 28.398" N	75.54019011	31.32455502
141	Basti Peer Dad Chowk(Lakkar Wala Pull)	75° 32' 41.336" E	31° 19' 47.692" N	75.54481564	31.32991434
142	Leather Complex Chowk(Ganda Nala)	75° 31' 38.000" E	31° 19' 46.000" N	75.52722222	31.32944444
143	Raj Nagar Morh Near Wine Shop	75° 32' 50.000" E	31° 20' 15.000" N	75.54722222	31.3375
144	Baba Budha Ji Pull	75° 32' 50.746" E	31° 19' 58.575" N	75.54742938	31.33293763
145	Adda Basti Bawa Khel	75° 32' 35.034" E	31° 20' 11.548" N	75.54306507	31.33654117
146	Sports Market Y-Point	75° 33' 16.180" E	31° 19' 29.670" N	75.55449451	31.32490834
147	Tarveni Park Dilbagh nagar	75° 32' 44.000" E	31° 19' 37.000" N	75.54555555	31.32694444
148	Rohni Colony Basti Peer Dad	75° 32' 3.000" E	31° 19' 42.000" N	75.53416667	31.32833333
149	Khambra Gate	75° 32' 58.416" E	31° 16' 49.764" N	75.54956	31.28049
150	Pholriwal Gate	75° 35' 13.020" E	31° 16' 0.732" N	75.58695	31.26687
151	Rly. Phatak Pholriwal	75° 35' 51.432" E	31° 15' 56.988" N	75.59762	31.26583
152	Y Point Dhina	75° 36' 36.576" E	31° 15' 55.296" N	75.61016	31.26536
153	Pragpur Chungi	75° 40' 18.919" E	31° 16' 49.481" N	75.67192184	31.2804115
154	Railway Station Jalandhar Cantt.	75° 37' 56.620" E	31° 18' 25.276" N	75.63239442	31.3070211

Functional Requirements:

General Requirements:

- All CCTV hardware products (Model wise) offered in the project should be min UL, CE, FCC, RoHS certified
- The OEM should have existence in India for more than 3 years in similar projects. (Under Companies Act, 1956/2013) in India
- The OEM for CCTV Camera should have technical support presence with its employees on its payroll in India. This will ensure long term after sales support & spare support from the OEM. Bidder to produce documentary proof to establish the eligibility
- OEM should be in the well repeated in Video surveillance equipment manufacturing and deployment
- Local Service/support must be available
- The server sizing shall be done with maximum of 70% utilization
- Edge level processing shall be planned to reduce use of network bandwidth and improve faster processing. For example, Face Recognition System, ANPR, SVDS (with ANPR) etc.

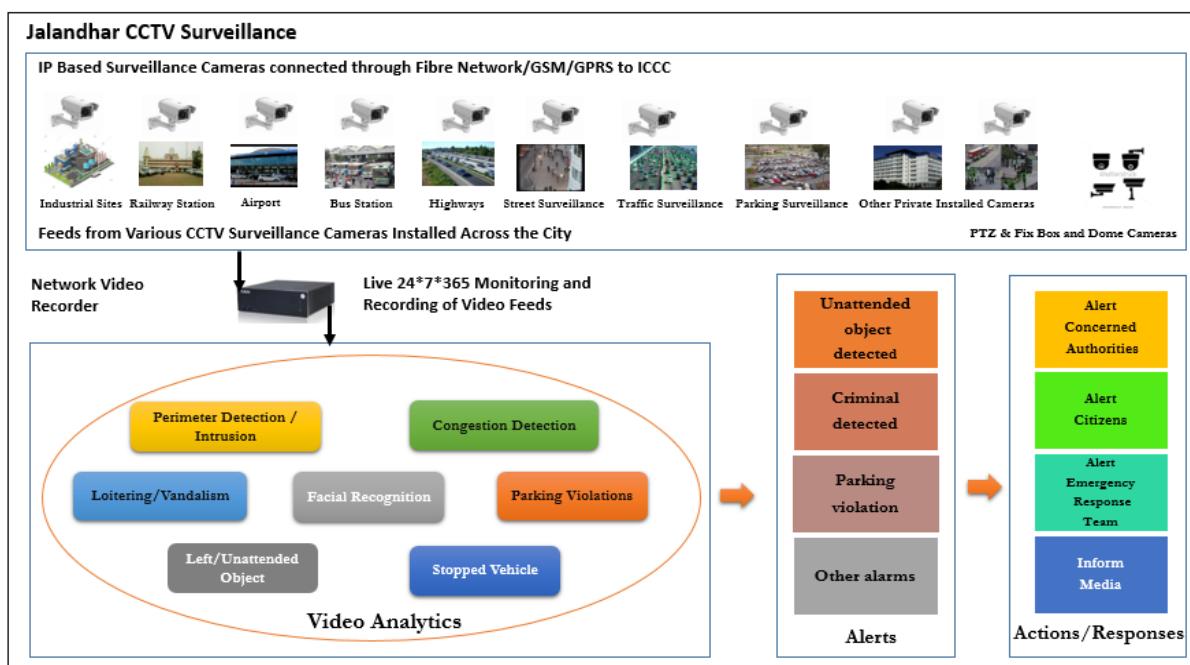


Figure: Illustrative diagram for CCTV surveillance

Functional Requirements:

1. Jalandhar City Surveillance System shall consist of:
 - a) PTZ Cameras, Fixed Box Cameras, Dome cameras, PTZ cameras etc.

- b) Video Management System (VMS) including central software application.
 - c) Camera Accessories i.e., Power Supplies, Cable, Connectors and associated accessories for an integrated system.
2. The cameras implemented as part of this project shall be rated for operations in outdoor environment (for outdoor installations) and depending on the objective/application, shall be of different configurations including PTZ or fixed cameras.
 3. All the Cameras shall be IP based.
 4. The CCTV surveillance system shall be ONVIF compliant.
 5. Cameras shall have an integral receiver/driver that shall be capable of controlling pan-tilt, zoom and focus locally and also remotely from the JICCC.
 6. All cameras shall support real-time video content analysis.
 7. The surveillance system shall support following Built-in-Analytics for the Cameras:
 - a) Perimeter Detection/ Intrusion – Virtual Tripwire
 - b) Auto-tracking for Facial Recognition - To detect and track movement in the field of view
 - c) Facial Recognition
 - d) Congestion Detection/People Counting/Crowd Gathering
 - e) Counter Flow and Movement/ Wrong or One-way detection
 - f) Camera Vandalism - Triggers an alarm if the lens is obstructed by spray paint, a cloth or a lens cap.
 - g) Parking Violation
 - h) People loitering within restricted area
 - i) Left/Unattended Object - To detect objects placed within a defined zone and triggers an alarm if the object remains in the zone longer than the user-defined time allows
 - j) Object Classification
 - k) Stopped Vehicle: - To detect vehicles stopped near a sensitive area longer than the user-defined time allows.
 8. Event (alarm) Handling: -
 - a) The camera shall be capable of recording an event as pre and post event images to on-board SD Media Card. Events may be triggered using camera motion detection or from an external device input such as a relay.
 - b) When triggered from an external input or the camera's motion detector, the camera shall be capable of sending JPEG images via e-mail and/or sequences of images to an FTP server or on-board compact flash.

- c) A relay output shall be available upon the activation of the camera's motion detector or external relay input. The relay output may also be manually activated from the live view screen.
- 9. Integration required with existing CCTV cameras deployed and functioning at important locations such as Hospitals, Schools, Market Places, etc. (actuals will be notified later) across city or bidder may propose alternate solution as required.

Video Management System (VMS)

Video Management System (VMS) shall bring together physical security infrastructure and operations and shall use the IP network as the platform for managing the entire surveillance system. End users shall have rapid access to relevant information for analysis.

This shall allow operations managers and master system integrator (MSI) to build customized video surveillance networks that meet their exact requirements. Software suite shall be a scalable and flexible video management system that could be easily managed and monitored. Scalable system shall permit retrieval of live or recorded video anywhere, anytime on a variety of clients via a web browser interface.

Video management server, on which the VMS is hosted upon, shall run seamlessly in the background to manage connections, access and storage. Video management server shall accept the feed from IP Camera installed at field locations. Server shall stream incoming video to a connected storage. VMS shall support video IP fixed colour / B &W cameras, PTZ / Dome cameras, infrared cameras, low light/IR cameras and any other camera that provides a composite PAL video signal or latest technologies like DVB, ISDB or DTMB.

General requirements:

1. Video Management System (VMS) shall be non-proprietary and open ended to support integration with JICCC platform.
2. System shall allow user to view live video stream.
3. The System shall be installable without any need for software or hardware license.
4. Recording failover shall be standard without need for additional license and/or hardware.
5. JSCL's workstations must remain "connected" to all recording devices simultaneously.
6. VMS shall be used for centralized management of all field camera devices, video servers and client users
7. VMS server shall be deployed in a clustered server environment or support inbuilt mechanism for high availability and failover.
8. VMS shall support a flexible rule-based system driven by schedules and events.

9. VMS shall be supported for fully distributed solution for monitoring and control function, designed for limitless multi-site and multiple server installations requiring 24/7 surveillance with support for devices from different vendors.
10. VMS shall support ONVIF compliant internet protocol (IP) cameras.
11. The MSI shall clearly list in their proposal the make and models that can be integrated with the VMS, additionally all the offered VMS and cameras must have (ONVIF) compliance.
12. VMS shall be enabled for any standard storage technologies and video wall system integration.
13. VMS shall be enabled for integration with any external Video Analytics Systems both server & edge based.
14. VMS shall be capable of being deployed in a virtualized server environment without loss of any functionality.
15. All CCTV cameras locations shall be overlaid in graphical map in the VMS Graphical User Interface (GUI). The cameras selection for viewing shall be possible via clicking on the camera location on the graphical map. The graphical map shall be of high resolution enabling operator to zoom-in for specific location while selecting a camera for viewing
16. VMS shall have an administrator interface to set system parameters, manage codecs, manage permissions and manage storage.
17. VMS day to day control of cameras and monitoring on client workstations shall be controlled through the administrator interface.
18. Whilst live control and monitoring is the primary activity of the monitoring workstations, video replay shall also be accommodated on the GUI for general review and also for pre- and post-alarm recording display.
19. The solution design for the VMS shall provide flexible video signal compression, display, storage and retrieval.
20. All CCTV camera video signal inputs to the system shall be provided to various command control centre(s), viewing centre etc., and the transmission medium used shall best suit the relative camera deployments and access to the CCTV Network.
21. System shall have the capability to work with touch enabled multi-monitor workstations. It shall be capable of displaying videos in up to three (3) monitors simultaneously.
 - AVI files
 - Motion- Joint Photographic Experts Group (M-JPEG)
 - Moving Picture Expert Group-4 (MPEG-4)
 - MP4 Export or Latest

22. All streams to the above locations shall be available in real-time and at full resolution. Resolution and other related parameters shall be configurable by the administrator in order to provide for network constraints.
23. The VMS shall support field sensor settings. Each channel configured in the VMS shall have an individual setup for the following settings, the specific settings shall be determined according to the encoding device.
24. The VMS shall support the following operations:
 - Adding an IP device
 - Updating an IP device
 - Updating basic device parameters
 - Adding/removing channels
 - Adding/removing output signals
 - Updating an IP channel
 - Removing an IP device
 - Enabling/disabling an IP channel
 - Refreshing an IP device (in case of firmware upgrade)
 - Multicast at multiple aggregation points
25. The VMS shall support retrieving data from edge storage. Thus when a lost or broken connection is restored, it shall be possible to retrieve the video from SD card and store it on central storage. System should support to view the recordings available over cameras local storage device (such as an SD card), and copy them to the server.
26. The VMS shall support bookmarking the videos. Thus, allowing the users to mark incidents on live and/or playback video streams.
27. The VMS shall allow the administrator to distribute camera load across multiple recorders and be able shift the cameras from one recorder to another by simple drag and drop facility.
28. VMS shall support automatic failover for recording.
29. VMS should also support dual recording or mirroring if required.
30. VMS shall support manual failover for maintenance purpose.
31. VMS shall support access and view of cameras and views on a smartphone or a tablet (a mobile device).
32. VMS shall support integration with the ANPR/RLVD or other video analytic application.
33. VMS shall support integration with other online and offline video analytic applications.
34. VMS shall be able to accept alerts from video analytics built into the cameras, other third party systems, sensors etc.

35. The system shall provide remote users with rich functionality and features as described below:
 - Viewing live video from cameras on the surveillance system.
 - Browsing recordings from storage systems.
 - Creating and switching between multiple of views.
 - Viewing video from selected cameras in greater magnification and/or higher quality in a designated hotspot.
 - Using digital zoom on live as well as recorded video.
 - Using sound notifications for attracting attention to detected motion or events.
 - Getting quick overview of sequences with detected motion.
 - Getting quick overviews of detected alerts or events.
 - Quickly searching selected areas of video recording for motion
36. The system shall offer live view of up to 20 or more cameras, including PTZ control (if applicable) and event / output activation. The Playback function shall give the user concurrent playback of multiple recorded videos with date, alert sequence or time searching.
37. User Authentication – The system shall support logon using the user name and password credentials
38. Shall allow distributed viewing of multiple cameras on the system on any monitor.
39. Shall access the H.264/MJPEG/MPEG4 or higher streams from the connected camera directly and not sourced through the recording server
40. The System shall allow for continuous monitoring of the operational status and event triggered alarms from various system servers, cameras and other devices. It shall provide a real-time overview of alarm status or technical problems while allowing for immediate visual verification and troubleshooting.
41. The system shall provide interface and navigational tools through the client including.
42. Graphical overview of the operational status and alarms from servers, network cameras and external devices including motion detectors and access control systems.
43. Intuitive navigation using a map-based, hierarchical structure with hyperlinks to other maps, servers and devices or through a tree-view format.
44. The system shall include flexible access rights and allow each user to be assigned several roles where each shall define access rights to cameras.
45. Basic VMS should be capable to accept third party generated events / triggers.
46. The System shall offer centralised management of all devices, servers and users.
47. The System should not have any limit on the number of cameras to be connected for Surveillance, Monitoring and Recording. Any increase in the no. of cameras should be possible by augmentation of Hardware components.

48. The System shall support distributed viewing of any camera in the system using Video walls or big screen displays.
49. The 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.
50. It should be possible to integrate the 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.
51. The system shall store the overall network elements configuration in central database, either on the management server computer or on a separate DB Server on the network.
52. System should be able to be integrated with or should have built-in Event Management /Incident Management System.
53. The System shall provide a feature-rich administration client for system configuration and day to-day administration of the system.
54. The System shall support different logs:
 - The System Log
 - The Audit Log
 - The Alert Log
 - The Event Log
55. The system shall support the use of rules to determine when specific actions occur. Rules shall define what actions shall be carried out under specific conditions. The system shall support rule initiated actions such as:
 - Start and stop recording
 - Set non-default live frame rate
 - Send notifications via email
 - Pop-up video on designated Client Monitor recipients
56. System should have a facility to create CDs or other storage media for submission to Judiciary, which can be treated evidence for legal matters. Such storage media creation should be tamper proof and MSI to provide appropriate technology so that integrity and quality of evidence is maintained as per requirements of the judiciary. MSI is required to specify any additional hardware / software required for this purpose. The MSI will also prepare the guideline document in coordination with the Police Department to be followed by the Police Personnel for the retrieval of Video / images from the CCTV System so as to maintain integrity of the evidence. Such a guideline document should include

but not limited to, methods of retrieval of data, check-list to be followed and flowchart of the entire process to be followed.

57. All the systems proposed and operationalization of Video Management System should comply with requirements of IT Acts issued by Government of India.
58. Security Platform shall have strong security mechanism such as the use of advance encryption/digital certificates/ authentication to ensure that only authorized personnel have access to critical information, prevent man-in-the-middle attacks, and that the data is kept private.
59. System should ensure that once recorded, the video cannot be altered, ensuring the audit trail is intact for evidential purposes.

Video Display System

1. Shall view live or recorded video from resizable and movable windows
2. Should have an ability to perform video controls for video systems from workstation
3. Shall play, fast-forward, rewind, pause, and specify time to play recorded video
4. Shall take a video still image (snapshot) from live or recorded video
5. Shall export video for user specified time and duration
6. Shall have the capability to move PTZ cameras
7. Shall view Video in Video Matrix
8. Shall display in 1x1, 2x2, 3x3 and 4x4 window formats
9. Shall enable operator to specify video windows to be displayed in matrix
10. Shall enable matrix settings to be saved per user
11. Shall view either live or recorded video can be displayed in the video matrix window.
12. Shall enable video snapshot to be taken and saved from any window pane in the matrix view
13. Shall enable the user to pause the rotation of video and resume the video rotation again
14. Shall enable alarms to be generated from any video pane
15. Shall enable user to only view and control video for which they have been assigned permissions by the administrator
16. Shall manually create an alarm from the live or recorded video with specified severity and description.

Recording and Storage

1. The storage solution proposed is that the video feeds would be available for 90 days. After 90 days, the video feeds would be archived unless it is flagged or marked by the Police or 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 or Authority deem it good for deletion.
2. For incidents that are flagged by the Police, Authority or any court order, the video of the relevant portion from all relevant cameras should be stored/archived separately for investigation purposes and a committee at Authority can decide when this video feed can be deleted.
3. 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.
4. The system shall support the use of separate networks, VLANs or switches for connecting the cameras to the recording servers to provide physical network separation from the clients and facilitate the use of static IP addresses for the devices.
5. The system shall support H.264 or better, MPEG-4 and MJPEG compression formats for all IP cameras connected to the system.
6. The system should not limit amount of storage to be allocated for each connected device.
7. The system shall allow for the frame rate, bit rate and resolution of each camera to be configured independently for recording. The system shall allow the user to configure groups of cameras with the same frame rate, bit rate and resolution for efficient set-up of multiple cameras simultaneously.
8. The system shall support archiving or the automatic transfer of recordings from a camera's default database to another location on a time programmable basis without the need for user action or initiation of the archiving process. Archiving shall allow the duration of the camera's recordings to exceed the camera's default database capacity. Archives shall be located on either the recording server or on a connected network drive. If the storage area on a network drive becomes unavailable for recording the system should have the ability to trigger actions such as the automatic sending of email alerts to necessary personnel.
9. Bandwidth optimization - The Recording Server / System shall offer different codec (H.264, H.265, MJPEG, MPEG-4, etc.) and frame rate (CIF, 4CIF, QCIF) options for managing the bandwidth utilization for live viewing on the Client systems.
10. From the Client systems, the user shall have the option of having video images continually streamed or only updated on motion to conserve bandwidth between the Client systems and the Recording Server.
11. The Recording Server/System shall support Camera devices from various manufacturers.
12. The Recording Server/System shall support the PTZ protocols of the supported devices listed by the camera OEMs.

13. The system shall support full two-way audio between Client systems and remote devices i.e. CCTV.
14. Failover Support - The system shall support automatic failover for Recording Servers. This functionality shall be accomplished by Failover Server as a standby unit that shall take over in the event that one of a group of designated Recording Servers fails. Recordings shall be synchronized back to the original Recording Server once it is back online. The system shall support multiple Failover Servers for a group of Recording Servers.
15. SNMP Support - The system shall support Simple Network Management Protocol (SNMP) in order for third-party software systems to monitor and configure the system. The system shall act as an SNMP agent which can generate an SNMP trap as a result of rule activation in addition to other existing rule actions.

Video Analytics

The Video Analytics shall be designed to provide Intelligent Video Analysis for 24/7 surveillance with support for devices from different vendors.

1. Support any architecture namely distributed, centralized and hybrid.
2. Support system openness without using any proprietary format.
3. Support commercial-off-the-shelf computing hardware without the need of any proprietary hardware.
4. Able to produce reliable analytics at lower resolutions like 4CIF resolution in order to save the computation.
5. Able to process at variable resolution and frame rate when if necessary.
6. It shall support open platform Video Management System (VMS).
7. It shall provide ONVIF (Open Network Video Interface Forum) device discovery.
8. It shall get video from camera or VMS and send alarms to VMS to be viewed in VMS client.
9. It shall stream the Analytics Video to VMS using open interface protocol like ONVIF.
10. It shall support multiple regions of analytics on single video feed.
11. It shall support multiple features to be enabled for each of the regions.
12. It shall support feature based scheduling so that that alarms can be enabled or disabled for a certain period of time.
13. It shall support both Virtual line and Virtual area based features. The virtual area can be of any shape and can be bound by at least 10 end points.
14. It shall support both indoor and outdoor environment.
15. It shall support setting of minimum and maximum object size for detection.

16. It shall support masking of area in a view.
17. It shall support object masking.
18. It shall support color detection for vehicle & Object.
19. It shall support alarms to filter based on object color, size, speed and aspect ratio.
20. It shall support analytics capability to run both on server as well as edge (on camera).
21. It shall support simultaneous running of different features both on edge as well as server for same camera.

All cameras should support motion detection, camera tampering and audio analytics. All cameras must be capable to run two analytics in addition to motion detection and camera tampering as required at any given time.

Solution shall be so designed to have automated PTZ camera control for zooming in on interesting events like motion detection etc. as picked up by camera without the need of human intervention. It shall be completely scalable, with a many-to-many Authority-server model allowing multiple physical systems to be used in an array of servers.

Surveillance system shall have the capability to deploy intelligent video analytics software on any of the selected cameras. This software shall have the capability to provide various alarms & triggers. The software shall essentially evolve to automate the Suspect activity capture and escalation; eliminate the need of human observation of video on a 24x7 basis.

Analytics software shall bring significant benefit to review the incidences and look for suspicious activity in both live video feeds and recorded footages.

Various video analytics that shall be offered on identified cameras are

1. Parking Violation
2. Wrong/One-way detection
3. Stopped vehicle
4. Slow traffic/congestion detection
5. Crowd detection
6. People loitering within restricted area
7. Motion detection
8. Walking against mandatory flow/pedestrian movement
9. Unattended/abandoned object and tracking
10. Detection and classification of human, animal and vehicle

11. Behavioural Biometry: Identification through multiple behaviour (Optional)
12. Accident detection
13. Person collapsing
14. Gesture recognition: Identification through gesture change
15. 'Vehicle of interest' tracking by colour, speed, number plate
16. Unwanted/ banned vehicle detection
17. Scheduled Reports and Alarms (Customizable MIS reports shall be possible)
 - a) Rule based scene analysis and alarms
 - b) Scene based SOPs
 - c) Real time alarms sent to authorized personal for action
 - d) Real-time scene analysis and counting data based on user definable rules
 - e) Reduce false alarms
 - f) Heat mapping
 - g) Video/Camera events - signal lost and restored
 - h) Alarm management
 - i) Real time alarm alerts used to perform specific actions using customization like video recording and snapshots
18. Other camera based analytics
 - a) Automatic Number Plate Recognition (ANPR)
 - b) Red Light Violation Detection (RLVD)
 - c) Speed violation detection system (SVDS)
 - d) Face Recognition System (FRS)

However, the list of functionalities mentioned are not limited to. MSI has to study the user requirements further and implement the solution.

The solution shall enable simultaneous digital video recording from network, intelligent video analysis and remote access to live and recorded images from any networked computer. It shall be able to automatically track and classify objects such as cars & people and push content to the respective security personnel as required for real time analysis. The system shall also have display of time line, customizable site map, live video, video playback, integrated site map, remote live view, multi-site capability, encryption, watermarking and event based recording.

All cameras should support motion detection, camera tampering and audio analytics. All cameras must be capable to run two analytics in addition to motion detection and camera tampering as required at any given time.

Central Application

1. The software shall be able to run on any PC based on industry standard OS.
2. The software shall support ONVIF compliant cameras and devices.
3. The software shall show live video from IP Cameras and Video Transmitters in MJPEG, MPEG4 H.264, H.265 formats.
4. The software shall support cameras with resolutions ranging from Standard Definition, High Definition (HD) and up to 5 Megapixel.
5. The software shall show video across 4 displays per workstation - each display can have up to 25 viewing panes.
6. The software shall allow configuration of the video and audio stream settings for each user, depending on the support hardware.
7. Users shall be able to change the video pane layout in each of the 4 screens independently:
 1. Grid layouts: 1x1, 2x2, 3x3, 4x4, 5x5
 2. Widescreen layouts: 2x3, 3x4, 4x6
 3. Hotspot layouts based on 3x3, 4x3, 4x4, 5x5 larger pane in top, left
 4. Hotspot layouts based on 4x3, 4x4, 5x5 larger panes in centre
8. Users shall be able to change the aspect ratio in each of the 4 video windows independently in order to display Standard Definition or High Definition video. Choose between:
 1. Widescreen (16:9)
 2. Standard (4:3)
9. Users shall be able to move any image from one display screen to another via drag-and-drop.
10. Users shall be able to digitally zoom up to 1000% and also digitally scroll live video from any camera using the mouse wheel.
11. The software shall allow the removal of interlacing artefacts from 4SIF video using the following criteria:
 1. Best performance
 2. Best image quality
 3. Smoothest rendering
12. The software shall allow the display of objects detected via analytics on the video (up to 10 at once).
13. Users shall be able to view stream statistics on all current video streams, including the following information:
 1. Frame rate
 2. Resolution (SIF, 2SIF, 4SIF, 720p, 1080p, 5MP)
 3. Current bit-rate

4. Audio bit-rate

Face Recognition System:

The facial recognition system shall be enabled at cameras identified by the purchaser. These cameras identified shall be installed at critical locations as identified by police department. The facial recognition system in offline mode shall be provided by the MSI in line with the requirement of police. Sufficient online and offline licenses shall be planned based on detailed system study.

The functional requirement specification of the facial recognition system is as follows:

Sl. No.	Parameter	Minimum Specifications
1	General Requirements	The facial recognition system should be able to integrate with IP Video Cameras as required in the solution and shall be able to identify multiple persons of interest in real-time, through leading-edge face recognition technology. The system shall be able to recognize subjects appearing simultaneously in multiple live video streams retrieved from IP surveillance cameras.
		The facial recognition system should be able to work on the server/desktop OS as recommended by OEM and provided by the Master System Integrator
		The user interface of the facial recognition system should have a report management tool without installation of any additional client software. It should be able to generate real time report such as Audit log report, Hit List Report, Daily Statistics Report, and Distribution Report.
		The facial recognition system should be accessible from 5 different Desktop/ laptops at any given time. When choosing a distributed architecture, the system shall be able to completely centralize the events and galleries from each local station into a unique central station, devoted to management and supervision
		The system should have ability to handle initial real-time watch list of at least 10,000 Faces (scalable to at least 1 Million faces) and 50 Camera Feeds simultaneously and generate face matching alerts
		The algorithm for facial recognition or the forensic tool should be able to recognise partial faces with varying angle
		The system should be able to detect multiple faces from live single video feed
		The system should have combination of eye-zone extraction and facial recognition
		The system should have short processing time and high recognition rate

		The system should be able to recognize faces regardless of vantage point and any facial accessories/ hair (glasses, beard, expressions)
		Face detection algorithms, modes and search depths should be suitable for different environments such as fast detection, high accuracy etc. The FRS system shall use of GPU technology instead of Traditional CPUs, to greatly improve the computational performance in crowded environments.
		The system should be able to identify and authenticate based on individual facial features
		The system should be compatible with the video management system being proposed by the Master system integrator
		The system should have capability for 1:1 verification and 1:N identification matching
		The system should be able to integrate with other systems in the future such as 'Automatic fingerprint identification system (AFIS)' etc.
		The system should be able to support diverse industry standard graphic and video formats as well as live cameras
		The system should be able to match faces from recorded media
		The system should be able to detect a face from a group photo
		The system should be able to trace from stored videos of any format
		The system should have bulk process of adding faces in the system
		The system should allow users to search or browse captured faces (based on date or time range), export any captured image for external use with a capability to support a Handheld mobile with app for windows OS or android OS to capture a face on the field and get the matching result from the backend server
		The proposed solution should provide the ability to assign different security levels to people and places. It should alert security staff when someone is spotted in an area where they're not permitted, whilst allowing them free access to non-restricted/public areas
		The system should be able to detect faces in different environmental changes like rain, wind, fog and poor light
		The system should have the facility to categorize the images like "Remember this person" or "hit-list" or "wanted".
		The OEM should have deployed the solution in India
		The system shall be able to do the parallel processing of long videos, so that operators can start working quickly even if videos are big
2	Integration with CCTNS and other databases	System shall be integrated with existing database as required
		The system should have the capability to link the captured data to CCTNS application using a Unique key / cases number/ FIR number and be able to send required reports / BI analysed data / raw data to CCTNS application and receive acknowledgement

		<p>System should have the capability to generate the fortnightly / monthly detailed report of the data shared with the CCTNS application. This will be required and support while conducting the forensic internal audits</p> <p>System should have the capability to integrate the Analytics Engine module with CCTNS application, so that at point of time if required, the intelligence capabilities of solution will benefit in smart policing</p> <p>The search module of our smart city solution designed under integration requirement of CCTNS application should have the capability to perform forensic data analytics and cyber threat intelligence to analyse and anticipate where the likely threats are coming from and when, increasing readiness</p>
3	Case Management	<p>The system shall be able to create cases corresponding to investigation operations</p>
		<p>The system shall be able to manage videos and photos within a certain case</p>
		<p>The system shall be usable by numerous investigators or video analysts together on the same case, working in parallel or in series, so that big cases could be processed efficiently</p>
		<p>The system shall make the findings of one operator immediately and easily available to all other operators, to increase video / photo case analysis efficiency and speed</p>
		<p>The system shall give a holistic view of all videos and photos of a case, so that operators get a full picture of the case (and not limited view, item by item)</p>
		<p>The system shall include purge capability at the case level or at the video level</p>
		<p>The system shall include the ability to backup and restore cases</p>
		<p>The system shall make it easy to navigate across the whole set of video and photo of the case for people and vehicle</p>
		<p>The system shall be able to manage video flow from IP cameras as RTSP streams</p>
4	Video and Photo Management	<p>The system shall be able to record live video flows or to rely on external video flow recording (e.g. in a DVR), to offer the same functionality on past live video than on recorded videos</p>
		<p>The system shall be able to manage videos up to 4K resolution, with no limitation in length or frame rate</p>
		<p>The system shall be able to ingest and manage any photo in JPEG or PNG format, of any size</p>
		<p>The system shall be able to manage context metadata on video and images (geographical location, image acquisition conditions, time stamp).</p>
5	Data Management	<p>The system shall allow edit, detect, and extract content metadata from videos and photos</p>
		<p>The System should allow Navigation of videos based on timestamp</p>

		The system shall be able to detect and extract content metadata from the live and recorded video and photos of a certain case: for person's face, body and vehicle's license plate
		System's users shall be able to control which metadata is extracted from the videos and photos of a case, individually at the video or photo level
		With face metadata, the system shall be able to detect and record a best image of the face, the gender and age range of the corresponding person, and generate a feature vector making it possible to use face for biometric comparison
		With person body metadata, the system shall be able to detect and record a best image of the person, the colour of the upper body and lower body of the person
		With license plate meta data, the system shall be able to detect and record a best image of the license plate, and the OCR corresponding to this license plate
		User friendly interface for browsing videos and photos such as filtering, album view and support adding descriptive text and sharing
		Meta data shall provide filtering like face, body, license plate, age, gender, upper body, lower body, colour, moving object etc.
		The system shall provide functions for colour marking in images included in reports and blurring out areas for privacy reasons
		The system shall provide operator with fast viewing tools on video: video display at variable speeds
		The system shall provide operators with most efficient abstract of individual videos: concatenation of sequence which are likely to be where wrong doing or suspect activity can be seen, restricted area of the video., face, people seen by their body, either in the full video or on a restricted area of the video, license plates
		The system shall display where specific types of detection have been found, as heat maps at any time or at a selected timeframe
		The system shall make it easy for operators to determine if multiple different people have been together / are related
6	Alerts	The system shall be able to search by face, in real time, in live video flows, people recorded in watch list and raise alerts when someone recorded in a watch list has been seen. Alerts review shall be available to operators
		The system shall offer parameters to select which faces detected in real time will be matched against the watch lists, in order to minimize false alerts

		The system shall include an advanced alert presentation user interface, both for watch list alerts and tracking alerts, by which the operator shall be able to see where the alert happened (on a map), the context of the alert, the person causing the alert and the person recorded in a watch list or tracked.
		The system shall include a personalized alert presentation user interface, where it is possible depending on operator right to select which kind of alerts are received and to tune the threshold used for the generation of alerts, at the camera and watch list levels.
		The system shall be capable of sending out the alerts as notifications, so that external systems and users could also see the alerts
		The system shall include a query capability to search detections within the whole case by textual description
7	Search	<p>The query results shall be easily displayed as a list of suitable respondents</p> <p>The query results shall be easily displayed as a map showing where the suitable respondents were seen</p> <p>The system shall display the path of respondents on a map</p> <p>The system shall make it easy for operator to visualize detect objects trajectories</p> <p>The query results shall be easily displayed as a graph where suitable respondent will be linked to each other if they appear on the same video or photo (i.e. together) in a configurable time interval</p>
8	Watch list Management	<p>The system shall come with watch lists management capabilities, where watch list will contain person data represented by face</p> <p>The system shall be able to attach watch lists to cases, so that upon detection of a face in a case, the face would be compared to all the watch lists attached to the case, and the corresponding comparison results could be shown to operators</p> <p>The system shall automatically associate a face detection to a watch list element when the comparison yields a score that is high enough</p> <p>A watch list search review interface should be proposed to operators, so that they could easily determine who in the available watch lists was seen in the videos and photos of a certain case</p> <p>Watch list management shall include deduplication of watch list content, so that it could be known if a given person already belongs to a watch list</p> <p>Watch list management shall include the ability to add a face detected in a case into a give watch list in one click</p> <p>The system shall be able to import face images in its watch lists by batch</p>
9	Security	<p>The system shall manage access control of operators</p> <p>The system shall manage security (access restriction) on watch lists</p> <p>The system shall manage security (access restriction) on cases</p>

		The system shall manage security (ability to use) on available functions
		The system shall manage users preferences (please specify what is managed)
10	Reports	The system shall include the ability to produce reports easily usable for investigators and in court
		The system shall come with a set of management reports
		The system shall come with dashboards showing the activity of the system

General camera specifications:

1. The camera shall use an Ethernet 10/100Base-TX network interface with RJ45 connector.
2. The camera and the associated equipment shall support communication protocols IPv4, IPv6, TCP, UDP, HTTP, HTTPS, DHCP, IGMP, ICMP, ARP, SNMP, Telnet, FTP, NTP, RTSP, and RTP as a minimum.
3. The camera shall incorporate a built-in web server, built-in FTP server, and a built-in FTP Authority.
4. The cameras shall have, at a minimum, the following configurable features:
 - a) Image resolution
 - b) Frame rate
 - c) Image quality adjustments (brightness and contrast)
 - d) Source and destination IP address settings
 - e) UDP port number
 - f) Bandwidth limits
 - g) Unicast and multicast settings, and
 - h) Support for two (2) simultaneous unicast streams
5. The cameras shall support at the minimum three individually configured video streams. The cameras shall be capable of three or more simultaneous streams with one of the streams being in H.264 or H.265 format.
6. All cameras shall have an operating temperature range of 0°C to +60°C (14°F-40°F to 122°F) at humidity: 20% -90% RH.
7. The environmental housing shall be of suitable size and provide a temperature controlled atmosphere for the camera, lens and receiver driver.
8. The housing shall allow for easy disconnect of all external cables.

9. The housing, mounting arm and the dome camera installed assembly shall be suited to withstand wind gusts of 150 km/h.
10. The housing shall meet the IP67, IK10 for protection.
11. The cameras shall have a Mean Time between Failure (MTBF) of at least 90000 hours. The Bidder may propose best specification as per the proposed solution and city requirements

Fixed and PTZ Camera, Lenses and Mounts

1. The camera should be manufacturer's official product line designed for commercial / industrial 24x7x365 use. The camera and camera firmware should be designed and developed by same OEM
2. The camera control shall comply with the latest release of Open Network Video Interface Forum (ONVIF) standards.
3. The camera shall include an integral receiver/driver. The receiver/driver shall be capable of controlling pan-tilt, zoom and focus locally and remotely from the JICCC.
4. The camera shall incorporate Automatic Gain Control (AGC) circuitry to provide for compensation at low light levels.
5. The lens shall be integrated with the camera.
6. Video output resolution shall not be less than 1920x1080 pixels.
7. The camera shall be capable to produce minimum 25 frames per second (fps)
8. The camera shall provide automatic white balance, automatic exposure, automatic gain control, electronic shutter, and backlight compensation.
9. The camera shall be a true day/night cameras with mechanical IR cut filter.
10. The camera shall be capable of providing a high contrast color picture with a full video output at a minimum illumination as mentioned in the specifications.
11. Automatic light range circuits shall be included to provide compensation for variations in scene brightness. The circuits shall provide pictures over a light range of 1 million to 1.
12. All cameras shall capture high definition video, compress the video using H.265 technique and transmit real-time using fiber optic based communications system.
13. The cameras shall capture audio and compress using G.711 technique and transmit real-time using fiber optic based communications system.
14. All cameras shall support on-board real-time video content analysis.
15. All cameras shall support both Constant Bit-Rate (CBR) and Variable Bit Rate (VBR) options.
16. The camera shall support up to 2 video profiles, each providing independent configuration of bit rate, frame rate and resolution.
17. The camera shall support video compression from 64kbps up to 10Mbps.

18. The camera shall support audio compression using the G.711 compression algorithm, streaming @ 32Kbps per channel sampled at 8 KHz or 16 KHz with a 16-bit resolution.
19. The camera shall support on-board storage via micro SDHC slot and card with a minimum capacity of 64 GB.
20. All cameras shall have integral in-built or external IR technology. For fixed cameras, the IR shall support a range of at least 50m and for PTZ it shall support a range of at least 200m moving with zoom.
21. For Fixed Cameras:
 - a. The fixed camera shall provide a minimum focal length range of 2.8-10 mm compensated with a minimum 12x digital zoom, Full HD (1080P), Auto IRIS / P IRIS, Corrected IR, CS Mount with IR cut filter and shall be remotely controllable from the camera control transmitter at JICCC.
 - b. The fixed camera shall capture video using 1/3.2" with True WDR, Progressive CMOS Sensor or better.
 - c. Fixed Camera resolution shall be 1920 x 1080 or better.
22. For PTZ Cameras:
 - a. Camera shall have capabilities of PAN of 360° continuous.
 - b. Camera shall have capabilities of Tilt of 180°.
 - c. Lens of 4.3 mm-129 mm with minimum 30X optical and 12X digital zoom.
 - d. PTZ camera shall capture video using minimum 1/3.2" with True WDR, Progressive CMOS Sensor or better.
 - e. It shall support resolution of 1920x1080 or better.
23. Camera shall support tilt of 100° either side. The tilt capability shall include both the horizontal (level view) and vertical (downward view) position. If the camera travels beyond straight down, automatic image flip circuitry shall prevent the display of an inverted image.
24. The pan and tilt mechanism shall be an integral part of the camera.
25. Pan speed shall be between 0.1-350°/s and Tilt speed shall be 0.1-350°/s.
26. There shall be a minimum of 100 assignable automatic pre-set positions.
27. There shall be a minimum of 8 definable privacy zones.
28. All cameras shall provide effective 24/7 imaging performance for CCTV surveillance applications.
29. All cameras should have IP 66 compliant enclosure
30. All cameras should be UL, CE, FCC, ONVIF 2.x/S certified
31. All cameras should be POE/POE+ IEE 802.3af compliant
32. The cameras should not be an end of life / end of service product.

33. All cameras shall provide user control, with remote configuration for functions including streaming and compression settings, exposure, white balance, flicker control, picture size, cropping/privacy, brightness, sharpness, saturation, day-night switching point, frame rate, image rotation, snapshot, dynamic bandwidth allocation and motion detection.
34. All cameras should have Vandal and impact resistant housing, IK 10, IP66/ NEMA 4X

Technical Specifications:

High Definition Fixed Box Camera with IR

Sl. No.	Parameter	Minimum Specification
1.	Image Sensor	1/2.7" progressive scan RGB CMOS
2.	Operating Frequency	50 Hz
3.	Day/ Night Operation	Yes with IR Cut Filter
4.	Minimum Illumination	Colour: 0.2 Lux @ 30 IRE B/W": 0.01 @ 30 IRE 0 Lux with Built in or External IR, IR Range 100 Meters
5.	Low light Capability	The camera shall be able to provide usable Color video in low light conditions
6.	Lens	8-50mm IR corrected, CS-mount lens, P-Iris
7.	Electronic Shutter	1/25 to 1/15000. or better
8.	Image Resolution	1920 x 1080, 1280 x 720, 800 x 450, 480 x 270, 320 x 240
9.	Compression	H.265 in High and Base profile, MPEG4, MJPEG
10.	Frame Rate and Bit Rate	50 FPS at all resolutions with Controllable Bit Rate/ Bandwidth and Frame Rate
11.	Video Streams	Minimum 3 Streams in H.265, 2MP, 25 fps
12.	Motion Detection	Yes built in with multiple configurable areas in the video stream
13.	Pan Tilt Zoom	Digital PTZ
14.	Electronic Exposure & Control	Automatic/ Manual
15.	Wide Dynamic Range	120 dB or better
16.	Backlight	Required

Sl. No.	Parameter	Minimum Specification
	Compensation	
17.	Privacy Masks	minimum 8 configurable 3D zones
18.	Connectors	1 Input & 1 Output for Alarm Interface
19.	Event Triggers	Intelligent video, Edge Storage event, External Input, Audio Level, Motion Detection, Day/Night Mode, Network, Time scheduled, Manual Trigger, Alarm Input Trigger
20.	Event Actions	File upload: FTP, HTTP, network share and email Notification: email, HTTP and TCP. PTZ function, Edge Storage/ NAS Storage, Pre & Post Alarm Recording, Actions configurable by web interface, External Output activation.
21.	Edge Storage	Built in SD card slot with support up to 128 GB with Class 10 speed
22.	Built in installation aids	Focus assistant, Pixel counter, Remote back focus
23.	Storage	The Cameras shall have the feature to directly record the videos/images onto NAS/SAN without any Software or integration
24.	Protocols	IPv4/v6, HTTP , HTTPS b, SSL/TLS b, QoS Layer 3 DiffServ, FTP SMTP, UPnP™,SNMPv1/v2c/v3 (MIB - II), DNS, DynDNS, NTP, RTSP, RTP,TCP, UDP,IGMP,RTCP,ICMP, DHCP,ARP,
25.	Text Overlay	Date & time, and a customer-specific text, camera name, graphical image etc.
26.	Security	Password protection, IP address filtering, HTTPS encryption, IEEE 802.1Xa network access control, Digest authentication, User access log
27.	Firmware Upgrade	The firmware upgrade shall be done through web interface, The firmware shall be available free of cost
28.	Logs	The camera shall provide minimum 200 logs of latest connections, access attempts, users connected, changes in the cameras etc.
29.	Interface	RJ 45, 100 Base TX
30.	Enclosure	IP66-and NEMA-4X-rated casing (polyester polycarbonate blend)

Sl. No.	Parameter	Minimum Specification
31.	Power requirements	Vendor to Specify
32.	Operating Temperature	-10 °C to 60 °C
33.	Operating Humidity	Humidity 20–90% RH (condensing)
34.	Certification	UL, CE, FCC, IEC
35.	Application Programmers Interface	The interface shall be available for integration with 3rd party analytics and applications in public domain free of cost
36.	Housing, Mount and IR	Shall be of the same make of OEM or better
37.	Onvif	S Required
38.	Warranty	Min 3 Years OEM Warranty

High Definition PTZ Dome Camera

Sl. No.	Parameter	Minimum Specification
1.	Image Sensor	1/2.8" Progressive Scan CMOS or better
2.	Operating Frequency	Min 50 Hz
3.	Day/ Night Operation	Automatic with IR Cut Filter
4.	Minimum Illumination	Colour: 0.05 Lux B/W": 0.01 Lux or better
5.	high-speed pan-tilt functionality	360° endless pan range and a 180° tilt range
6.	Optical Zoom	30x Minimum & 12x Digital Zoom, Total 360x Zoom or better
7.	Lens	4.5-129 mm or better
8.	Pan, tilt, manual and pre-set speed The speed shall be applicable for Manual, Tour and Pre-set Mode	Auto 360° endless pan range and a 160° tilt range or better Manual Pan: 0.5°/s - 240°/s; Manual Tilt: 0.5°/s - 120°/s; preset speed: 240 °/s or better

Sl. No.	Parameter	Minimum Specification
9.	Image Resolution	1920 x 1080 or better
10.	Compression	H.265 Baseline, Main and High Profiles, Motion JPEG
11.	Frame Rate and Bit Rate	25 FPS at all resolutions with Controllable Bit Rate/ Bandwidth and Frame Rate. In CBR Priority to be defined for Video quality or frame rate and the bandwidth upper limit shall not exceed the defined limit
12.	GOP/ GOV	Ability to change the GOP/GOV Length to optimize the bandwidth and storage
13.	Video Streams	Minimum 3 Streams @ 1920x1080, H265, 25 fps
14.	Motion Detection	Yes built in with multiple configurable areas in the video stream
15.	Electronic Shutter	1/10000 s to 1 s or better
16.	Electronic Exposure & Control	Automatic/ Manual
17.	Wide Dynamic Range	90 dB or Better
18.	Backlight Compensation	Required
19.	Electronic Image Stabilization	Required
20.	Image Freeze on PTZ	Required
21.	Privacy Masks	Minimum 8 configurable 3D zones or better
22.	Pre-set Positions	Minimum 256 or better
23.	Image Flip	Yes Automatic
24.	Guard Tour	Minimum 2 Nos
25.	Built In Heater & FAN	Required
26.	Temperature Control	Required
27.	Alarm	Min 2 Alarm Input / Output ports or better
28.	On-screen directional indicator	Required
29.	Compression	The camera shall for its H.265 implementation support scene adaptive bitrate control, in order to lowering bandwidth and storage requirements.

Sl. No.	Parameter	Minimum Specification
		The camera shall support automatic dynamic GOP for optimal bitrate utilisation. The camera shall support automatic dynamic ROI to reduce bitrate in un-prioritized regions.
30.	Event Triggers	The camera shall be able to send and received trigger directly from any other camera without interface of VMS. Live Stream Accessed, Motion Detection, Shock Detection, Audio Detection, Network, Temperature, Manual Trigger, Virtual Inputs, Alarm Inputs, PTZ: Error, Moving, Pre-set Reached, Ready, Storage Disruption, Storage Recording, System Ready, User schedule
31.	Event Actions	File upload via FTP, SFTP, HTTP and email Notification via email, HTTP and TCP Pre- and post-alarm video buffering, External output activation, PTZ pre-set, guard tour, Video recording to edge storage, Day/night mode, Overlay text
32.	Pixel Counter	Built in
33.	Edge Storage	Built in SD card slot with support up to 128 GB with Class 10 speed
34.	Storage	The Cameras shall have the feature to directly record the videos/images onto NAS without any Software
35.	Protocols	At least IP, HTTP, HTTPS, SSL/TLS, TCP, ICMP, SNMPv1/v2c/v3 (MIB-II), RTSP, RTP, UDP, IGMP, RTCP, SMTP, FTP, DHCP, UPnP, ARP, DNS, DynDNS, NTP. IPv4 & IPv6
36.	Text Overlay	Date & time, and a customer-specific text, camera name, graphical image etc.
37.	Security	Password protection, IP address filtering, HTTPS encryption, IEEE 802.1Xa network access control, Digest authentication, User access log
38.	Firmware Upgrade	The firmware upgrade shall be done though web interface, The firmware shall be available free of cost

Sl. No.	Parameter	Minimum Specification
39.	Logs	The camera shall provide Minimum 200 logs of latest connections, access attempts, users connected, changes in the cameras etc.
40.	Interface	RJ 45, 100 Base TX
41.	Enclosure	Die Cast Aluminium, IP66 rated, polycarbonate clear dome and sunshield, PVC free complying to WEEE Standards
42.	Mount	Wall / Pole Mount
43.	Power requirements	Power over Ethernet (POE/PoE+) IEEE 802.3at Type 2 Class 4, max. 24 W, Typical 9W; 24 V DC max. 30 W 24 V AC, max. 40 VA or better
44.	Operating Temperature	-10 °C to 55 °C or better
45.	Operating Humidity	20–85% RH or better
46.	Certification	UL, CE, FCC
47.	Embedded Applications	The camera shall provide a platform allowing the upload of third party applications into the camera
48.	Application Programmers Interface	The interface shall be available for integration with 3rd party analytics and applications in public domain free of cost
49.	Onvif	S required
50.	Warranty	Min 3 Years OEM warranty

Multi Sensor 360° Panoramic View PTZ Camera

Sl. No.	Parameter	Minimum Specification
1	General Requirements	The camera should be manufacturer's official product line designed for commercial / industrial 24x7x365 use. The camera and camera firmware should be designed and developed by same OEM.
2	General Requirements	The camera should be based upon standard components and proven technology using open and published protocols

Sl. No.	Parameter	Minimum Specification
3	Image Sensor	2 MP Progressive scan RGB CMOS 4 x 1/2.8" or better
4	Lens Specs	Varifocal, 2.0–6 mm, F2.0 with 4x1080p or better
5	Video Resolution	1920 X 1080 or better
6	Minimum illumination	Colour: 0.4 lux or better, Monochrome: 0.05 Lux or better with IR
7	Video Compression	H.265, Motion JPEG
8	Frame Rate	15 fps or better
9	Wide Dynamic Range	100 dB or better
10	Camera Angle Adjustment	Pan: - ±90° Tilt: - 28° - 92° Rotate: - ±90°
11	Network Interface	100 Base-T ports
12	Power Supply	POE/POE+ IEE 802.3af compliant
13	Industry Standards	ONVIF Compliant
14	Certifications	UL, FCC
15	Enclosure Type	IP66; IK 08 or better
16	Operating Temperature	-10° C to 60° C or better
17	Operating Humidity	20 - 90%
18	Supported Network protocols	Minimum of the following RTSP, RTP/TCP, RTP/UDP, HTTP, DHCP protocols to be supported
19	Support	The system should not be an end of life / end of service product.

Bullet Camera

Sl. No	Parameter	Minimum Specifications
1	Image Sensor	1/2.8" progressive scan RGB CMOS or better
2	Operating Frequency	50 Hz
3	Day/ Night Operation	Yes with IR Cut Filter

4	Minimum Illumination	Color: 0.1 Lux, B/W: 0.1 Lux 0 Lux with IR
5	Mechanical Pan Tilt Adjustment	Pan: $\pm 135^\circ$, Tilt: 0° – 90°
6	Lens	3 - 16 mm or better, IR corrected, P-Iris, Megapixel Lens with remote zoom and focus
7	Electronic Shutter	1/25000 s to 1 s or better
8	Image Resolution	1920 x 1080 or better
9	Compression	H.265 compression or equivalent
10	Frame Rate and Bit Rate	Up to 60 FPS at all resolutions with Controllable Bit Rate/ Bandwidth and Frame Rate. In CBR Priority to be defined for Video quality or frame rate and the bandwidth upper limit shall not exceed the defined limit
11	Image reproduction	The camera shall have the capability to produce Colored video images in low light conditions
12	Video Streams	Minimum 3 Streams @ 1920x1080, H265, 25 fps
13	Motion Detection	Yes built in with multiple configurable areas in the video stream
14	Image Configuration	The Camera shall be able to Include or Exclude any area of any size/ dimension within the scene in order to Eliminate False alarm and also optimize the bandwidth and storage
15	Pan Tilt Zoom	Digital PTZ
16	Wide Dynamic Range	100 dB or better
17	Backlight Compensation	Required
18	IR	30 Meter (Built in or External) Optimized IR with adjustable intensity and angle
19	Alarm Connectors	1 Input & 1 Output for Alarm Interface
20	Event Triggers	Live Stream Accessed, Motion Detection, Day/Night Mode, Network, Temperature, , Camera Tampering, Edge Storage Disruption, Video Analytics, Manual Trigger
21	Event Actions	FTP, HTTP, network share, email Notification: email, PTZ function, Edge Storage/ NAS Storage, Pre & Post Alarm Recording, Actions configurable by web interface, WDR Mode, External Output Trigger, Text Overlay
22	Edge Storage	SD Card Slot with 128 GB Support Class 10 speed
23	Protocols	IPv4/v6, HTTP, HTTPS, SSL/TLS, QoS Layer 3 DiffServ, FTP, SMTP, UPnP, SNMPv1/v2c/v3 (MIB - II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SSH
24	Text Overlay	Date & time, and a customer-specific text, camera name, graphical image etc.
25	Security	Password protection, IP address filtering, HTTPS encryption, IEEE 802.1X network access control,

		Digest authentication, User access log
26	Firmware Upgrade	The firmware upgrade shall be done through web interface, The firmware shall be available free of cost
27	Interface	RJ 45, 100 Base TX
29	Enclosure	IP66 rated and NEMA-4X-rated casing Polycarbonate/Aluminum, IK 08
30	Power requirements	PE IEEE 802.3af / POE+ IEEE 902.3at compliant
31	Operating Temperature	-10 °C to 60 °C
32	Operating Humidity	Humidity 20–90% RH (condensing)
33	Certification	UL, CE, FCC, IEC,
34	Application Programmers Interface	The interface shall be available for integration with 3rd party analytics and applications in public domain
35	Embedded Applications	The camera shall provide a platform allowing the upload of third party applications into the camera
36	Mount	Wall Mount/ Pole Mount
37	Onvif	S Required
38	Warranty	5 Years OEM warranty
39	Security	Detection of camera tampering and Detection of Motion should be possible using either camera or VMS
40	Functional	Self-cleaning / anti-dust / hydro-phobic coating features
41	White Balance	Auto and Manual setting
42	Support	The system should not be an end of life / end of service product
43	General Requirements	The camera should be manufacturer's official product line designed for 24x7x365 use.
44	General Requirements	The camera should be based upon standard components and proven technology using open and published protocols

Body Camera

Sl. No	Parameter	Minimum Specifications
1	Dimensions	95.9 mm x 52.2 mm x 27.6 mm (3.78" x 2.06" x 1.09") ±5%
2	Weight	100-150 Grams
3	Lens	f/2.0 , 130° wide angle
4	Connection Interface	USB 2.0
5	Storage	64 Gb or Higher
6	Wi-Fi	Yes
7	Bluetooth	Yes

8	Microphone	Yes
9	Battery Life (Fully Charged)	12 Hours or more
10	Resolution	Full HD 1080P
11	Frame Rate	30 FPS
12	Operating Temperature	-10°C ~ 60°C
13	Storage Temperature	-10°C ~ 70°C
14	IP Rating	IP67
15	Viewing Angel	130° (diagonal)
16	IR	Built-in
17	Required Accessories	USB cable/360° rotatable clip/Adapter/Velcro holder

4.3 Intelligent Traffic Management System

Jalandhar, a city which has urbanized rapidly in recent years and due to usage of more cars than bikes, has witnessed enormous growth in traffic volumes which have, resulted in several traffic problems in and around the city, such as traffic jams, increase in number of road accidents etc. Therefore, it is intended to develop an Adaptive Traffic Control System (ATCS) & Automated Traffic Counting and Classification (ATCC). ATCS, which would aim at improving the efficiency and effectiveness of the traffic on arterial and VIP roads in Jalandhar roads and ATCC (Automated Traffic Counting and Classification) shall be implemented at the traffic junctions which are standalone.

To realize the benefits of ATMS & ATCC, it is pertinent to adopt an approach that includes technology based regulation, intervention, information and enforcement system to improve the mobility, discipline and safety on Jalandhar roads. Therefore, ATMS & ATCC is envisaged with multiple applications, including Adaptive Traffic Control System and Automated Traffic Counting and Classification (ATCC), Red Light Violation Detection (RLVD) systems, Automatic Number Plate Recognition (ANPR), Speed Violation Detection Systems (SVDS), Pilican Signals, Variable Message System (VaMS), eChallans, Traffic Surveillance Cameras & Pelican signals amongst others which will ensure that the intended outcomes have been accomplished.

ATMS & ATCC integrates various sub systems (such as CCTV, vehicle detection, communication, Local processing units, variable message signs etc.) in a coherent single interface that provides real time data on status of traffic and predicts traffic conditions for more efficient planning and operations. Thus, a system

such as ATMS & ATCC shall aim to help police and security agencies to take proactive/ reactive measures and ensure safe & smooth environment on road. Wherever the current Jalandhar City CCTV Surveillance System cameras can be utilized for the traffic management, necessary integration is expected.

The proposed technical solution should cater to the following challenges:

1. Traffic congestion and huge waiting time
2. No right of way to emergency vehicles like ambulance, police etc.
3. VIP movement clearance
4. Lack of information on prominent & frequent traffic congestions both location wise and time wise
5. Absence of street level public information & communication channel
6. Absence of central control mechanism to monitor & regulate the Jalandhar City traffic flow

The Key Performance Indicators

The KPIs for the project are as follows:

1. **Improve Journey Time Reliability:** Improve reliability in journey times between various locations, so that citizens can experience an enhanced quality of road based transportation, through improving sustainability and efficiency in operation of the road network
2. **Increased Traffic Signal Efficiency:** Reduction in traffic delays, optimized cycle times at intersection to regulate and maintain free flow of traffic to enhance the efficiency of the transport infrastructure.
3. **Increase Operational Efficiency:** Jalandhar Traffic Police intends to spend more time on the public facing functions. Thus Information technology solutions should help in reducing the repetitive paperwork/records and making the back-office functions more efficient.
4. **Improve Customer Services:** The traffic services to the public can be improved through the user friendly presentation of the various traffic information in real time through sharing of all relevant data feeds for public consumption.
5. **Safety Improvement:** The real time traffic monitoring and intelligent traffic systems can prevent accidents by recognizing and thus responding to the potentially dangerous situation in advance. It shall also provide safety for pedestrians.
6. **Higher Productivity:** Achieving improvement in the productivity, logistics and other economic activities by obtaining the precise-real time information on transport due to the availability of data on traffic flow in key areas of the city.

7. **Real Time Information, Event Tracking & Response, and Fast Access to Stored Information:** The real time information at the JICCC shall enable the operator to take necessary actions based on the type of information. Sending an emergency vehicle to the spot, arranging alternate route to VIP convoys, diverting the traffic to different routes are some of the actions that can be taken based on the Real Time Information. It shall be possible to track a particular event using the cameras installed at the traffic junction. A vehicle, violating the traffic could be tracked and penalized at the next traffic junction based on the number plate.
8. **Creating awareness for public:** Through sign boards, awareness on road traffic rules and safe driving precautions shall be imparted to road users.
9. **Enforcement:** Effective enforcement of traffic violation, checking and monitoring shall reduce the traffic related offences of Red Light violations
10. **Create a platform for sharing traffic information across the city:** There is a critical need to create a platform for sharing traffic related information among traffic police and citizens in order to increase the effectiveness of Adaptive Traffic Control System.
11. **Planning & Operations:** Intelligent Signal planning & operational aspects shall be handled at command centre using City Operations Platform/IoT Platform (COP).
12. **Integration:** Intelligent Signalling aspects shall be enabled by integration with City Operations Platform and GIS Maps.

Various Components of Intelligent Signalling

1. Intelligent traffic Management systems:
 - a) Adaptive Traffic Control System (ATCS) – Video based Vehicle detection (integrated signals forming a green tunnel), Signal controller, Traffic light aspects, poles, power supply provisioning and related accessories and associated civil work including cabling for successful operation of the system
 - b) Automated Traffic Counting and Classification (ATCC) – Video based Vehicle detection (Independent signal control), Signal controller, Traffic light aspects, poles, power supply provisioning and related accessories and associated civil work including cabling for successful operation of the system
2. Red Light Violation Detection (RLVD) System along with related accessories and required mounting infrastructure including civil work for successful operation of the system
3. Automatic Number Plate Recognition (ANPR) system along with related accessories and required mounting infrastructure including civil work for successful operation.
4. Speed violation detection system

5. Pelican Signals
6. Automated e-challan systems
7. Traffic Surveillance Cameras along with related accessories and required mounting infrastructure including civil work for successful operation of the system
8. Public Address Systems for dissemination of critical information.
9. Emergency call box for use of citizens to notify JICCC / public authorities regarding emergent situations.
10. Video Management Server & Video Analytics server
11. Establish Network Connectivity to transfer the data from field devices to the Data Centre and Integrated Command Control Centre (JICCC)
12. Set up Traffic Operations at JICCC with required application platform capability to aggregate incoming data streams onto a single platform, provide traffic flow estimates for near term future on a real time basis and assist in analysing impact of alternate traffic management strategies.
13. IT infrastructure including hardware and software at JICCC and Local DC for the management of the edge devices signals, command centre and the traffic management software platform
14. Develop individual signal control strategies including definition of signal grouping, setting of potential strategies for traffic control under various scenarios, specification of traffic management strategies for planned and unplanned events.
15. Consolidated database of incoming real time data for future analysis and evaluation purposes.

It is envisaged that the proposed adaptive traffic control system will incorporate historic trends for development of traffic management strategies and adaptive control strategies.

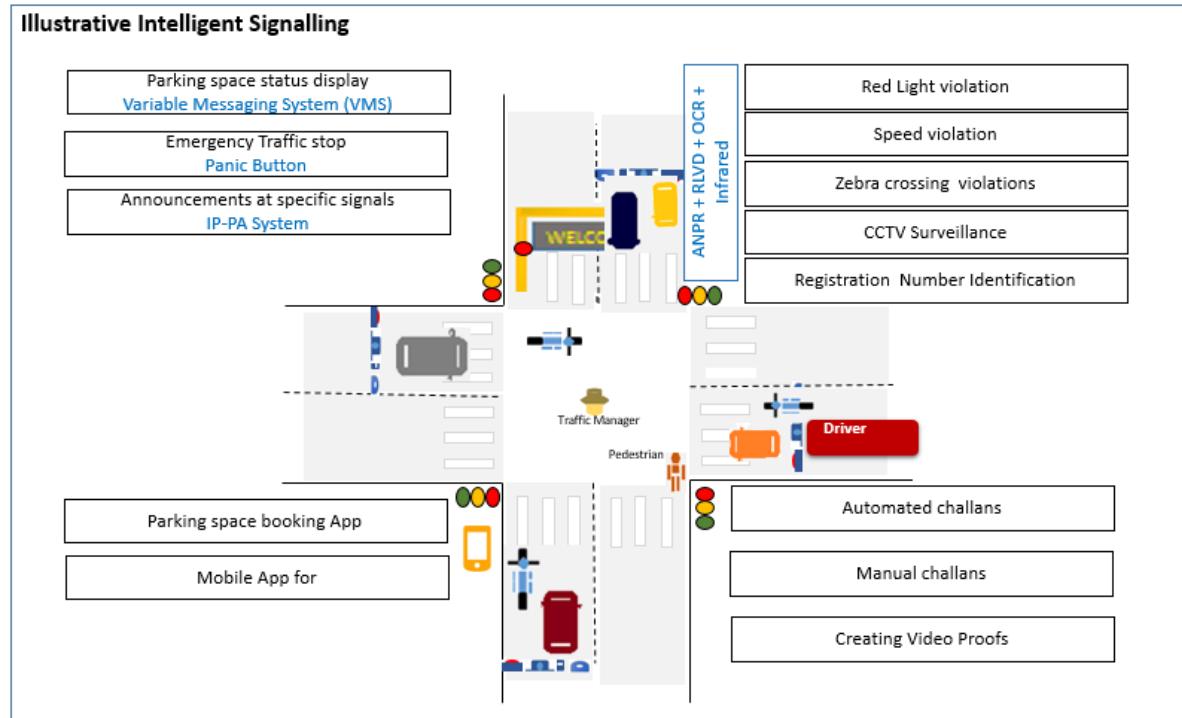


Figure: Illustrative representation of Intelligent Traffic Management System

Existing Systems

Traffic Police has over the last few years, put in a number of traffic signals to help commuters navigate traffic with ease. Traffic Management has 26 Traffic Signal systems at important road intersections across city. Out of which 6 signals are non-functional which should be considered for upgradation as part of the RFP. The detailed list of 26 existing and proposed signals is provided as below:

Sl. No.	Name of the Junction	No of Legs	Traffic Signal Functional
1	T-Point PAP	3	Non-functional
2	BSF Chowk	3	YES
3	Sutlej Cinema Chowk	4	Non-functional
4	BMC Chowk	5	Timer non-functional
5	Guru Nanak Mission Chowk	4	YES
6	Dr. BR Ambedkar Chowk	4	Timer non-functional
7	Football Chowk	4	YES
8	Adarsh Ngr Chowk	4	YES

Sl. No.	Name of the Junction	No of Legs	Traffic Signal Functional
9	Kapurthala Chowk	4	YES
10	Work Shop Chowk	4	YES
11	Maqsudan Chowk	3	YES
12	Pathankot Chowk	4	Timer non-functional
13	Lama Pind Chowk	4	YES
14	Kishan Pura Chowk	4	NO.
15	Gpo Chowk	3	YES
16	PNB Chowk	3	YES
17	Basti adda Chowk	4	YES
18	Patel Chowk	4	YES
19	Ravidass Chowk	4	Non-functional
20	Manbro Chowk	4	YES
21	Chun Mun Chowk	4	YES
22	Samra Chowk	4	YES
23	Geeta Mandir Chowk	4	YES
24	Model Town Mkt. Chowk	3	YES
25	Urban Estate Ph.-2	4	YES
26	T-Point Sodal Mandir	3	YES

Geographical Spread

Competent Authority is the nodal agency for regulating and managing the entire road network and traffic signals in the Jalandhar City. Currently, there are total 26 following kinds of traffic junctions.

Arms	Number of Junctions
3	7
4	18
5	1

The following figure illustrates the junctions, which are functional, non-functional signals, arterial road and VIP road for which ATCS shall be installed. And ATCC shall be installed at two locations at an identified junction during the detailed survey by MSI.

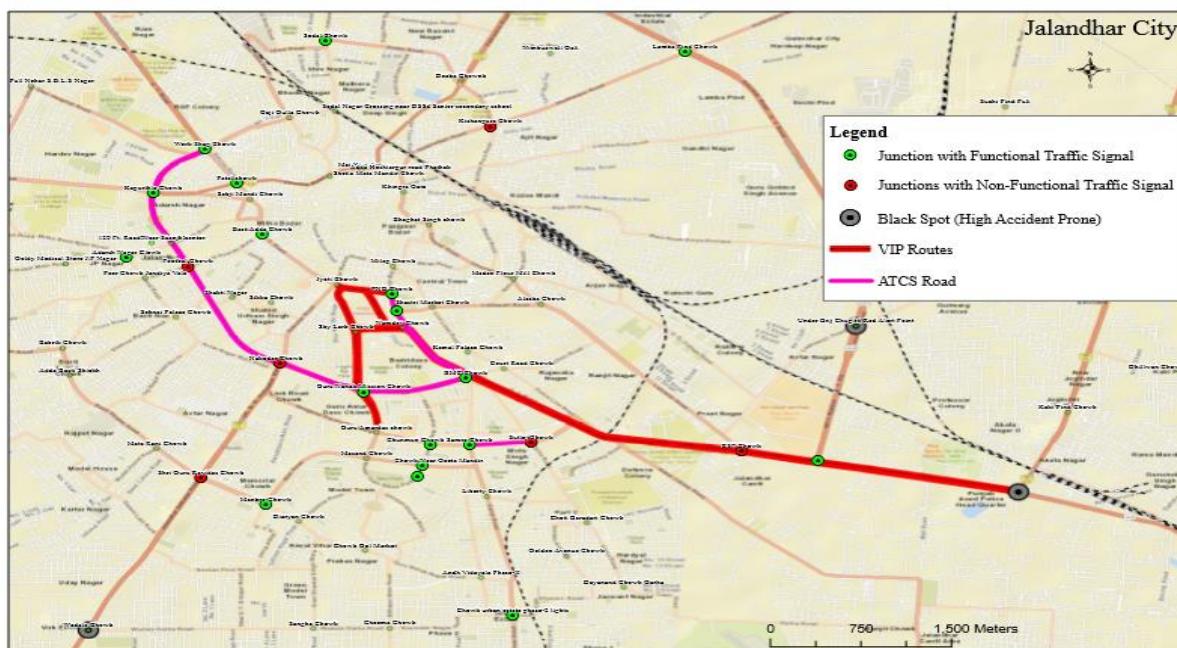


Figure – ATCS road, VIP road, Functional and Non-functional junctions

There shall be Pelican signal installed at one identified locations during detailed survey by MSI.

The component scope

Specifically, the scope of MSI will include the following systems and capabilities linked with Integrated City Management Control Centre:

- Installation of Traffic Light Aspects with all accessories at the selected junctions.
- Adaptive Traffic Control System (ATCS)
- Automated Traffic Counting and Classification (ATCC)
- Red Light Violation Detection (RLVD) system
- Automatic Number Plate Recognition(ANPR)
- Speed violation detection (SVDS)
- Pelican signals
- Emergency call box

- i) E-Challan System
- j) Traffic Surveillance
- k) Real Time Traffic Analytics Platform
- l) PAS system
- m) Variable Message Sign boards
- n) Integration with Vahan and Sarathi databases
- o) Integration with GIS Map
- p) Repair of existing signals should be considered as part of this RFP (like timer were observed)
- q) Existing non-functional signals should also be considered to be upgraded for implementation of ATCS and ATCC
- r) All traffic elements should be branded to showcase as smart city elements
- s) Additional components like timer etc. shall be added as required based on the detailed study
- t) Field equipment maintenance like cleaning and checking the fitments every quarter until O&M period

The scope of work shall include but will not be limited to the following broad areas.

1. **Scoping and Feasibility Study:** Conduct a detailed scoping study and develop a comprehensive project plan, including:
 - Feasibility study for finalization of detailed technical architecture and project plan
 - Development of traffic management plans for individual signal controls and groups of signal controllers along with pre-planned intervention strategies for special scenarios
 - Site surveys to identify need for junction improvement, junction signage, lane markings and other necessary site infrastructure
 - Site Clearance obligations & other relevant permissions.
2. **Field Equipment:** Design, Supply, Installation and Commissioning of following field equipment envisaged in Intelligent traffic management system.:
 - Adaptive Traffic Control System at Signalized traffic junctions
 - Variable Message Signs (detailed out in subsequent section)
 - Red Light Violation Detection system
 - Automatic Number plate recognition

- E-Challan System
 - Emergency call box etc. as mentioned above
3. **Network Connectivity:** Provision of Network Connectivity for ATMS equipment/solution
- Developing necessary connectivity for ATMS
 - Integrating live data streams from other traffic information systems such as real time PCR vans, Solid waste Management trucks/tippers, Variable messaging Systems, parking information systems, etc.
4. **Hardware and Software Infrastructure:** Design, Supply, Installation and Commissioning of IT Infrastructure at JICCC and DC: This shall consist of following activities:
- Basic Site preparation services
 - IT Infrastructure including server, storage, other required hardware, application portfolio, licences
 - Centralized platform for traffic data analytics and signal optimization
 - JICCC infrastructure including operator workstations, video walls, IP phones, joystick controller etc.
 - Establishment of LAN and WAN connectivity at JICCC and DC
 - Application Integration Services & SMS gateway
5. **Capacity Building:** Preparation of operational manuals, training documents and capacity building support, including:
- Preparation and implementation of the Information security policy, including policies on backup and redundancy plan
 - Preparation of revised traffic signal control plans, alternate signal control plans, KPIs for performance monitoring of transport network, dashboards for MIS
 - Training of the city authorities and Traffic Police personnel on operationalization of the system
 - Acceptance testing
 - System and configuration Documents, User Documents

- Setting up Helpdesk Services and provide support to users at Jalandhar traffic police and other associated stakeholder locations in compliance to the defined SLAs.
6. Warranty and Annual Maintenance: provide maintenance services for the software, hardware and other IT infrastructure installed as part of ATMS project for a period of 4 years.

The surveyors shall also finalize the approximate location of foundation for junction box and camera poles. The route for all the underground cable laying shall be finalized during this survey (wherever required). Every detail, finalized during the survey, shall be demarcated on an AutoCAD drawing by the MSI and submitted to JSCL or designated agency and Jalandhar police in the form of a detailed site survey report along with other details for its approval in the specified format. For more details, please refer CCTV surveillance section.

Component Architecture

The schematic diagram below shows the systems envisaged under ATMS & ATCC and the information flow across the systems to be integrated.

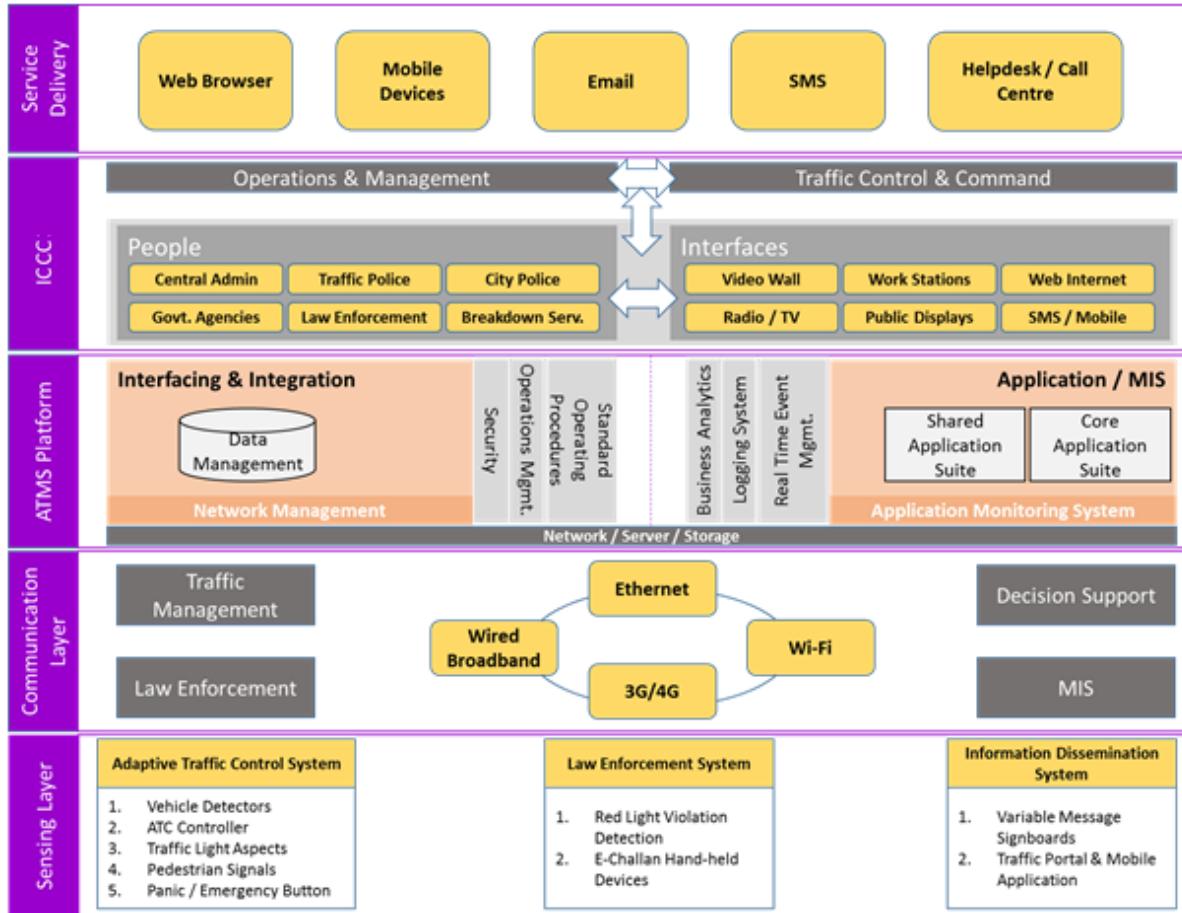


Figure: Logical Architecture of ATMS/ATCC Solution

Solution Requirements

The MSI shall be responsible for Supply, Installation, Implementation and Operation & Maintenance of Jalandhar Surveillance System for a period of 4 Years from the date of Go-Live. The indicative requirement for MSI is broadly categorized into following:

Sl. No.	Parameter	Minimum requirements
1	Min Signalling System Infrastructure at field locations	1. Public Announcement System (PAS), Emergency call box
		2. Supply, Install, Implement and Maintenance of IP based cameras with IR
		a. Fixed box Cameras

		<p>b. PTZ Cameras</p> <p>c. RLVD</p> <p>d. ANPR</p> <p>e. SVDS</p> <p>Additional features for the cameras :</p> <p>Camera to support Adaptive Traffic Control System (ATCS)</p> <p>Camera to support ANPR</p> <p>Camera to support RLVD</p> <p>Camera that support Analytics</p> <p>Sensor/Camera configurations required for (ATCS and ATCC)</p> <p>Note: There is pole and traffic light aspects installation required for traffic signals and cameras as required. The cameras should be installed using appropriate fittings. Installation configuration and maintenance of poles & required power, backup, network connectivity and any other additional hardware and software fittings is in the scope of MSI.</p> <p>Data Retention Period: 2 years</p>
2	Network Infrastructure	<p>1. Between camera & aggregation point – Field location</p> <p>2. Between aggregation points & Data centre</p> <p>3. Between Data Centre & JICCC</p> <p>4. Between Data Centre & viewing/monitoring centre and satellite control centre</p> <p>5. It is envisaged that the MSI will coordinate and take services of the existing Network Providers in Jalandhar like BSNL, Airtel, Railtel etc. However, a tri-party Agreement among Authority, MSI & the Network Service Providers would be signed in order to meet networking requirements as defined within Service Level Agreement.</p>
3	Data Centre	<p>1. Supply & installation of all the requisite ICT Infrastructure including server, storage, network components and peripherals to handle 100% load along with provisioning for redundancy</p> <p>2. Supply & installation of all the requisite Non IT infrastructure like furniture, AC, and interior work etc. excluding the civil work at the space, which will be provided by the Competent Authority.</p>

4	Integrated Command Control Centre	1. Supply & installation of all the IT & Non IT infrastructure such as the Video Wall, Workstation, AC, and interior work, etc. excluding civil work at the space provided by Competent Authority
5	Applications at JICCC	1. Video Management System (VMS)
		2. Video Analytics (VA)
		3. Red Light Violation Detection (RLVD) System
		4. Automatic Number Plate Recognition (ANPR) System
		5. Integration with RTO applications like Vahan / Parivahan to extract details like Owner Name, Address, Age, Engine Number, Chassis Number, vehicle Registration Date,, vehicle Registration City, Type, Model, City ,State
		6. Analyse and implement User specific requirement implementation
		7. ATCS, ATCC central applications and e-challan application
6	Capacity Building	MSI shall provide all Technical & Functional training/capacity building/handholding for the designated officials/staff/personnel on a continuous basis

Field Locations general guidelines

This component covers planning & implementation of the Signalling System comprising cameras and other field equipment at locations identified by Authority. However, actual placement of pole & number of cameras at each location, type of cameras, fixation of height & angle for the cameras to ensure maximum coverage should be undertaken in consultation with Jalandhar Police / Traffic Police.

A detailed survey shall be conducted, by the MSI along with a team from the Authority and Jalandhar Police, at each of the strategic locations. This survey shall finalize the position of all field equipment's and the orientation/ field of view of the cameras. Appropriate field of view snapshot shall be taken by a handheld camera for future reference at the time of survey. The surveyors shall also finalize the approximate location of foundation for junction box and poles. The route for all the underground cable laying shall be finalized during this survey (wherever required). Every detail, finalized during the survey, shall be demarcated on an AutoCAD drawing by the MSI and submitted to Authority in the form of a detailed site survey report along with other details for its approval.

The system shall provide inter-operability of hardware, operating system, software, networking, printing, database connectivity, reporting, and communication protocols. MSI shall prepare the Detailed Report

for field level requirements such as Cameras (types & numbers), Camera Mounting requirements, Power Requirements, Connectivity Requirements etc. for perusal of Authority. Indicative list of the field level hardware to be provided by MSI is as follows:

1. Cameras with IR illuminators (Fixed Box, PTZ, ANPR, RLVD cameras etc.)
2. IR illuminators - External
3. Local processing unit for ANPR / RLVD cameras
4. Switches
5. Outdoor Cabinets
6. Pole for cameras / Mast
7. Outdoor Junction box
8. UPS
9. Networking and power cables, solar panels and other related infrastructure

Supply & Installation of Camera Infrastructure

Based on detailed field survey as mentioned above, MSI shall be required to supply, install and commission the surveillance and monitoring systems at the identified locations and thereafter undertake necessary work towards its testing. MSI shall use industry leading practices during the implementation phase w.r.t positioning and mounting the cameras, poles and junction boxes. Some of the check-points that need to be adhered to by the MSI while installing / commissioning cameras are as follows:

1. Ensure that surveillance and monitoring objective is met while positioning the camera such that the required field of view is being captured as finalized in field survey
2. Ensure that camera is protected from the field challenges of birds, weather, physical damage and theft.
3. Make proper adjustments so as to have the best possible image / video captured.
4. Ensure that the pole is well placed for vibration resistance adhering to the road safety norms.
5. Deployment of Collision preventive barriers around the junction box & pole foundation in case it's installed in collision prone place.
6. Deployment of Appropriate branding or colour coding (Police/Authority Branding) of poles and junction boxes, to warn mischief mongers against tampering with the equipment at the junction.

Installation of Poles/Cantilevers/Gantry if required

1. The MSI shall ensure that all installations are done as per satisfaction of the Authority.
2. For installation of Cameras, Public Address System, Emergency call box etc. MSI shall provide appropriate poles & cantilevers and any supporting equipment.
3. MSI shall be required to supply, install, configure and integrate surveillance cameras at the identified locations and thereafter undertake necessary work towards their commissioning.
4. MSI shall ensure that the poles erected to mount cameras are good, both qualitatively and aesthetically
5. MSI shall use the industry leading practices while positioning and mounting the cameras and ensure that the pole / mast implementation is vibration resistant. Arrangements for bird scare spikes on top of camera shall be made to prevent birds from sitting on top of camera box.
6. The poles shall be installed with base plate, pole door, pole distributor block and cover.
7. Base frames and screws shall be delivered along with poles and installed by the MSI.
8. In case the cameras need to be installed beside or above the signal heads, suitable stainless steel extensions for poles need to be provided and installed by the MSI so that there is clear line of sight.
9. MSI shall be responsible to undertake required structural analysis regarding the regulated load conditions and considering the respective wind load while installing the poles / cantilevers for cameras
10. MSI shall provide structural calculations and drawings for the approval of Authority. The design shall match with common design standards as applicable under the jurisdiction of Authority/authorized entity.
11. MSI shall coordinate with concerned authorities / municipalities for installation.
12. Poles and cabinet shall be so designed such that all elements of the field equipment could be easily installed and removed.
13. MSI shall ensure that physical look of the installation area returns to neat & tidy conditions after installation of poles, cantilevers etc. The placement shall be designed keeping in mind the normal flow of vehicular traffic and pedestrian movement is not disturbed.

UPS for field locations

1. UPS shall serve as a backup for commercially available utility power at the intersections and shall ensure no-break functioning of all field components at each intersection in event of failure of utility power supply

2. MSI shall carry out a study and identify locations to provide UPS backup, depending upon power situation across Jalandhar City, to meet the camera and other field equipment's uptime requirements.
3. MSI shall install UPS at the identified intersections in secure, tamper-proof housing in corrosion resistant cabinets.
4. MSI shall ensure that the UPS is suitably protected against storms, power surges and lightning.
5. MSI shall provide UPS for efficient heat dissipation without air conditioning. It shall be able to withstand temperatures prevalent in Jalandhar throughout the year.

Outdoor Cabinets / Junction Boxes

1. Each intersection shall be fitted with outdoor cabinets dimensioned to host all equipment necessary to operate enforcement systems and traffic surveillance systems as defined in this RFP
2. The cabinets provided shall be plug and play
3. MSI shall reserve additional room in the intersection controller cabinet to accommodate the future system requirements
4. The size of outdoor cabinet / Junction Boxes shall be sufficient to house all the system components, which may be installed at the intersection or nearby. Boxes shall be dustproof and impermeable to splash-water (IP65 or better). They shall be suitable for Jalandhar's environmental conditions. They shall have separate lockable doors for:
 - a. Power cabinet: This cabinet shall house the electricity meter, online UPS system and the redundant power supply system
 - b. Control cabinet: This cabinet shall house the controllers for all the field components at that particular location e.g. ANPR, PTZ, RLVD, Fixed box cameras etc.
5. Internal cabinet cabling shall be designed for an easy connection and disconnection of the equipment and power
6. The cabinets shall be of robust construction and shall include 3-point security-locking mechanisms to prevent unauthorized access to the field equipment
7. **Temperature and Humidity Control:** All enclosure compartments shall be equipped with a natural convection air circulation system via provision of air circulation filters that shall not require maintenance and shall allow free circulation of air inside the enclosures to prevent

overheating as well as the build-up and effects of humidity and heat, without permitting the entry of elements that might endanger system operation

8. MSI shall ensure that all the hardware is placed inside the junction boxes that could withstand temperatures prevalent in Jalandhar throughout the year

Civil and Electrical Works

1. MSI shall be responsible for carrying out all the civil & Electrical work required for setting up all the field components of the system including:
 - a. Preparation of concrete foundation for MS-Poles & cantilevers
 - b. Laying of GI Pipes (B Class) complete with GI fitting
 - c. Hard soil deep digging and backfilling after cabling
 - d. Soft soil deep digging and backfilling after cabling
 - e. Chambers with metal cover at every junction box, pole and at road crossings
 - f. Concrete foundation from the Ground for outdoor racks
2. MSI shall provide power to the cameras through the aggregation point. Since this component has dependency on approval from local authorities, it is recommended that MSI plans this requirement well in advance & submits the application to the concerned electricity distribution agency with requisite fees, as applicable.
3. MSI shall carry out all the electrical work required for powering all the components of the system
4. Electrical installation and wiring shall conform to the electrical codes of India
5. MSI shall make provisions for providing electricity to the cameras (ANPR, PTZ, and Fixed) via Junction Box, housing the UPS/SMPS power supply, with minimum backup as defined in this RFP
6. For the wired Box cameras, MSI shall provision for drawing power through PoE/POE+ (Power over Ethernet), while PTZ cameras shall be powered through dedicated power cable laid separately along with STP/SFTP cable
7. Registration of electrical connections at all field sites shall be done in the name of the Competent Authority.
8. MSI shall house the electricity meters inside the power cabinet as mentioned in the controller Cabinet section as above.

Earthing and Lightning Proof Measures

1. MSI shall comply with all the specified Technical Specifications taking into account lightning-proof and anti-interference measures for system structure, equipment type selection, equipment earthing, power and signal cable laying. MSI shall describe the planned lightning-proof and anti-interference measures in their Technical Bid.
2. Corresponding lightning arrester shall be erected for the entrance cables of power line, video line, data transmission cables
3. All interface board and function board, interfaces of equipment shall adopt high speed photoelectric isolation to reduce the damage to integrated circuit CMOS (Complementary metal–oxide–semiconductor) chip due to the surge suppression
4. Install the earthing devices for the equipment, including lightning earthing, protection earthing and shielded earthing. All earthing shall meet the related industry standards
5. The earthing cable shall be installed in a secure manner to prevent theft and shall be rust proof. Earthing down lead and the earthing electrode shall be galvanized.

Public Address System (PAS)

Public Address System shall be used at the intersections as identified by Authority to make important announcements for the citizens / public. It shall be able to broadcast messages across all PA systems or specific announcement could be made to a particular location supporting single zone / multi zone operations. The system shall also deliver pre-recorded messages to the loud speakers attached to them from CD/DVD Players & Pen drives for public announcements. The system shall contain an IP based amplifier and use PoE/POE+ power that could drive the speakers. The system shall also contain the control software that could be used to control/monitor all the components of the system that includes Controller, Calling Station & keypad, Amplifier (Mixing & Booster).

The MSI shall describe in detail the design, operational and physical requirements of the proposed public announcement system to demonstrate compliance with all the specified requirements of RFP.

Emergency Call Box

Emergency box shall be installed at intersections identified by Authority to improve the safety and security of citizens within the city where they can seek assistance from JICCC's Emergency Response Team. Emergency call box will enable citizens to establish a two-way audio (microphone and speaker) – video (video camera and a video screen) communication link with operation staff at JICCC. On pressing

the emergency button the system will establish a connection with Emergency Response Team call taker and the video shall be displayed on the video wall in the JICCC.

Speed Violation Detection Systems (SVDS)

- a) The speed violation detection system captures speed of the vehicles which are passing through this system. The speed detection system detects speed of the vehicle and compares with the speed limit set in the configuration. If the actual speed of the vehicle is more than the speed limit, then it triggers the ANPR system to capture the number plate of the vehicle. Both the number plate and actual speed of the violated vehicle will be stored in the system. The system detects speed accuracy of 10% (+/-) of the actual vehicle speed.
- b) The number plate deciphered are stored in the deciphered database. The number plate not deciphered by ANPR system are stored in the non-deciphered database. Later the non-deciphered number plate is manually further classified into soiled, broken and vernacular number plate.
- c) All the deciphered number plate of violated vehicles e-Challans generated automatically. Non deciphered number plate of violated vehicles e-Challans are generated manually

Pelican Signals

Pelican Signal (Pedestrian Light Controlled Crossing) shall be a definitive light controlled crossing signal featuring a set of traffic lights (Green Man & Red Man Signal) with a push button, operated by pedestrian and shall also be able to facilitate differently-abled/Senior Citizens for crossing. The controls to operate the light signals shall be on the pedestrian's corner while the light signal for crossing on the other side of the road. Pelican Signal shall be installed at identified locations.

Miscellaneous

1. Competent Authority shall assist in obtaining all necessary go ahead, legal permissions, NOC (No Objection Certificate) from various departments to execute the project. MSI shall have to identify and obtain necessary legal / statutory clearances for erecting the poles and installing cameras, for provisioning of the required power, etc. MSI shall provide & manage all necessary paper work to pursue permission from respective authorities. No commercial/legal fees (except the RoW charges) shall be applicable for obtaining the necessary permissions.

2. The MSI shall provide all material required for mounting of components such as cameras and other field equipment. All mounting devices for installation of CCTV cameras to enable pan and tilt capabilities shall be included in the costs of the respective component. The same is also applicable to crossheads and cross arms, mounting brackets, stainless steel bands, screws and other accessories.
3. All the equipment, Hardware, Software and workmanship which form a part of the MSI services will be under O&M to be undertaken by the MSI throughout the contract period.
4. MSI shall also get comprehensive insurance from reputed insurance company for the project duration for all the equipment's/components installed under this project.
5. MSI shall ensure all the equipment's installed in the outdoor locations are vandal proof and in case the equipment get damaged /stolen for reasons whatsoever, it shall repair/replace the same in the specified time as per SLAs at no extra cost to the Competent Authority. All such costs shall be factored in the comprehensive insurance of field equipment for the duration of the contract.
6. Preventive maintenance shall be carried out once in a quarter along with corrective maintenance and also when calls are placed by Competent Authority or its designated agency. A report has to be maintained and submitted to Authority.
7. In addition to above, the MSI shall be fully responsible for all maintenance activities for the period between installation of equipment and roll-out of the system.
8. During implementation, if observed that any camera / field equipment requires change in the field of view / orientation, it shall be done by MSI without any extra cost.
9. In case of request for change in location of field equipment post installation, the same shall be borne by Competent Authority at either a unit rate as per commercials or a mutually agreed cost.

10. It is assumed that the existing signal infrastructure like poles etc shall be reused and electronic components shall be replaced for which warranty is applicable in Operations and Maintenance period.

Functional Requirements:

Sl. No.	Parameter	Minimum Specifications
1	General	<ul style="list-style-type: none"> ▪ The specifications mentioned for various IT / Non-IT components are indicative requirements and should be treated for benchmarking purpose only. ▪ All IT Components should support IPv4 and IPv6 ▪ The user interface of the system should be a user friendly Graphical User Interface (GUI). ▪ Critical core components of the system should not have any requirements to have proprietary platforms and should conform to open standards. ▪ For custom made modules, industry standards and norms should be adhered to for coding during application development to ensure debugging and maintenance is easier. Object oriented programming methodology must be followed to facilitate sharing, componentizing and re-use of standard code. Before hosting the application, it shall be subjected to application security audit (by any of the CERTIN empanelled vendors) to ensure that the application is free from any vulnerability; and approved by the Authority. ▪ All the Authority's Machines / Servers shall support static assigned IP addresses or shall obtain IP addresses from a DNS/DHCP server. ▪ Cameras and the Video Management / Video Analytics Software should be ONVIF Core Specification '2.X' or 'S' compliant and provide support for ONVIF profiles such as Streaming, Storage, Recording, Playback, and Access Control.
2	Traffic Signal Controller	<ul style="list-style-type: none"> ▪ The Traffic Signal Controller equipment is a 32 bit or 64-bit microcontroller with solid state traffic signal lamp switching module with the ability to program any combination of traffic signal stages, phases and junction groups. The controller will ideally have a conflict

Sl. No.	Parameter	Minimum Specifications
		<p>monitoring facility to ensure that conflicting, dangerous are pre-flagged at the programming stage and these are disallowed even during manual override phase.</p> <ul style="list-style-type: none"> ▪ The Traffic Signal Controller will be adaptive so that it can be controlled through the central traffic control centre as an individual junction or as part of group of traffic junctions along a corridor or a region. The signal controller design must be flexible for the junction could be easily configured to be part of any corridor or group definition and could be changed through central command controller easily. ▪ Site specific configuration data shall be stored in a non-volatile memory device (FLASH memory) easily programmable at the site through keypad or laptop. A minimum of 512KB flash memory and 128KB RAM shall be provided. Volatile memory shall not be used for storing the junction specific plans or signal timings. ▪ All timings generated within a traffic signal controller shall be digitally derived from a crystal clock which shall be accurate to plus or minus 100 milliseconds. ▪ The controller shall provide a real time clock (RTC) with battery backup that set and update the time, date and day of the week from the GPS. The RTC shall have minimum of 10 years' battery backup with maximum time tolerance of 10 secs per day. ▪ The controller shall have the facility to update the RTC time from ATCS server, GPS and through manual entry. ▪ The controller shall be capable of communicating with the ATCS server through Ethernet on a managed leased line network or any other appropriate stable communication network <p>A) Police Panel:</p> <p>The controller shall provide the following facilities in a separate panel with provision for lock and key arrangements for use by the Traffic Police.</p>

Sl. No.	Parameter	Minimum Specifications
		<ul style="list-style-type: none"> ▪ Four Hurry Call switches: The Hurry Call mode will provide the means to force the controller to a defined stage, without violating safety clearances. A pre-emption input may be used to demand the Hurry Call mode to give right of way to emergency vehicles. It should be possible to configure the Hurry Call switches to any stage as per site requirements. ▪ One Forced Flash Switch: Activation of this switch should force the signal to Flashing Amber / Flashing Red. ▪ One Auto / Manual Switch: Activation of this switch should enable manual operation of the controller. Deactivation of the manual switch shall continue from the current stage without interruption. ▪ One Manual Advance Pushbutton Switch: In manual operation mode, the stages appear in the sequence specified in the signal plan timetable. Activating the pushbutton switch shall terminate the currently running stage and start the next, without violating safety clearances. ▪ One Junction OFF Switch: Activating this switch should put OFF all signal lamps. On deactivation of the switch the traffic signal controller shall resume its normal operation without violating any safety clearances.

B) Modes of Operation:

The traffic signal controller shall have the following modes of operation:

- **Fixed Time:** In fixed time (pre-timed) mode the traffic signal controller shall execute stage timings according to the site specific timetable maintained in the traffic signal controller FLASH memory. Inputs from vehicle detectors shall be ignored in this mode and no pre-emption shall be made on any stage. Cycle time remains constant in every cycle execution for a given time period.
- **Vehicle Actuation with All Stages Pre-emption:** In the vehicle actuation with all stages pre-emption mode, the traffic signal controller shall execute stage timings as per demand from vehicle detectors within the constraints of minimum Green, Maximum Green

Sl. No.	Parameter	Minimum Specifications
		<p>running period for the stage and Cycle time stored in the traffic signal controller FLASH memory. Pre-emption shall be possible for all demand actuated stages. Cycle time may vary in every cycle execution.</p> <ul style="list-style-type: none"> ▪ Semi-Actuation: In the semi-actuation mode, the traffic signal controller shall execute stage timings in the vehicle actuated stages as per demand from vehicle detectors within the constraints of minimum Green, Maximum Green running period for the stage and Cycle time stored in the traffic signal controller FLASH memory. All other stages shall execute the Maximum green time configured for the stage. Pre-emption shall be possible for all demand actuated stages. Cycle time may vary in every cycle execution. ▪ Stage Skipping: The traffic signal controller shall not execute the stage enabled for skipping when there is no vehicle demand registered for the stage till clearance amber time of the previous stage. ▪ Vehicle Actuation with Fixed Cycle length: In vehicle actuation with fixed cycle length mode, the traffic signal controller shall execute stage timings as per demand from vehicle detectors within the constraints of minimum Green, Maximum Green running period for the stage and Cycle time shall be maintained constant during a given timeslot. Pre-emption to be carried out for all demand actuated stages except for Priority Stage. ▪ Full ATCS (FATCS): In FATCS mode, the traffic signal controller shall execute stage timings as per demand within the constraints of minimum Green, Maximum Green running period for the stage and Cycle time specified by the Central Computer during every cycle switching. Pre-emption for all demand actuated stages except Priority Stage shall be possible in this mode. The traffic signal controller shall identify a communication failure with the central computer within a specified time period. In such an event the signal plan timings shall be executed from the local timetable stored in the traffic signal controller FLASH memory. Fall-back mode of the traffic signal controller shall be vehicle actuated. On restoration of the communication with central computer the traffic signal controller shall automatically resort to

Sl. No.	Parameter	Minimum Specifications
		<p>FATCS mode.</p> <p>The traffic signal controller shall accept commands for remote selection / de-selection of the following from the Central Computer at JICCC.</p> <ul style="list-style-type: none"> ○ Hurry Call ○ Flashing Amber / Flashing Red ○ Junction Off <p>If not reverted to the normal operation within the time period listed below, the traffic signal controllers shall timeout the commands and operate normally:</p> <ul style="list-style-type: none"> ○ Hurry Call – 5 Minutes ○ Flashing Amber / Flashing Red – 30 Minutes ○ Junction Off – 30 Minutes <p>The traffic signal controller shall report the following to the Central Computer through the communication network every cycle or on an event as appropriate.</p> <p>Green time actually exercised for each approach (stage pre-emption timing) against the Green running period set for the approach by the Central Computer.</p> <p>Mode of Operation</p> <ul style="list-style-type: none"> ▪ Lamp failure, if any ▪ Output short circuit, if any ▪ Detector failure, if any <p>C) Traffic Signal Controller Operating Parameters</p> <p>Phases - The controller shall have facility to configure 32 Phases either for vehicular movement, filter green, indicative green, pedestrian movement or a combination thereof.</p> <ul style="list-style-type: none"> ▪ It shall be possible to operate the filter green (turning right signal) along with a vehicular phase. The filter green signal shall flash for a time period equal to the clearance amber period at timeout when operated with a vehicular phase. ▪ The pedestrian phase signal shall be configured for flashing red or flashing green aspect during pedestrian clearance.

Sl. No.	Parameter	Minimum Specifications
		<ul style="list-style-type: none"> ▪ It shall be possible to configure any phase to the given lamp numbers at the site. ▪ Stages – The controller shall have facility to configure 32 Stages. ▪ Cycle Plans – The controller shall have facility to configure 24 Cycle Plans and the Amber Flashing / Red Flashing plan. It shall be possible to define different stage switching sequences in different cycle plans. The controller shall have the capability for a minimum of 32 cycle-switching per day in fixed mode of operation. ▪ Day Plans – The controller shall have facility to configure each day of the week with different day plans. It shall also be possible to set any of the day plans to any day of the week. The controller shall have the capability to configure 20 day plans. ▪ Special Day Plans – The controller shall have facility to configure a minimum of 20 days as special days in a calendar year ▪ Starting Amber – During power up the controller shall initially execute the Flashing Amber / Flashing Red plan for a time period of 3 Seconds to 10 Seconds. The default value of this Starting Amber is 5 Seconds. Facility shall be available to configure the time period of Starting Amber within the given limits at the site. ▪ Inter-green – Normally the inter-green period formed by the clearance Amber and Red extension period will be common for all stages. However, the controller shall have a facility to program individual inter-green period from 3 Seconds to 10 Seconds. ▪ minimum Green – The controller shall allow programming the minimum Green period from 5 Seconds to 10 Seconds without violating the safety clearances. ▪ It should not be possible to pre-empt the minimum Green once the stage start commencing execution. ▪ All Red – Immediately after the Starting Amber all the approaches should be given red signal for a few seconds before allowing any right of way, as a safety measure. The controller shall have programmability of 3 Seconds to 10 Seconds for All Red signal.

Sl. No.	Parameter	Minimum Specifications
		<ul style="list-style-type: none"> ▪ Signal lamps monitoring – The controller shall have inbuilt circuitry to monitor the lamp status. ▪ Green – Green Conflict Monitoring – The controller shall have a facility to list all conflicting phases at an intersection. The controller should not allow programming of these conflicting phases in a Stage. A hardware failure leading to a conflict condition (due to faulty devices or short circuit in the output) shall force the signal into Flashing Amber/ Flashing Red. ▪ Cable less Synchronization – It shall be possible to synchronize the traffic signal controllers installed in a corridor in the following modes of operation, without physically linking them and without communication network. GPS enabled RTC shall be the reference for the cable less synchronization. ▪ Fixed Time mode with fixed offsets. ▪ Vehicle Actuated mode with fixed offsets. <p>D) Input and Output facilities</p> <ul style="list-style-type: none"> ▪ Lamp Switching: The controller shall have minimum 64 individual output for signal lamp switching, configurable from 16 to 32 lamp groups where in each group is RED, AMBER & GREEN. The signal lamps may be operating on appropriate DC/AC voltage of applicable rating. ▪ Detector Interface: A minimum of 16 vehicle detector inputs shall be available in the controller. All detector inputs shall be optically isolated and provided with LED indication for detection of vehicle. ▪ Communication Interface: The traffic signal controller shall support Ethernet interface to communicate with the ATCS server. ▪ Power Saving: Bidders are requested to propose appropriate energy saving mechanisms and approaches. The traffic signal controller shall have a facility to regulate the intensity of signal lamps during different ambient light conditions. ▪ Real-time Clock (RTC): The GPS receiver for updating time, date and

Sl. No.	Parameter	Minimum Specifications
		<p>day of the week information of the traffic signal controller should be an integral part of the traffic signal controller.</p> <ul style="list-style-type: none"> ▪ The traffic signal controller shall update the date, time and day of the week automatically from GPS during power ON and at scheduled intervals. ▪ Manual entry for date, time and day of week shall be provisioned for setting the traffic signal controller RTC (Real Time Clock). ▪ It shall be possible to set the RTC from the Central Server when networked. ▪ Keypad (optional): The traffic signal controller shall have a custom made keypad or should have provision for plan upload and download using PC/laptop/Central Server. ▪ Operator Display (optional): The traffic signal controller shall optionally have a LED backlit Liquid Crystal Display (LCD) as the operator interface.
3	Vehicle Detectors	<ul style="list-style-type: none"> ▪ Solution / product should be able to count vehicles at each arm of the traffic junctions. The outputs of the detectors shall indicate the presence of vehicles and shall be used to influence the operation of the traffic signal controller and shall generate counts, demands and extensions for right-of-way. Means shall be provided so that a detector may be connected to demand and / or extend a phase movement as specified. ▪ Specific placement of the detectors (upstream, downstream, stop line, exit etc.) for independent straight and right turn signals. ▪ The detector shall be able to count vehicles in non-lane based mixed traffic flow conditions and differentiate between different vehicle types (two-wheeler, three-wheeler, car, HGV, etc.). The accuracy of counts shall be bigger than 90% over all light and weather conditions. ▪ A detector that does not change its status at least once during a stage execution shall be notified to the Central Computer (in ATCS mode) at the termination of the associated stage.
4	Communication	<ul style="list-style-type: none"> ▪ Function of the Communication network is for remote monitoring of

Sl. No.	Parameter	Minimum Specifications
	Network	the intersection and its management. Real time data (like RTC time, stage timing, mode, events, etc.) from the traffic signal controller is required to be sent to the Central Computer in Traffic Management Centre. Central Computer running the ATCS application shall calculate and send optimum signal timings to all intersections in the corridor.
5	ATCS Application software	<p>Objective of the ATCS is to minimize the stops and delays in a road network to decrease the travel time with the help of state-of-the-art technology. The adaptive traffic control system will provide simulation based traffic flow modelling capability with the capacity to calculate traffic flows, OD movements, and queues and turning movement along entire primary road transport network in the defined study area covering the ATCS junctions and beyond. The Application software or platform will be able to predict traffic flow in the network for the near term over various interval horizons (e.g. T+5, T+10 ... T+30 mins). The ATCS application will provide estimated traffic flow for each of the junction to calculate optimal cycle times, effective green time ratios, and change intervals for all system traffic signal controllers connected to it either as individual junctions or groups of junctions. These calculations will be based up on assessments carried out by the ATCS application software running on a Central Computer based on the data and information gathered by vehicle detectors at strategic locations at the intersections controlled by the system. The ATCS application software shall be divided into two modules with the following as the expected capabilities of the individual modules:</p> <p>Module 1: Real Time Traffic Prediction Capability</p> <ul style="list-style-type: none"> ▪ Shall provide a decision support tool for assessing strategies to minimize congestion, delays and emergency response time to events via simulation and planning tools linked with real time traffic data fusion and control of traffic Signaling infrastructure on ground. ▪ Shall collect continuously information about current observed traffic conditions from a variety of data sources (like Bus GPS data, parking

Sl. No.	Parameter	Minimum Specifications
		<p>data, mobile phone data etc. Bidders can propose alternate data sources that could be integrated) and of different kind (traffic states, signal states, vehicle trajectories, incidents, road works etc.)</p> <ul style="list-style-type: none"> ▪ Shall infer a coherent and comprehensive observed traffic state (speeds, vehicular densities, and presence of queues) on all network elements, from above mentioned observations, including vehicle trajectories, through a number of map matching, data validation, harmonization and fusion processes. ▪ Shall have a Graphical User Interface (GUI) to be able to display traffic state along the observed and unobserved parts of the network through GIS maps. The bidder is expected to create a layer of edge equipment within that GIS platform and integrate with ATMS modules) of the transport network and must be able to display traffic flow, building of queues, delays, location of traffic signals and junctions, key Points of Interests (POI), Variable Message signs etc. In addition, the GUI must be: <ul style="list-style-type: none"> ✓ Flexible for the operators to zoom and navigate with ability to interact with objects on the map. ✓ Should be interoperable across multiple platforms and key graphical results and MIS must be made available across the Web ✓ Graphically present time-space diagram for selected corridors on desktop ✓ Graphically present signal plan execution and traffic flow at the intersection on desktop ▪ Shall have the ability to predict, forecast and estimate the traffic pattern across the signals over the near term future (e.g. T+5, T+10, T+15, T+30 mins ... T + 1 hour) ▪ Shall extrapolate the measurements made on a limited number of junctions and arms along the rest of the unmonitored network, and obtain an estimation of the traffic state of the complete network and the evolution of this traffic state over the near term future (e.g. T+5, T+10, T+15, T+30 mins ... T + 1 hour)

Sl. No.	Parameter	Minimum Specifications
		<ul style="list-style-type: none"> ▪ Shall be able to forecast the traffic state with respect to current incidents and traffic management strategies (e.g. traffic signal control or variable message signs), improving the decision making capabilities of the operators even before problems occur ▪ Shall provide customizable estimates of Key Performance Indicators (KPI) for alternate traffic management strategies to quickly assess the results ▪ Shall provide calculated traffic flows estimation and forecast, queues and delays to Urban Control and Adaptive Traffic Control Systems, allowing for proactive Traffic Management and Control. ▪ To raise alerts to the operator that trigger on customizable conditions in the network (starting with simple drops in flow, up to total queue lengths along emission sensitive roads surpassing a definable threshold); To distribute both collected and calculated traffic information via a variety of communication protocols and channels, ensuring high interoperability degree and thus acting as a “traffic data and information hub. ▪ Shall include a traffic data warehouse (for minimum 4 years) for all historic traffic information gathered from the hardware installed on the road network. Bidder to propose how data storage requirements could be minimized using consolidation techniques. ▪ Shall operate in real time that is continuously updating the estimates on the state of the network and the travel times on the basis of data collected continuously over time. ▪ Shall operate the traffic lights with the adaptive traffic controls, based on the current and ▪ Forecasted traffic demand and the current incidents, thus optimizing the green waves continuously throughout the network ▪ Shall be possible to interface the ATCS with a popular microscopic traffic flow simulation software for pre and post implementation analysis and study of the proposed ATCS control strategy.

Sl. No.	Parameter	Minimum Specifications
		<p>Module 2: Adaptive Traffic Control System</p> <ul style="list-style-type: none"> ▪ To operate the traffic lights with the adaptive traffic controls, based on the current and forecasted traffic demand from the above Real Time Traffic Prediction Tool including the current incidents, thus optimizing the green waves continuously throughout the network. ▪ Enable a smart public transport priority respecting the delays for all road users at once with the adaptive signal controller. To have the capability to integrate with Bus GPS data to identify oncoming buses at the junction and be able to provide priority clearance of buses. ▪ Identify the critical junction (Master Junction) for each of the defined corridor or a region based on maximum traffic demand and saturation. ▪ The critical junction cycle time estimated shall be used as the group cycle time i.e. cycle time common to all intersection in that corridor or region. ▪ Stage optimization to the best level of service shall be carried out based on the traffic demand. ▪ Cycle optimization shall be carried out by increasing or decreasing the common corridor cycle time based on the traffic demand within the constraints of minimum and Maximum designed value of cycle time. ▪ Offset correction shall be carried out to minimize number of stops and delays along the corridor for the priority route and for the adjoining road network at once. Offset deviation shall be calculated with a traffic flow model based on the distance, traffic demand and speed between successive intersections and be corrected within 5 Minutes maximum. ▪ The system shall have provision to configure priority for upstream signals as default. The ATCS software shall continuously check the traffic demand for upstream and downstream traffic and automatically assign the priority route to the higher demand direction. ▪ The system shall use optimization algorithms that minimize a function based on the delays, number of stops and queue lengths simultaneously, using a traffic flow model, thus providing a true

Sl. No.	Parameter	Minimum Specifications
		<p>optimum for all road users.</p> <ul style="list-style-type: none"> ▪ Develop appropriate stage timing plans for each approach of every intersection under the ATCS, based on real time demand and the predicted traffic flow values from the traffic flow model. ▪ Propose timing plans to every intersection under the ATCS at least every five minutes. ▪ Calculate the current queue lengths for each approach that has detection cycle-by-cycle based on the succession of time gaps between cars. ▪ Adjust the proposed timing plans second-by-second according to the current and past detector states and the current queue lengths for every intersection under detection. ▪ Enable transit signal priority with minimize disruption of car traffic, dependent on predefined weights for public transport vehicles in comparison to individual traffic. In order to decrease the workload for operation and maintenance, each supply item (road network, lanes, signals and detectors) shall be supplied just once, so that the all macro and microscopic traffic models and the microscopic traffic flow software used for calibration and verification of the ATCS share the same supply. ▪ Shall provide calculated traffic flows estimation and forecast, queues and delays to Urban Control and Adaptive Signal Control Systems, allowing for proactive Traffic Management and Control. Such estimation will be updated at least every 5 minutes or less, and will not be based on a machine learning approach that would not provide enough flexibility in case of unexpected events. ▪ Should be able to route emergency vehicles to minimize the impact of events on the travel time of emergency vehicles. ▪ Shall be able to export the calculated traffic flow data continually to a multi-modal journey-planner that allows all internet users in the city to find the best route with each traffic mode based on the current travel times in the network.

Sl. No.	Parameter	Minimum Specifications
		<ul style="list-style-type: none"> ▪ Identify Priority routes and synchronize traffic in the Priority routes. ▪ Manage and maintain communication with traffic signal controllers under ATCS. ▪ Maintain database for time plan execution and system performance. ▪ Maintain error logs and system logs. ▪ Generate Reports on request: - The ATCS shall generate standard and custom reports for planning and analysis. <p>Reports</p> <p>System shall generate Corridor based and Intersection based reports. The application software shall generate the following reports, but not limited to the below. All the reports shall be possible for selected dates.</p> <ul style="list-style-type: none"> ▪ Intersection based reports ▪ Stage Timing report – The report shall give details of time at which every stage change has taken place. The report shall show the stage sequence, stage timings and stage saturation of all stages of all cycles for a day. The saturation is defined as the ratio between the available stage timings to the actual stage timing executed by the traffic signal controller for the stage (stage pre-emption time). ▪ Cycle Timing report – The report shall give details of time at which every cycle has taken place. The report shall show the cycle sequence and cycle timings for all the cycles in a day. ▪ Stage switching report – The report shall give details of time at which a stage switching has taken place. The report shall show the stage sequence, stage timings and stage saturation for a day. ▪ Cycle Time switching report – The report shall give details of time at which a cycle switching has taken place. The report shall show the cycle sequence and cycle timings for the cycle in a day. ▪ Mode switching report – The report shall give details of the mode switching taken place on a day. ▪ Event Report - The report shall show events generated by the controller with date and time of event.

Sl. No.	Parameter	Minimum Specifications
		<ul style="list-style-type: none"> ▪ Power on & down: The report shall show time when the master is switched on, and last working time of the master controller. ▪ Intensity Change – The report shall show the brightness of the signal lamp is changed according to the light intensity either manually through keypad or automatically by LDR with time stamp. ▪ Plan Change – The report shall show the time of change of plan either through keypad or remotely through a PC or Server. ▪ RTC Failure – The report shall show the time when RTC battery level goes below the threshold value. ▪ Time Update – The report shall show the time when the Master controller updated its time either manually through keypad, automatically by GPS or through remote server. ▪ Mode Change – The report shall show the time when Master controller's operating mode is changed either manually through keypad or a remote server. The typical modes are FIXED, FULL VA SPLIT, FULL VA CYCLE, FLASH, LAMP OFF and HURRY CALL. ▪ Lamp Status Report – The report shall show lamp failure report with date and time of failure, color of the lamp and associated phase. ▪ Loop Failure Report – The report shall show the date and time of detector failure with detector number and associated phase. ▪ Conflict – The report shall show the conflict between lamps (RED, AMBER, GREEN) in the same phase or conflict between lamps with other phase. ▪ Corridor Performance Report – The report shall show the saturation of all the intersections in a corridor for every cycle executed for the corridor and the average corridor saturation for a day. ▪ Corridor Cycle Time Report – The report shall show the Corridor cycle time, Intersection cycle time, Mode of operation and degree of saturation of all the intersections in a corridor for every cycle for a day <p>Graphical User Interface</p>

Sl. No.	Parameter	Minimum Specifications
		<p>The application software shall have the following Graphical User Interface (GUI) for user friendliness, which will have the following functionalities in additions to those described above.</p> <ul style="list-style-type: none"> ▪ User login – Operator authentication shall be verified at this screen with login name and password ▪ Network Status Display – This online display shall indicate with appropriate color coding on site map whether an intersection under the ATCS is online or off. On double clicking the intersection a link shall be activated for the traffic flow display for the intersection. ▪ Traffic Flow Display – This online display shall indicate the current traffic flow with animated arrows, mode of operation, stage number being executed and elapsed stage time. ▪ Saturation Snapshot – This display shall show the current saturation levels of all intersections in a corridor. ▪ Reports Printing / Viewing – This link shall allow selection, viewing and printing of different reports available under ATCS ▪ Time-Space Diagram – The time-space diagram shall display the current stages being executed at every intersection in a corridor with immediate previous history. ▪ Junctions shall be plotted proportional to their distance on Y-axis and time elapsed for the stage in seconds on X-axis. ▪ Junction names shall be identified with each plot. ▪ Facility shall be available to plot the time-space diagram from history ▪ Currently running stage and completed stages shall be identified with different colors. ▪ Stages identified for synchronization shall be shown in a different color. ▪ Speed lines shall be plotter for stages identified for synchronization to the nearest intersection in both directions. ▪ It should be possible to freeze and resume online plotting of Time-Space diagram. ▪ The system shall have other graphical interfaces for configuring the

Sl. No.	Parameter	Minimum Specifications
		ATCS, as appropriate
6	ATCC	<ul style="list-style-type: none"> ▪ Central software application should be a browser-based software application that allows authorised operators and other users to perform all Traffic Management related and other functions. ▪ The system integrates key operational functions such as event entry, addressing, sign control, traffic data, travel times and reporting in one simple solution that allows users to identify and respond to incidents on the city network. ▪ Central Application GUI shall allow authorized users of the software to access the system without the need for any client side software ▪ Application GUI should allow each user to open multiple instances. ▪ All active sensors shall be plotted on a map in central application. ▪ Map should provide mouse-click functionality on icons, graphics and map areas to access to additional information on any map and user feature ▪ Uploaded data should not be deleted from individual field devices/systems until the central system has provided confirmation that the data files have been successfully received. ▪ Central application should have Standard Operation Procedures feature in which the system shall generate an automated Plan for every event generated in the system ▪ Central application should be able to update its date and time applying time synchronization to servers using the internet and using this to in turn update the date and time on all system devices and workstations. ▪ All active equipment shall have an internally maintained date and time clock synchronized at a time interval via the communications controller with the Central System date and time clock. ▪ If the data connection to the central system is temporarily lost, all equipment shall seamlessly switch to an offline mode in which all data is temporarily stored in internal memory and transmitted to the central system as soon as the data connection is re-established. ▪ It should be possible to “future-date” challan value so that they can be

Sl. No.	Parameter	Minimum Specifications
		<p>uploaded ahead-of-time and automatically activated at the planned date and time.</p> <ul style="list-style-type: none"> ▪ The reports should be non-editable. ▪ All sub-systems and devices shall only allow access to authorized user group. ▪ For all data transactions, the system security shall include authentication features to verify that all claimed source, recipient or user identities are correct and valid. ▪ Central software application shall be an industry standard application
7	Red Light Violation Detection Systems (RLVD)	<p>General</p> <p>The following Traffic violations to be automatically detected by the system by using appropriate Non-Intrusive sensors technology:</p> <ul style="list-style-type: none"> ▪ Red Light Violation ▪ Stop Line Violation ▪ The system should be capable of capturing multiple infracting vehicles simultaneously in different lanes on each arm at any point of time with relevant infraction data like: ▪ Type of Violation ▪ Date, time, Site Name and Location of the Infraction ▪ Registration Number of the vehicle through ANPR Camera system for each vehicle identified for infraction. ▪ The system should be equipped with a camera system to record a digitized image and video of the violation, covering the violating vehicle with its surrounding and current state of signal (Red/Green/Amber) by which the system should clearly show nature of violation and proof thereof: ▪ When it violates the stop line. ▪ When it violates the red signal. ▪ Besides, a closer view indicating readable registration number plate patch of the violating vehicle for court evidence for each violation ▪ The system shall be able to detect all vehicles infracting simultaneously in each lane/ arm at the junction as per locations provided. It should

Sl. No.	Parameter	Minimum Specifications
		<p>also be able to detect the vehicles infracting serially one after another in the same lane. The vehicles should be clearly identifiable and demarcated in the image produced by the camera system.</p> <ul style="list-style-type: none"> ▪ The Evidence image produced by the system should be wide enough to give the exact position of the infracting vehicles with respect to the stop line and clearly indicate color of the Traffic light at the instant of Infraction even if any other means is being used to report the color of the light. ▪ The system should interface with the traffic controller to validate the color of the traffic signal reported at the time of Infraction so as to give correct inputs of the signal cycle. ▪ The Evidence and ANPR camera should continuously record all footage in its field of view to be stored at the local base station. This should be extractable onto a portable device as and when required. The option of live viewing of evidence cameras from the locations shall be available at the JICCC. The network should have the capability to provide the real time feed of the evidence camera to the JICCC at the best resolution possible on the available network ▪ The system shall be equipped with IR Illuminator to ensure clear images including illumination of the Number Plate and capture the violation image under low light conditions and night time. <p>Recording & display information archive medium</p> <ul style="list-style-type: none"> ▪ The recording and display of information should be detailed on the snapshot of the infracting vehicle as follows: <ul style="list-style-type: none"> ○ Computer generated unique ID of each violation ○ Date (DD/MM/YYYY) ○ Time (HH:MM: SS) ○ Equipment ID ○ Location ID ○ Carriageway or direction of violating vehicle ○ Type of Violation (Signal/Stop Line)

Sl. No.	Parameter	Minimum Specifications
		<ul style="list-style-type: none"> ○ Lane Number of violating vehicle ○ Time into Red/Green/Amber ○ Registration Number of violating vehicle ▪ The size of file chunks that a camera should send to JICCC should be configurable <p>On site-out station processing unit communication & Electrical Interface</p> <ul style="list-style-type: none"> ▪ The system should automatically reset in the event of a program hang up and restart on a button press. However, the system should start automatically after power failure. ▪ The system should have secure access mechanism for validation of authorized personnel. ▪ Deletion or addition and transfer of data should only be permitted to authorized users. ▪ A log of all user activities should be maintained in the system. ▪ Roles and Rights of users should be defined in the system as per the requirements of the Authority ▪ All formats of the stored data with respect to the infractions should be Non Proprietary ▪ The communication between the on-site outstation processing unit housed in the junction box and the detection systems mounted on the cantilever shall be through appropriate secured technology. ▪ The system should have the capability to transfer the data to SP's Office through proper encryption in real time and batch mode for verification of the infraction and processing of challan. Call forwarding architecture shall be followed to avoid any data loss during transfer ▪ In the event that the connectivity to the SP's Office is not established due to network/connectivity failures, then all data pertaining to the infraction shall be stored on site and will be transferred once the connectivity is re-established automatically. There shall also be a

Sl. No.	Parameter	Minimum Specifications
		<p>facility of physical transfer of data on portable device whenever required. There should be a provision to store minimum one week of data at each site on a 24x7 basis.</p> <p>Mounting Structure</p> <ul style="list-style-type: none"> ▪ Should be cantilever mounted and shall have minimum 6 Mtrs. height with appropriate vertical clearance under the system from the Road surface to ensure no obstruction to vehicular traffic. ▪ It should be capable to withstand high wind speeds and for structural safety, the successful bidder has to provide structural safety certificate from qualified structural engineers approved/ certified by Govt. Agency. ▪ It shall be painted with one coat of primer and two coats of PU paint. The equipment including poles, mountings should have an aesthetic feel keeping in mind the standards road Infrastructure (e.g. Poles, Navigation boards etc.) currently installed at these locations. The equipment should look “one” with the surroundings of the location and not look out of place. ▪ Rugged locking mechanism should be provided for the onsite enclosures and cabinets. <p>RLVD - ANPR Application</p> <ul style="list-style-type: none"> ▪ It should be capable of importing violation data for storage in database server which should also be available to the Operator for viewing and retrieving the violation images and data for further processing. The application should allow for viewing, sorting, transfer & printing of violation data. ▪ It should print the photograph of violations captured by the outstation system which would include a wider view covering the violating vehicle with its surrounding and a closer view indicating readable registration number plate patch of the violating vehicle along with all data as per clause 4.

Sl. No.	Parameter	Minimum Specifications
		<ul style="list-style-type: none"> ▪ All outstation units should be configurable using the software at the Central Location ▪ Violation retrieval could be sorted by date, time, location and vehicle registration number and the data structure should be compatible with Jalandhar Police database structure. It should also be possible to carry out recursive search and wild card search ▪ The operator at the back office should be able to get an alarm of all fault(s) occurring at the camera site (e.g. sensor failure, camera failure, failure of linkage with traffic signal, connectivity failure, Camera tampering, sensor tampering). ▪ The automatic number plate recognition Software will be part of the supplied system, Success rate of ANPR will be taken as 75% or better during the day time and 40% or better during the night time with a standard number plate. ▪ The application software should be integrated with the e-Challan software for tracing the ownership details of the violating vehicle and issuing/printing notices. Any updates of the software (OS, Application Software including any proprietary software), shall be updated free of cost during the contract period by the SI. ▪ Image zoom function for number plate and images should be provided. In case the number plate of the infracting vehicle is readable only through the magnifier then in such cases the printing should be possible along with the magnified image ▪ Various users should be able to access the system using single sign on and should be role based. Different roles which could be defined (to be finalized at the stage of SRS) could be Administrator, Supervisor, Officer, Operator, etc. ▪ Apart from role based access, the system should also be able to define access based on location. ▪ Rights to different modules / Sub-Modules / Functionalities should be role based and proper log report should be maintained by the system for such access.

Sl. No.	Parameter	Minimum Specifications
		<ul style="list-style-type: none"> ▪ Components of the architecture must provide redundancy and ensure that there are no single points of failure in the key project components. Considering the high sensitivity of the system, design shall be in such a way as to be resilient to technological sabotage. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage ▪ The evidence of Infraction should be encrypted and protected so that any tampering can be detected. ▪ Ease of configuration, ongoing health monitoring, and failure detection are vital to the goals of scalability, availability, and security and must be able to match the growth of the environment. ▪ System shall use open standards and protocols to the extent possible and declare the proprietary software wherever used. ▪ The user interface should be user friendly and provide facility to user for viewing, sorting and printing violations. The software should also be capable of generating query based statistical reports on the violation data. ▪ The data provided for authentication of violations should be in an easy to use format as per the requirements of user ▪ User should be provided with means of listing the invalid violations along with the reason(s) of invalidation without deleting the record(s). ▪ Basic image manipulation tools (zoom etc.) should be provided for the displayed image but the actual recorded image should never change. ▪ Log of user actions be maintained in read only mode. User should be provided with the password and ID to access the system along with user type (admin, user). ▪ Image should have a header/footer depicting the information about the site IP and violation details like date, time, equipment ID, location ID, Unique ID of each violation, lane number, Regn. Number of violating vehicle and actual violation of violating vehicle etc. so that the complete lane wise junction behaviour is recorded including (Speed of violating vehicle, notified speed limit, Signal Jumping, Stop

Sl. No.	Parameter	Minimum Specifications
		<p>Line Violation, Speed Violation with Registration Number Plate Recognition facility.</p> <ul style="list-style-type: none"> ▪ Number plate should be readable automatically by the software/interface. There should be user interface for simultaneous manual authentication / correction and saving as well. Number plate should be readable automatically by the software/interface. There should be user interface for simultaneous manual authentication / correction and saving as well ▪ Interface for taking prints of the violations (including image and above details).
8	e-Challan Application	<p>The objective of the e-Challan application is as follows:</p> <ul style="list-style-type: none"> ▪ Issuing challan for traffic violations on a 24x7 basis. ▪ Maintaining the details pertaining to all the activities of the Traffic circles/violations/violators. ▪ Providing requisite structured/unstructured information to the traffic management officials as and when required. ▪ Generating various statutory reports for the administrative use and functioning of the Traffic unit in matters of prosecution of violators and monitoring the functioning of field officers. ▪ Integrating and networking the system with state-of-the-art hardware and application software for the Traffic Police to access and using the information in their day-to-day work. <p>The following are the key functional requirements of the e-Challan System:</p> <ul style="list-style-type: none"> ▪ E-challan software shall work in Authority -server mode, where the handheld devices units, workstation units will act as Authority's connected to the server through cellular network for data transfer. ▪ E-challan system shall be able to retrieve vehicle owners details and vehicle data from RTO data base to minimize data entry ▪ E-challan system shall be able to retrieve vehicle registration details and driving license details by reading appropriate smart card to minimize data entry

Sl. No.	Parameter	Minimum Specifications
		<ul style="list-style-type: none"> ■ Server should maintain log of all current devices. Any access to the system must be recorded along with date, time, user id and IP address ■ Traffic officer should log in to the hand held device through the unique user id and pass word or smart card issued for the purpose ■ A unique Challan number should be generated through Authority software for each challan ■ As soon as a vehicle registration number is entered, the handheld device should automatically check from the server if the vehicle is stolen, wanted in any criminal case or is in the list of suspicious vehicle ■ The most frequent traffic offences should be kept at the top in the drop down menu and offence details should be available if required by officer ■ Date, time and GPS coordinates of place of challan should be automatically populated in the relevant fields of Authority software ■ Compounding amount must populate in the field automatically from master table ■ The successful bidder should develop the GUI and functionality as per requirements of the Jalandhar Traffic Police ■ The GUI should be Multi lingual i.e., English, Hindi and Punjabi ■ It should be possible to integrate payment gate way operator interface with the system for facilitation of payment ■ The Application Software should work in a web based environment. ■ The application software should be user friendly, easy to operate ■ The software must provide comprehensive data back-up and restoration capability. ■ The system will function in web-based system where the hand-held device shall work as a node. ■ The application software should maintain the logs of user activities to facilitate the audit trail. ■ The system should have sufficient security features such as firewall, access control system, biometrics, password protection, audit trail, anti-virus etc.

Sl. No.	Parameter	Minimum Specifications
		<ul style="list-style-type: none"> ▪ Database server should be able to handle the activities of all the handheld devices at one time simultaneously with huge database size of prosecution, ownerships, driving license etc., without affecting the performance. ▪ The software should be able to generate various periodical reports, summaries, MIS reports, query reply etc... as per the requirements of Jalandhar Traffic Police. ▪ Administrator should be able to modify the master tables as and when required and should have the capability to push the changes to handheld devices. ▪ All database tables, records etc. required for various dropdown menus etc. shall also be created by the vendor. ▪ The application software is to be provided by the vendor to handle various processes of the prosecution required by the office of senior police officers, Courts etc.
9	Hand Held Devices for e-challan system	<ul style="list-style-type: none"> ▪ Once the application is loaded on the hand-held device there should be no possibilities to modify the application by the user. Reloading and modifying of application should be possible only by an administrator. ▪ On switching on the hand-held device the system must give access only after validation through user ID and password. ▪ The communication between the server and hand-held device would be through GSM/GPRS/ 3G or better connectivity etc. ▪ Every challan created must have a unique system generated identification number. ▪ The HH application must be able to access information from the main Server and display upon request, pop- up tables/codes, vehicle and license details, all types of offences, compounding amount, challan types, vehicle details, court calendar etc. in order to minimize the typing by the prosecuting officer. ▪ The hand held device should be light weight and easy to hold. ▪ The HH device should be able to access data/ information on the

Sl. No.	Parameter	Minimum Specifications
		<p>basis of driving license number, vehicle registration number etc. from the main server data relating to previous offences.</p> <ul style="list-style-type: none"> ▪ The hand-held application software should also suggest date of challan, place of challan, name of the Court and court date etc. to further reduce typing by the officer. These fields should be designed in consultation with Jalandhar Traffic Police. ▪ When a challan is issued, the name and ID of the officer should be printed on the Challan. ▪ The HH device must be able to input and print multiple offences on the same Challan ▪ The HHD software must validate Challan fields automatically before the Challan is printed. The system must ensure that certain fields are properly completed before allowing the Challan to be printed. ▪ When downloading application software or pop-up tables or lists to the HH, or uploading challan records to the Server, synchronization of HH system must be automatic, in order to minimize human intervention ▪ Uploading data to the Database Server should be automatic in consistent manner. ▪ The application should provide features wherein when a driving license/ vehicle registration number is entered, it should be able to pull from the server all the details relating to the driving license holder/ vehicle owner including history of previous offences. ▪ Software should capture the list of documents seized during prosecution and such list must be reflected on the printed court challan. ▪ The handheld application software shall allow the user to generate a summary report to facilitate evaluation of his daily work. The entire day report of the official be auto submitted to the administrator at the end of the day or closing hours of the official duty when HH is submitted at Office ▪ Once the Challan is complete and saved any further editing should not

Sl. No.	Parameter	Minimum Specifications
		<p>be possible unless so authorized by administrator.</p> <ul style="list-style-type: none"> ▪ Each hand-held device should be provided with original printed user manual and appropriate carry case for HH device with charger. ▪ The application software should allow online payment through payment gateway ▪ There should be automatic rejection of payment for the settlement of expired notices or challans. Partial payment of an offence must not be accepted by the system including previous violations fees. ▪ The software should update DL/RC smart card with the booked offence.
10	Public Address System	<ul style="list-style-type: none"> ▪ The Public Address System (PAS) should be capable of addressing citizens at specific locations from the JICCC. ▪ The proposed system shall contain an IP-based announcing control connected to the JICCC. ▪ Public Address System shall be used at intersections, public places, market places or those critical locations as identified by Authority to make important announcements for the public. It shall be able to broadcast messages across all PAS or specific announcement could be made to a particular location supporting single zone / multi zone operations. The system shall also deliver pre-recorded messages to the loud speakers attached to them from CD/DVD Players & Pen drives for public announcements. ▪ The system shall contain an IP-based amplifier and uses PoE/PoE+ power that could drive the speakers. The system shall also contain the control software that could be used to control/monitor all the components of the system that includes Controller, Calling Station & keypad, Amplifier (Mixing & Booster). ▪ The SI shall describe in detail the design, operational and physical requirements of the proposed public announcement system to demonstrate compliance with all the specified requirements of RFP. ▪ PAS master controller should have function keys for selecting the single location, group of locations or all locations, simple operation on

Sl. No.	Parameter	Minimum Specifications
		<p>broadcasting to any terminal or separated zones.</p> <ul style="list-style-type: none"> ▪ PAS master controller should facilitate multiple MIC inputs and audio inputs. ▪ IP and PC based solution – easy to use and maintain ▪ Remote configuration and administration ▪ POE / PoE+ or 12V power ▪ 10/100Base-TX Ethernet ▪ The system should not be an end of life / end of service product.
11	Emergency call Box	<ul style="list-style-type: none"> ▪ The emergency box (or panic button) will enable citizens to establish a two-way audio (microphone and speaker) – video (video camera and a video screen) communication link with operation staff at JICCC (or other locations where control solutions is deployed) through a press of a button. ▪ Emergency Call box to be strategically located, suitably sized and identified/clearly labelled for “Emergency”. Emergency button once pressed will send a call to the nearest police station. ▪ The emergency feature must also be available within the mobile app (to be developed as part of the RFP) which will enable the user to initiate a bidirectional audio – video call with operation staff at JICCC. In absence of connectivity, the application should send the current location and contact number of the citizen using emergency feature through text message to JICCC.

Technical requirements:

Adaptive Traffic Control-

Traffic Sensor Appropriate camera based traffic sensors may be chosen to provide the operational levels and accuracy as required for successful function of the ATMS system as per the SLAs defined

Adaptive Traffic Control- Traffic Controller

Appropriate camera based traffic sensors may be chosen to provide the operational levels and accuracy as required for successful function of the ATMS system as per the SLAs defined

Adaptive Traffic Control- Traffic Light Aspects

Key Features:

- Lowest power consumption for all colours
- Meets or exceeds intensity, colour and uniformity specifications
- Temperature compensated power supplies
- Uniform appearance light diffusing
- ITE products shall be Intertek/ETL/EN/Equivalent certified
- All units operate on AC or DC as the per the suggested solution by bidder

LED Aspects:

- Red, Amber, Green-Full (300 mm diameter): Hi Flux
- Red, Amber, Green-arrow (300 mm diameter): Hi flux
- Red, Green-Pedestrian (300 mm diameter): Hi Flux and Hi Brite
- Animated Pedestrian-Red and Green Animated c/w countdown (200 mm) Hi Brite with diffusions

LED Retrofit Specifications

Sl. No.	Parameter	Minimum Specifications
1	Power Supply	230 Vac *10% and frequency 50*5Hz – Solar shall be used for lights
2	Standards	EN 12368 complaint
3	Convex Tinted Lens	Available
4	Fuse and Transients	Available
5	Operating Temperature Range	0 - 55 degrees
6	Turn Off/Turn On Time	max 75 milliseconds
7	Total Harmonic Distortion	<20%
8	Electromagnetic interference	Meets FCC Title 47, Subpart B, Section 15 Regulation or equivalent EN/IRC standard
9	Blowing Rain/Dust Spec	MIL 810F complaint or equivalent EN/IRC standard
10	Minimum Luminous Intensity	Red 250, Amber 250, Green 250

Sl. No.	Parameter	Minimum Specifications
		(Measured at intensity point) (nm)
11	Dominant Wavelength (nm)	Red 630, Amber 590, Green 49
12	Lamp conflict compatibility :	Compatible with lamp failure and conflict System detection

Red Light Violation Detection Systems (RLVD)

Sl. No.		Description
1		General
	a	The system should be capable of generating a video in any of the standard industry formats (MJPEG, avi, mp4, mov, etc.) with at least 10 frames per second. The video shall be from t-5 to t+5 sec of the violation and should also be recorded (t being the instant at which the violation occurred).
2		Automatic Number Plate Recognition(ANPR) camera
	a	Sensor Type : Progressive scan CCD/CMOS, Day/Night Camera
	b	Resolution : 2 Megapixels or better
	c	Video Compression: Motion JPEG,H.265
	d	Video Resolution 2 Megapixels(1920X10180) or better HD camera
	e	Video H.265
	f	Frame rate Min. 25 FPS (For ANPR on highways. Refer BOM)
	g	Normal Horizontal Field of View at least 3.5 Mtr. (One lane)
	h	Typical Range 30 Mtrs. or better
	i	Operating Temp. 0 to 55 Degree C
	j	Auto Iris Control Yes
	k	Protection rating NEMA 4X / IP-66 rated
3		On site - out station processing unit communication & Electrical Interface (Junction Box)
	a	Data Storage on site The system should be equipped with appropriate storage capacity for minimum 24 hour recording, with overwriting capability. The images should be stored in tamper proof format only.
	b	Network Wired/GPRS based wireless technology with 3G upgradable to

Sl. No.	Description	
	Connectivity	4G capability.
	c	minimum 2(two) USB Port to support the latest external mass storage devices and Ethernet (10/100) Port for possible networking. However all logs of data transfer through the ports shall be maintained by the system.
	d	The system should be capable of working in ambient temperature range of 0oC to 55oC.
	e	Lightening arrester shall be installed for safety of system (As per BIS standard IS 2309 of 1989).
	f	The housing(s) should be capable of withstanding vandalism and harsh weather conditions and should meet IP66, IK10 standards (certified).
	g	UPS Backup (of minimum 30 minutes) to be provided only for RLVD System
4	Violation Transmission and Security	
	a	Encrypted data, images and video pertaining to Violations at the Onsite processing station should be transmitted to the MCJ electronically through GPRS based wireless technology with 3G upgradable to 4G, in Jpeg format.
	b	Advanced Encryption Standard (AES) shall be followed for data encryption on site and MCJ, and its access will be protected by a password.
	c	The vendor shall ensure that the data from the onsite processing unit shall be transferred to MCJ within one day
5	Video Recording	
	a	The system should be capable of continuous video recording in base station for 7 days. The system shall automatically overwrite the data after 7 days. It should be noted that at any point of time the local storage at the base station should have the data of previous 7 days
	b	Direct extraction through any physical device like USB, Hard disk shall be possible

Speed Violation Detection System:

- The speed violation detection system detects the over speeding vehicles and generate an automatic e-Challan for the over-speeding violation. The below figure shows the speed violation detection system installation
- The speed violation detection system captures speed of the vehicles which are passing through this system. The speed detection system detects speed of the vehicle and compares with the speed limit

set in the configuration. If the actual speed of the vehicle is more than the speed limit, then it triggers the ANPR system to capture the number plate of the vehicle. Both the number plate and actual speed of the violated vehicle will be stored in the system. The system detects speed accuracy of 10% (+/-) of the actual vehicle speed.

- The number plate deciphered are stored in the deciphered database. The number plate not deciphered by ANPR system are stored in the non-deciphered database. Later the non-deciphered number plate is manually further classified into soiled, broken and vernacular number plate.

All the deciphered number plate of violated vehicles e-Challans generated automatically. Non-deciphered number plate of violated vehicles e-Challans are generated manually

Speed violation detection camera specific details:

Sl. No	Description	
1	Speed	
a	Unit of Speed Measurement	Kmph
b	Speed detection system to Capture speed	250 Kmph +/- 5%
c	Speed Enforcement Technology	Radar
2	Digital Camera/Automatic Number Plate Recognition(ANPR) camera	
a	Video Compression:	H.265
b	Video Resolution	1280X720
c	Frame rate	Min. 50 FPS
d	Image sensor	Colour, Progressive scan CCD 1/3"
e	Exposure Control	Global shutter/rolling shutter, software adjustable 1/30 s – 1/27700 s
f	Day/Night Mode	Configurable day/night mode switching
3	Lens	
a	Lens Type	5. – 50 mm with high precision motorized positioning
b	Iris	Automatic motorized, programmable
C	Focus	Automatic motorized, programmable
D	Zoom	Automatic motorized, programmable
e	Optical Filter	Switchable: All pass / IR cut above 850 nm
f	ANPR Range	3 m – 20 m (10 feet – 65 feet)
4	Illumination	
a	Type	High power IR LED, regulated
b	IR Wavelength	850 nm
c	Intensity	3 preconfigured modes (low, medium, high)
d	Flash Time	Software adjustable, up to 950 µs
5	Processing & I/O	

a	CPU	Minimum 1.6 GHz x86 processor
b	Storage Memory	Storage for 7 Days violation data
c	Operating System	Linux
d	ANPR	ANPR software
e	Communication Protocol	ARP, ICMP, TCP/IP, DHCP, NTP, FTP, HTTP, SMTP, RTP
f	Communication Interface	100Mbit/sec, Ethernet
6	Radar frequency	
a	Measurement Principle	Doppler-Radar
b	Radar frequency	Approved frequency in India
c	Direction Selectable	uni- or bidirectional
d	Normal Horizontal Field of View	at least 3.5 Mtr. (One lane)
e	Operating Temp.	-20 to +55 Degree C
f	Protection rating	IP67
g.	Certification	CE, FCC, UL, cUL, C-tick, CB, VCCI
7	Local processing unit communication & Electrical Interface (Junction Box)	
a.	Data Storage on site	The system should be equipped with appropriate storage capacity for 7 days 24X7 recording, with overwriting capability. The images should be stored in tamper proof format only.
b.	Network Connectivity	Wired/ GPRS based wireless technology with 3G upgradable to 4G
c.	The system should be capable of working in ambient temperature range of -20 degree C to 55 degree C.	
d	Lightening arrester shall be installed for safety of system (As per BIS standard IS 2309 of 1989).	
e	The housing(s) should be capable of withstanding vandalism and harsh weather conditions and should meet IP66, IK10 standards (certified).	
8	Violation Transmission and Security	
a.	Encrypted data, images pertaining to Violations at the local processing unit should be transmitted to the TCC electronically through wired/ GPRS based wireless technology with 3G upgradable to 4G, in Jpeg format.	
b.	Advanced Encryption Standard (AES) shall be followed for data encryption on site and TCC, and its access will be protected by a password.	
c.	The vendor shall ensure that the data from the onsite processing unit shall be transferred to TCC within one day.	

E-Challan Handheld device

Core board	
Operating System	Latest Windows or Android OS
Processor	Min 1 GHz min.
Memory (Flash ROM)	minimum 8 GB

RAM	1 GB Min
Extend Slot	Micro SD 32 GB
Motherboard	
Display	minimum 5.5 inch IPS, 1280*720 res.
Touch Screen	Yes
Form Factor	Yes
GPS	GPS/Galileo/Glonass/Beidou
Connectivity	4G/LTE/3G/2G/Wi-Fi/Bluetooth
Smart/Magnetic Card Reader	Support
QR Code Reader	Camera/QR Code Reader
Local-USB Connector	USB2.0 connection minimum
SIM card slot	Yes
TF card slot	Yes
Power jack	Yes
Audio Jack	Yes
Thermal Printer	Printing of minimum 2 inch in width
Barcode scanner	1D and 2 Scanner
External Interface	USB HOST/RS232(Customized)
Protection class	IP54
Drop resistance level	2m
Camera	
Camera	5 MP min (Auto focus)
Touch Screen	Support still image and video capture
Keypad	
Front	Touch screen/ On screen Keys
Battery	
Type	rechargeable Li-ion battery 2000mAh, minimum Working Hours- 10 hrs
Operating & storage temperature	-5°C to 50°C
Operating Humidity	20% - 90%
Weight	Maximum 550 g
Payment PINPAD	The device should have lPCI , EMV certified PINPAD as per RBI guideline for accepting payment through Credit / Debit card

Field Junction Box

Sl. No.	Parameter	Minimum Specifications
1	Size	Suitable size as per site requirements to house the field equipment
2	Cabinet Material	Powder coated CRCA sheet/ Stainless steel
3	Material Thickness	Min 1.2mm
4	Number of Locks	3 way lock
5	Protection	IP 55, Junction Box design should ensure to keep the temperature within suitable operating range for equipment's and should also avoid intentional water splash and dust intake
6	Mounting	On Camera Pole / Ground mounted on concrete base
7	Form Factor	Rack Mount/DIN Rail
8	Other Features	<ul style="list-style-type: none"> • Rain Canopy, Cable entry with glands and Fans/any other accessories as required for operation of equipment's within junction box. • Shall have separate inlet/outlet and lockable doors for: <ol style="list-style-type: none"> a. Power Cabinet: This cabinet shall be capable of housing electricity meter, online UPS system and the redundant power supply system. b. Control cabinet: This cabinet shall house the controllers for all the field components at that particular location e.g. ANPR, PTZ, RLVD, Fixed cameras, etc.

Poles

Sl. No.	Parameter	Minimum Specifications
1	Pole type	Hot Dip Galvanized after Fabrication with Silver coating of 86 micron as per IS:2629; Fabrication in accordance with IS-2713 (1980)
2	Height	5-10 Meters, as-per-requirements for different types of cameras & Site conditions
3	Pole Diameter	Min. 10 cm diameter pole (bidder to choose larger diameter for higher height)

Sl. No.	Parameter	Minimum Specifications
4	Cantilevers	Based on the location requirement suitable size cantilevers to be considered with the pole
5	Bottom base plate	Minimum base plate of size 30x30x1.5 cm
6	Mounting facilities	To mount RLVD Cameras, CCTV cameras, Traffic Signals, Pedestrian Signals, Switch, etc.
7	Pipes, Tubes	All wiring must be hidden, through tubes/pipes. No wires shall be visible from outside.
8	Foundation	Casting of Civil Foundation with foundation bolts, to ensure vibration free erection (basic aim is to ensure that video feed quality is not impacted due to winds in different climatic conditions). Expected foundation depth of min. 100cms. Please refer to earthling standards mentioned elsewhere in the document
9	Protection	Lightning arrester at select sites as per the requirements

Edge Level Switch (at Traffic Junctions)

Sl. No.	Parameter	Minimum Specifications
1	General Features	The switch should be Industrial Grade ruggedized in nature that provides minimum 8 x 10/100/1000 BASETX access ports, additional 2 x 1000 Base-X SFP & 2x 1GE Uplink ports. One (1) ruggedized single mode SFP should be supplied with the switch.
		The switch should support backup storage drives, which will store the last known configuration of the switch, in the case of hardware failure and replacement. Reinserting the storage drive should restore the switch to original working condition without any manual intervention.
2	Layer 2 Features	802.1Q VLAN on all ports with minimum 8k MAC address
		Spanning Tree Protocol as per IEEE 802.1d, ring protection protocol like REP or equivalent
		Should support Jumbo frames up to 9000 bytes & Link Aggregation Control Protocol (LACP) as per IEEE 802.3ad.

Sl. No.	Parameter	Minimum Specifications
		The switch should support IGMP v1/v2/v3 & up to 1000 IGMP groups as well as IGMP snooping & IGMP filtering. Should also support MLD v1/v2.
3	Layer 3 Features	Static, Inter-VLAN routing must be enabled from day one
		The switch should support Dynamic Routing.
4	Quality of Service (QoS)	Switch should support classification and scheduling as per IEEE 802.1P on all ports with minimum four egress queues per port
5	Features	The switch should provide traffic shaping and rate limiting

IP Amplifier

Sl. No.	Parameter	Minimum specifications
A	Amplifier Type	Class D
B	Amplifier output	50 Watts
C	Connectivity	IP-POE/ PoE+ based
D	Power	Automatic on/off operation
E	Operating temperature	-10°C and +60°C at a maximum relative ambient humidity of 90%.
F	Certification	CE
G	Monitoring functionality	Line monitoring
H	Environment protection	IP 55 or better

Public Address System

Sl. No.	Parameter	Minimum Specification
1	PAS system	<p>a) Should have the capability to control individual PAS i.e. to make announcement at select location (1:1) and all locations (1: many) simultaneously.</p> <p>b) The PAS should also support both Live and Recorded inputs.</p>
2	Speaker	Minimum 2 speakers, To be used for Public Address System
3	Connectivity	IP Based

Sl. No.	Parameter	Minimum Specification
4	Access Control	Access control mechanism would be also required to establish so that the usage is regulated.
5	Integration	With VMS and Command and Control Centre or any other component if required
6	Construction	Cast Iron Foundation and M.S. Pole, Sturdy Body for equipment
7	Battery	Internal Battery with different charging options (Solar/Mains)
8	Power	Automatic on/off operation
9	Casing	IP-66 rated for housing
10	Operating conditions	0° to 50°C

Emergency call box

1. A high quality digital transceiver, to be placed at mentioned traffic signals.
2. The unit shall preferably have a single button which when pressed, shall connect to JICCC over the network developed as a part of this RFP

Sl. No.	Parameter	Minimum Specification
1	Construction	Cast Iron/Steel Foundation, Sturdy Body for equipment
2	Call Button	Watertight Push Button, Visual Feedback for button press
3	Speaker & Microphone	Watertight and Industrial grade equipment
4	Connectivity	Fibre based
5	Sensors	For tempering/Vandalism
6	Battery	Internal Battery with different charging options (Solar/Mains)
7	Power	Automatic on/off operation
8	Casing	IP-66 rated for housing
9	Operating Conditions	0-55 degrees

ANPR LIU

Sl. No	Minimum Specification
1.	Shall have minimum Quad Core CPU (4 physical CPU cores)
2.	Shall have minimum 64-bit architecture

3.	Shall have minimum 8 GB RAM (DDR3-1600 or above)
4.	Shall have minimum 500 GB Hard Disk
5.	Shall have Dedicated Gigabit network port per camera (MTU 9000 / jumbo frames), +1 LAN port
6.	Shall have capability to connect 4 cameras per LPU

4.4 Variable Messaging System (VaMS)

The purpose of Variable Message Displays is to provide public information to citizens related to traffic, environment, disasters, city information, route information etc.

Variable messaging displays will be used to display the useful information related to:

- Traffic congestion
- Accidents incidents
- Ongoing Roadwork zones
- Speed limits
- Key notices or messages from JICCC like information about any emergency or disaster
- Display the parking availability information, etc.

VaMS system is one of the important and effective tool to manage traffic in response to road incidents, special events and construction or maintenance activities on the road. When drivers are to be warned of an incident, advised to opt for an alternate route, guided to reach a specific location or clear a lane as a response to an incident, the message posted should be appropriate and precise. The messages and the procedure for displaying them should be such that the information is grasped by a driver whose primary focus is driving his vehicle while ensuring his and his co-passenger's safety.

The VaMS unit shall be able to communicate with the Jalandhar Integrated Command and Control Centre System (JICCC) using GSM Data/Wi-Fi/ Ethernet/SMS Channel. GSM data channel (GPRS) / Wi-Fi shall be used to send online messages and SMS channel shall be used to send configuration packets to configure the SIM. Ethernet port shall also be extended to ground level using necessary cables for local troubleshooting. Each unit shall be provided with a unique identification number and shall communicate with Jalandhar Integrated Command and Control Centre System (JICCC).

VaMS shall be managed and operated from the JICCC where information in the form of data messages shall be fed in a manner to be displayed on a specific VaMS installed at a particular location or across all locations. The VaMS boards shall be viewable from a distance of 100m and various angles on the road.

For installing VaMS Signboards, the MSI shall provide Gantry with spans, as required at various locations (single lane road, double lane road). Spans need to be specified depending on the number of lanes that need to be bridged. MSI shall consider additional space for lateral clearance as well as a vertical clearance height as per NHAI (National Highway Authority of India) guidelines. Variable messaging System (VaMS) will be used by other applications like Intelligent Signalling, Smart Parking, Environment Monitoring, etc. as mentioned in respective sections.

The signage, which appears on the road to be readable and visible, should be displayed for a certain time duration so that it is read by the road user. The reading time is the time that driver actually takes to read a sign message. The exposure time is the length of time a driver is within the legible distance of the message. Exposure time of the message must be always greater than reading time.

Speed (Kmph)	Time (sec) to Travel 300m
50	21.6
70	15.4
90	12
100	10.8
120	9

It is, however, recommended that the size and distance for clear legibility should be designed for at least 15 seconds for NH and 20 seconds for access controlled expressways. Furthermore, the messages need to be displayed alternately in JUNJABI, HINDI, and 'ENGLISH', if possible pictorially as well. The board having the facility to display minimum of 2 lines of 12 or 15 English characters, can have English display in 1st line and other language in 2nd line, at the same time as well. When the VMS displays a series of message, 2-4 seconds per message is recommended. The blinking feature may be used on one or more of the messages. It should, however, not be used for more than one line of each message.

Scope of Services

The broad scope of work to be covered under this component will include the following, but is not limited to:

- Installation of IP based VaMS boards at approximately 25 locations across the city. These VaMS boards shall have different characteristics depending upon the location and purpose of installation. VaMS board displays are to be controlled by Jalandhar Traffic Police or personnel from the JICCC.

- Installation of Installation of Poles/Cantilevers/Gantry as required power connection, power backup, Installation and configuration of application and network connectivity.
- Details of Installation of Poles/Cantilevers/Gantry if required, Civil and Electrical works, earthing, etc. from Intelligent Signalling components etc.

Geographical Scope of Services:

Sl. No	Locations
1	Bus stand
2	Central railway station
3	Cantonment railway station
4	Verka Milk Plant
5	Gulshan Hotel
6	PAP chowk
7	Dakoha Railway Crossing Chowk Point
8	Wadala Chowk
9	Municipal corporation
10	Guru Nanak Mission Chowk
11	Pholriwal Gate

Note : Above is the tentative list of locations and detailed list of all 25 location will be finalized post system study/ feasibility report submitted by MSI

Functional specifications:

Sl. No.	Minimum Specification
1	<p>System Requirements</p> <p>The system should be capable to display warnings, traffic advice, route guidance and emergency messages to motorists from the JICCC in real time</p> <p>The system should also be capable to display warnings, traffic advice, route guidance and emergency messages to motorist by using local PC/Laptops.</p> <p>The VaMS should display text (multi lingual – Hindi & English or any other local language) and graphic messages using Light Emitting Diode (LED) arrays.</p> <p>The System should able to display failure status of any LED at JICCC.</p> <p>The System should support Display characters in true type fonts and adjustable based on the Operating system requirement</p> <p>The VaMS workstation at the JICCC should communicate with the VaMS controller through the network. It should send out command data to the variable message sign controller and to confirm normal operation of the signboard. In return, the VaMS workstation should receive status data from the VaMS controller.</p>

Sl. No.	Minimum Specification
	VaMS controllers should continuously monitor the operation of the VaMS via the provided communication network.
	Operating status of the variable message sign should be checked periodically from JICCC.
	It shall be capable of setting an individual VaMS or group of VaMS's to display either one of the pre-set messages or symbols entered into the computer via the control computer keyboard or by another means.
	It shall be capable of being programmed to display an individual message to a VaMS or a group of VaMS's at a pre-set date and time.
	A sequence of a minimum of 10 messages/pictures/ pre-decided sign or group of signs shall be possible to assign for individual VaMS or group of VaMS's.
	It shall also store information about the time log of message displayed on each VaMS. The information stored shall contain the identification number of the VaMS, content of the message, date and time at which displayed message/picture starts and ends.
	The central control computer shall perform regular tests (pre-set basis) for each individual VaMS. Data communication shall be provided with sufficient security check to avoid unauthorized access
2	Variable Message Sign board application
	Central Control Software allows controlling multiple VaMS (up to 20) from one console.
	Capable of programming to display all types of Message/ advertisement having alphanumeric character in English, Hindi, Punjabi and combination of text with pictograms signs.
	Capable of controlling and displaying messages on VMS boards as individual/ group.
	Capable of controlling and displaying multiple font types with flexible size and picture sizes suitable as per the size of the VaMS.
	Capable of controlling brightness & contrast through software.
	Capable to continuously monitor the operation of the Variable Message sign board, implemented control commands and communicate information to the Traffic Monitoring Centre via communication network.

Sl. No.	Minimum Specification
	<p>Real time log facility – log file documenting the actual sequence of display to be available at central control system</p> <p>Multilevel event log with time & date stamp</p> <p>Access to system only after the authentication and acceptance of authentication based on hardware dongle with its log.</p> <p>Location of each VMS will be plotted on GIS Map with their functioning status which can be automatically updated.</p> <p>Report generation facility for individual/group/all VaMSs with date and time which includes summary of messages, dynamic changes, fault/repair report and system accessed logs, link breakage logs, down time reports or any other customized report.</p> <p>Configurable scheduler on date/day of week basis for transmitting pre-programmed message to any VaMS unit</p> <p>Various users should access the system using single sign on and should be role based. Different roles which could be defined (to be finalized at the stage of SRS) could be Administrator, Supervisor, Officer, Operator, etc.</p> <p>Apart from role based access, the system should also be able to define access based on location</p> <p>Rights to different modules / Sub-Modules / Functionalities should be role based and proper log report should be maintained by the system for such access</p> <p>Components of the architecture must provide redundancy and ensure that there are no single points of failure in the key project components. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage.</p> <p>Ease of configuration, ongoing health monitoring, and failure detection are vital to the goals of scalability, availability, and security and must be able to match the growth of the environment.</p> <p>System shall use open standards and protocols to the extent possible</p> <p>Facility to export reports to excel and PDF formats.</p>
3	<p>Remote Monitoring</p> <p>All VaMS shall be connected/configured to Traffic Monitoring Centre for remote monitoring through network for two-way communication between VaMS and control Room to check system failure, power failure & link breakage.</p>

Sl. No.	Minimum Specification
	Remote Diagnostics to allow identifying reason of failure up to the level of failed individual LED.

Technical specifications:

Sl. No.	Minimum Specification	
1	Dimensions	3.0 mtr length X 1.5 mtr height X 0.2 mtr depth. (3000mm x 1500mm X 200mm)
2	Colour LED	Full Colour, class designation C2 as per IRC/EN 12966 standard
3	Luminance Class/Ratio	L3 as per IRC/EN 12966 standards
4	Luminance Control & auto Diming	
	a	Should be automatically provide different luminance levels but shall also be controllable from the traffic centre using software
	b	Auto dimming capability to adjust to ambient light level (sensor based automatic control)
	c	Photoelectric sensor shall be positioned at the sign front and sign rear to measure ambient light. Capable of being continually exposed to direct sunlight without impairment of performance.
5	Contrast Ratio	R3 as per IRC/EN 12966 standard
6	Beam Width	B6+ as per IRC/EN12966 standards
7	Pixel Pitch	20mm or better
8	Picture Display	
	a	At least 300mm as per IRC /EN 12966 standards
	b	Full Matrix: Number of lines & characters adjustable, active area: 2.88mX1.2m at least
	c	Synchronized Dot to Dot display.
	d	Capable of displaying real time, customized messages generated by JICCC.
	e	Special frontal design to avoid reflection.
	f	Display shall be UV resistant
9	Viewing Angle	B6+ as per IRC/EN12966 standard- Viewing angle shall ensure message readability for motorists in all lanes of the approach road

Sl. No.	Minimum Specification	
10	Viewing Distance	Suitable for readability from 150 Mtrs. or more at the character size of 240mm, from moving vehicles.
11	a	Self-Test
	b	VMS shall have self-test diagnostic feature to test for correct operation.
	c	Display driver boards shall test the status of all display cells in the sign even when diodes are not illuminated.
	d	All periodic self-test results shall be relayed to the JICCC in real time to update status of VaMS
12	a	Alarms
	b	Door Open sensor to Inform Control room during unauthorized access
	c	LED Pixel failure detection alarm
13	Flicker	Refresh Frequency should not be less 90 Hz. No visible flicker to naked eye.
14	Multiple Data Communication interface/Ports	RJ45 Ethernet, RS232, RS 485, FC port and any other suitable
15	Communication (connectivity)	Wired/GPRS based wireless technology with 3G upgradable to 4G capability.
16	Ambient Operating Temperature	The system should be capable of working in ambient temperature range of -10 degrees to 60 degrees.
17	Humidity (RH)	Operating ambient humidity: 20% - 90% Rh or better.
18	Protection against Pollution/dust/water	Complete VMS should be of IP 65 protection level from front and IP54 from side and rear. As per EN60529 or equivalent Standard
19	Power	
	a	170-250V AC (more than 90% power factor) or DC as per equipment requirement.
	b	Protection for overvoltage/ fluctuation/drop of the nominal voltage (50%) shall be incorporated.
	c	The enclosure shall contain at least two 15 Amp VAC (industrial grade) outlet socket for maintenance purpose

Sl. No.	Minimum Specification	
20	Power Back-up & its enclosure	UPS for 15 Mins power back-up with auto switching facility. The enclosure of UPS and battery should be pole mountable with IP 65 protected housing and lockable. Batteries with solar charging options can also be recommended as back up
21	Material for VaMS frame	at least 2mm aluminium or non-corrosive, water resistant or better
22	Mounting, Installation and finishes	<p>a Mounting structure shall use minimum 6 Mtrs. high hexagonal/octagonal MS Pole or suitable structure with 5.5 mtr. Minimum vertical clearance under the VaMS sign from the Road surface. MSI shall be responsible to carry out the site survey to assess site requirement including pole height/suitable structure for VaMS installation at various places in the city.</p> <p>b The mounting shall be capable of withstanding road side vibrations at site of installation.</p> <p>c It shall be provided with suitable walkway for maintenance access.</p> <p>d The sides interior and rear of enclosures shall be provided in maintenance free natural aluminium finish. All enclosure shall be flat and wipe clean.</p> <p>e Rugged locking mechanism should be provided for the onsite enclosures and cabinets</p> <p>f For Structural safety, the successful bidder has to provide structural safety certificate from qualified structural engineers approved/ certified by Govt. Agency.</p>
23	Wind Load	WL9 as per EN12966 to withstand high wind speeds and its own load.
24	Cabling, connections and Labelling.	<p>a All cable conductors shall be of ISI marked for quality and safety. It shall be of copper insulated, securely fastened, grouped, wherever possible, using tie warps approximately every 10-20 cms or cable trays.</p> <p>b All connections shall be vibration-proof quick release connections except for power cables terminating in terminal blocks, which shall be screwed down.</p> <p>c All terminal block shall be made from self-extinguishing materials. Terminations shall be logically grouped by function and terminals carrying power shall be segregated from control signal terminals.</p>

Sl. No.	Minimum Specification		
	d	All cables shall be clearly labelled with indelible indication that can clearly be identified by maintenance personnel using “As built: drawings”.	
	e	Lightening arrester shall be installed for safety on each VMS.	
	f	The successful bidder has to provide safety certificate from qualified Electrical engineers approved/certified by Govt. Agency	
25	Local VaMS	Storage in	Embedded VaMS controller should be capable to store at least 100 messages and symbols/pictograms to allow display to run in isolated mode on a predefined structure/timings, in case of connectivity failure.

4.5 Disaster Management

MSI has to provide a separate module of Disaster Management as part of software solution. The Disaster Management module should be able to collect, gather and analyse the critical data of city from various channels. The system should be able to display a strategic view or big picture of probable disaster. The system will act as a communication channel and dissemination of information to authorized personals using JICCC. The critical data elements may be decided in consultation with JSCL and nodal authorities. The system should be able to receive predictive analysis which can finally reduce response time and improve SLAs.

Disaster Management module should be able to communicate or to be integrated with National Emergency Operation Centre (NEOC) of **National Disaster Response Force (NDRF)** based on defined SOPs. The Disaster Management system should be in compliance to applicable laws. The Disaster management module should have interoperability between cities, here it refers that disaster management module of any city should be able to cater the disaster management operation of any of the other cities as applicable. Standard Operating Procedures (SoPs) must adhere with the Governance structure of JSCL and Municipal Corporations, as in case of any incident or disaster decision making ability lies with the authority.

4.6 Jalandhar Environmental Monitoring System (JEMS)

Environmental pollution, particularly of the air, is nowadays a major problem that unknowingly affects lives in the cities. As clear focus of building [city] as one of the finest example of SMART city, Authority believes it is important that citizens know of the air that they breathe. Citizens & visitors to City can enjoy unique experiences that keep them feeling good by knowing city's environment condition at different locations.

The Air quality should be monitored by a network comprising:

- Fixed monitoring stations
 - Data processing
 - Data transmission to a central system
- A central processing system

KPIs for Environmental Monitoring System:

- Provide better quality air to citizens of Jalandhar
- Monitor environment pollution and have measures to control pollution
- Environmental monitoring to be implemented in all major parts of the city especially in crowded places
- Environmental monitoring should consist of measuring levels for Temperature, Humidity, Ambient Light, Sound, Pressure, CO, CO₂, NO₂, O₂, SO₂ and compulsorily PM 2.5 and PM 10.
- Integrate with other disaster management applications from other nodal organizations of environment
- Additional monitoring will be done in crowded areas of Jalandhar
- Environment monitoring sensors will be installed dump yards and solid waste management locations and crowded areas of Jalandhar

Scope of services

- Install minimum of 5 environment sensors (as per the functional requirement) & display environment related information at various strategic locations through variable message system (VaMS)

- The environment sensors shall be integrated with the central control system at JICCC to capture and display/ provide feed on Temperature, Humidity, Pollutants like SoX, NoX, CoX, etc., Noise Pollution, Electromagnetic Radiation, UV radiation etc. The data collected should be location-marked.
- Various environment sensors shall sense the prevailing environment conditions and send the data to the integrated control system where real time data resides and the same shall be made available to various other departments and applications for decision making.
- Then this information is relayed instantaneously to signage – large, clear, digital-display screens which let citizens know regarding the prevalent environmental conditions. The environmental monitoring data should be displayed by picking data from VMS application in real time.
- Further environmental sensors recorded data shall be used by Mobile application developed as part of e-Governance to enable user for alarm management and notification of environmental details on real time basis.
- Grievance Redressal of Citizen integration to e-Governance Mobile App where citizen can take the picture, upload the same with Geo Tagging. The complaint should be automatically forwarded to the respective staff, with escalation within specified timelines supported with multilingual text to speech, speech to text and speech to speech systems.

Components of Environmental Sensors:

1. Wireless Environment Sensor
 - Collect sensor data
 - Send recorded information to central system
2. Central System
 - Receive information from environment sensors
 - Display the information on real-time basis
 - Send information to mobile phone application
 - Save information in database
3. Mobile Device of Driver
 - Connect to central web-server
 - Receive environment information from central system
 - Alarm management and safe environment mode features
4. Digital Display Unit
 - Shall receive information from the central application System and operate accordingly

Functional Specifications for Environmental Monitoring System:

1. Smart environment sensors should gather data about pollution, ambient conditions (temperature and humidity), levels of gases in the city (pollution) and any other events on an hourly and subsequently daily basis. User should be able to set the schedules as per requirements. It is for information of citizens and administration to further take appropriate actions during the daily course / cause of any event.
2. The environment sensors should be having the following capabilities:
 - They should be ruggedized enough to be deployed in open air areas, on streets and parks
 - They should be able to read and report at least the following parameters: Temperature, Humidity, Ambient Light, Sound, Pressure, CO, CO₂, NO₂, O₃, SO₂ and compulsorily PM 2.5 and PM 10 Noise and UV
3. The analysers must function properly in all conditions without any defect between 0 to 50 degrees C ambient temperatures, 0 ambient dust levels. The data capture rate should not be less than 90%
4. The manufacturer of the Equipment should assure technical support for the equipment for the duration as indicated in the scope
5. Smart environment sensors will inform and enable citizens and administrators to keep a check on their endeavours which impact environment and enable the city to take remedial action if required. These environmental sensors can also be connected via 3G or 4G wireless network or Wi-Fi networks. It is not mandatory to connect all sensors via MPLS fiber network.
6. The data should be collected in a software platform that allows third party software applications to read that data. Various environment sensors shall sense the prevailing environment conditions and send the data to the integrated control system where real time data resides and the same shall be made available to various other departments and applications for decision making. It is preferred if the platform also includes intelligent analytical engines that makes information meaningful to all stakeholders and helps ease decision making.
7. Integration of environmental monitoring system with Variable messaging system (VaMS) to be displayed wherever possible (need to be finalized post detailed survey of locations).

8. The sensor management platform should allow the configuration of the sensor to the network and also location details etc.
9. The sensors should be able to be managed and calibrated remotely. This includes sensors being updated with calibration parameters, software upgrades. Sensors must also provide updates and detect faults with self-diagnosis functionality.
10. Apart from information provision, the sensors must ensure data is transmitted securely and have security measures from sensors to the software platform. It must also ensure tamper alerts are provided in cases of vandalism, security breaches, etc.
11. Any sensor failure should alarm and generate an event that should be linked with Incident Management system automatically and should be capable to schedule the automation of sending the failure report to the vendor
12. The sensors provided should be 99% accurate and should be of industry standards
13. Apart from information provision, the sensors must ensure data is transmitted securely and have security measures from sensors to the software platform. It must also ensure tamper alerts are provided in cases of vandalism, security breaches, etc.
14. Calibration system should be provided for the calibration of the air quality analysers, data acquisition system.
15. The data collected should also be available on permitted mobile devices as necessary
16. Real time or averaged data can be viewed quickly and easily client interface on the central computer
17. It should have a feature for viewing instantaneous and historical data in the form of tables and graphs either locally or from a remote client
18. Generation of reports for pollution load, wind etc. should be available
19. Alarm annunciation of analyser/sensor in abnormal conditions in the control centre so that appropriate action can be taken by authorities
20. The environmental sensors should be visible as a layer in GIS Maps

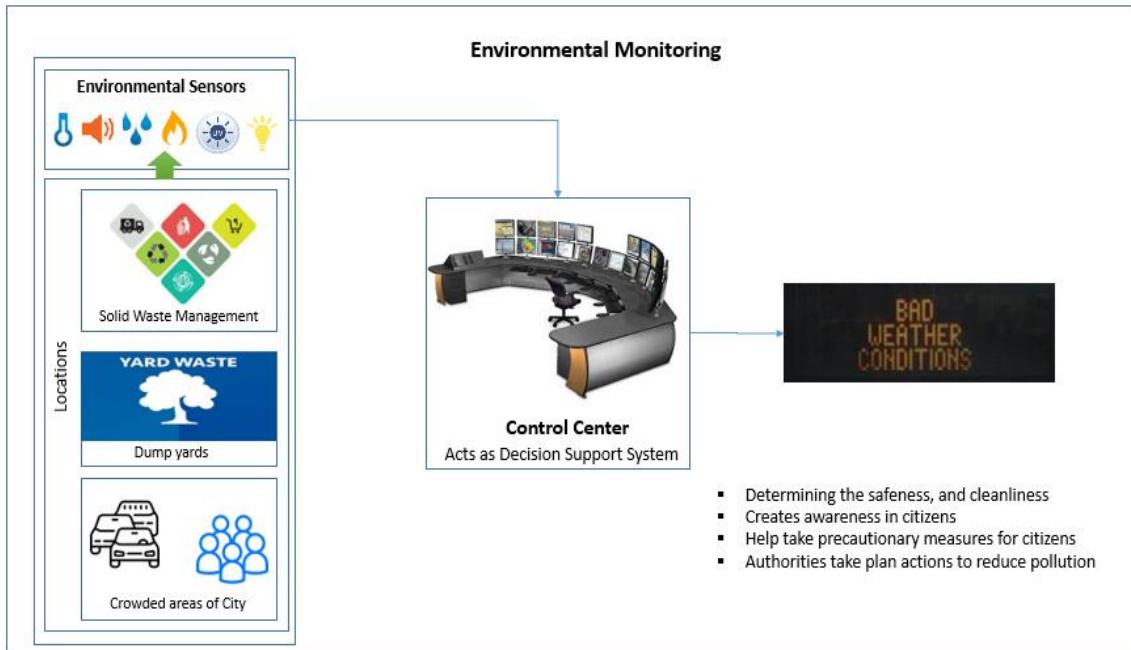


Figure: Illustrative diagram for Environmental Monitoring

Geographical Scope of Services

Sl. No	Locations
1	Bus stand
2	Model Town
3	Cantonment railway station
4	BMC Chowk
5	Guru Nanak Mission Chowk

Technical Specifications:

Sl. No	Parameter	Minimum Specification
1	Measurement elements	Temperature, Humidity, Ambient Light, Sound, CO, NO ₂ , O ₃ , SO ₂ , PM2.5, PM 10
2	Measurement component Measurement range	O ₃ : 0 – 390 ppb
		SO ₂ : 0 – 630 ppb
		CO : 0 – 31 ppm

Sl. No	Parameter	Minimum Specification
		CO2 : 0 to 10% / 0 to 20%
		O2 : 0 to 10% / 0 to 25% (2 ranges each, maximum range ratio 1: 25 except O2) * Optionally, N2O and CH4 can be measured
		PM 2.5: 0 to 250 micro gms / cu.m
		PM 10: 0 to 450 micro gms / cu.m
		Light: up to 10,000 Lux
		UV: Proportion of UV Present in μW /Lumen & Total amount in $\mu\text{W}/\text{M}^2$
		Noise: up to 100 dB (A)
3	Temperature, Pressure and Humidity Sensor	Real-time Temperature Range: outdoor $0^\circ\text{C} \sim 50^\circ\text{C}$
		Real-time in Air Humidity Level Display
		Real-Time Pressure Display (in Bars or millibars)
4	Connectivity	Wi-Fi, Ethernet or GSM (3G)
		Sensors must have provision to interchange between Wi-Fi or GSM systems easily
5	Software and Data backup	Backup measurement data for up-to 5 days in case of network failure or system maintenance cycles
6	Mechanical Enclosure	Single enclosure with all components inside or simplified mounting
7	Data validity and stabilization	Sensors must ensure data of sensors is valid and not require stabilization times in case of power outages less than 5 hours.
8	Product origin and certification	Must also qualify a minimum international standards on product certification such as CE, FCC and PTCRB
9	Rain Water measurement	in mm
10	Repeatability	$\pm 0.5\%$ FS
11	Zero Drift	$\pm 1.0\%$ FS max./week ($\pm 2.0\%$ FS/week max. if range is less than 200ppm) $\pm 2.0\%$ FS max./month for O2 meter
12	Respond Speed	120 seconds max. for 90% response from the analyses inlet

4.7 Integration with NERS (Mohali, Punjab)

National Emergency Response System (NERS) with Smart City solution

Vision of Government of India is to have a single Emergency number across the State for all emergency services. State government has nominated an agency as the PSAP (Public Safety Answering Point) to implement “112” NERS in the state. The Emergency services will report to centralized call centre and then further action is performed by respective department and designated nodal agencies. This would ultimately lead to better service delivery, satisfaction of citizens and transparency in department processes.

An integrated Centralized Emergency 112 call centre with command and control room will enable call takers, dispatchers and other staff working in the control room environment to be able to efficiently access all communication and information resources required to manage operational incidents effectively. Seamless interaction among various Control Rooms of nodal departments (Police, Health & Fire) shall take the lead position depending on the type of emergency. For example: in case of report of fire at some farmer’s field during summer, the Fire Emergency Control Room will take the lead by all the call will land on Centralized Emergency 112 call centre.

Under Jalandhar smart city- Emergency operations, a provision has made to Integrate IoT elements of JICCC and NERS for a holistic view of emergency operations.

Some of the IoT elements (Vehicle tracking units) shall be installed in PCR vans of Jalandhar by JSCL and are tracked and managed at JICCC. Few of the VTU’s shall be installed by NERS in some of the vehicles like Ambulance, Fire and PCR vans. As part of this RFP, MSI shall study the feasibility of integration of IoT elements of NERS project into JICCC and IoT elements installed by JSCL shall be integrated into NERS project at Mohali.

As part of NERS projects, there shall be four dispatchers located at JICCC for managing emergency situations at Jalandhar. The number of dispatchers can grow to ten in next 4 years. Provision for seating of these dispatchers to be part of planning as part of JICCC. The hardware and software required for the dispatchers shall be procured by NERS. MSI shall perform a detailed study of integration with NERS and get approval from Authority before integration of the components of Emergency Response System.

Scope of work:

Sl. No	Features
1	To facilitate a common live view in case of an incident, the IoT data shall be Geo-tagged and Geo-referenced on Jalandhar GIS Map and integrate with common operations platform of JICCC). The VTU's installed by NERS project shall be integrated with JICCC.
2	During an incident when a call is received by NERS, the location of the incident will be displayed in NERS control centre and should also be simultaneously displayed at JICCC. This information shall help dispatchers to take relevant action near the premises of the incident using common operations platform .
3	Write integrated SOPs as required for JICCC
4	To establish connectivity between two locations, a dedicated channel/ any other wireless technology can be implemented between NERS & JICCC, the cost incurred for setting up the connectivity should be considered as part of this RFP.
5	There shall be seamless integration between the components of NERS and JICCC for managing emergency operations
6	The data gathered for an incident including location & activities performed during emergency operations should be recorded for further analysis.
7	MSI reports for emergency response calls shall be made available at JICCC

Technical Specifications

Automated Vehicle Locator System

Sl. No	Parameter	Minimum Specifications
1.	General Requirement	<p>Each vehicle, using the GPS vehicle tracking (VTS) device, shall determine its precise location through GIS based GPS System and transmit the same to the City Operation Centre at defined intervals of time. The location shall be displayed on GIS based route maps at City Operation centre</p> <p>The AVLS shall be able to give ETA at next bus stops in real time based on speed and distance measurement. The system shall update ETA at each bus stop on all PIS accordingly.</p> <p>The system shall be able to compare the actual location of the vehicle / bus, at any given time, with its scheduled location</p> <p>The system at the control rooms shall be able to calculate the time for the vehicle / bus to reach all subsequent stops along the route, factoring in the current vehicle / bus and any deviations from the schedule and reported traffic congestion enroute</p> <p>Shall provide inputs/feeds to Passenger Information System</p>

	(PIS) with the real-time data to be displayed at various display units and announcement systems
	Information elements that need to be captured and transmitted to City Operation Centre at the minimum include longitude, latitude, and physical location en-route with date and time stamps, vehicle / bus number, route number, and Driver ID, etc.
	Shall provide these data on real time basis at pre-determined and configurable intervals (10 seconds) over GPRS/GSM network
	Tracking of vehicle / buses that deviate from the scheduled route based on definition of permitted geographic regions of operation
	Vehicle Fleet Summary Dashboard – Quick view on vehicle fleet performance
	Register a vehicle / bus on unscheduled route from backend on real time basis
	Exception Recording/ Actions (Over-Speeding, Harsh Acceleration, Harsh Braking, Off route Detection, unscheduled stoppage, Non-Stoppage at Bus stops/collection points, Trip Cancellation).
	Real-time Running Trip Line diagram of vehicle / buses on a particular route, for headway detection.
	Applications Software shall have a facility to define the Masters New routes shall be created in the application.
	Business rules engine for fare stages, fare structures, various routes etc. shall be configurable.
	The facility shall be provided to collate the transactional data received from Depots and Bus Stations. The transaction data shall be uploaded once every day for the previous day.
	Officials shall be able to access the application as per the pre-defined roles and responsibilities
	The application shall provide facility to query the data and generate the customized reports as per the requirements.
	The system shall display the contact details of the bus driver / conductor so that the operation centre staff can communicate with them directly.
	The Operation Centre operator shall be able to drill down to the exact location of the event by clicking on the alert and see the position of event drawn over the map along with driver, vehicle and standard description of event details related to the business rule.
	The system be able to integrate with the City IOP/City Operations Platform with all the available data like Location , route information, Vehicle telemetry information, Speed etc.
	The system should allow programmability, allowing actions to be triggered based on events. e.g. speed metric can triggers API call to GIS Maps pulling speed limit on the road based on GPS or GTFS location.
	The platform should offer an Application builder for developing custom Applications as needed and also Should support an

		Interactive Development Environment that can facilitate in-house expertise to develop widgets and create API extensions
--	--	---

Fleet Management System – FMS

Sl. No	Nature of Requirement	Minimum Requirement Specification
1.	General Requirement	System shall have list of all the buses, routes, drivers & conductors available for duty allocation
		Provision to enter duty for driver, conductor and buses and shall be able to assign to all buses.
		It shall have provision to send SMS to respective driver and conductor about their duty.
		It shall have provision to create report for the vehicles available for duty, under maintenance and on casual duty to manage the fleet effectively
		It shall keep records of KM run of bus to monitor and plan the maintenance of the bus after certain run. The system shall have provision to set the KM manually in the system if required.
		Provision to alter driver and conductor duty in system and in such scenario immediate SMS shall go to driver and conductor about the change in their duty
		Should be able to integrate with Integrated Operation Platform for complete dashboard view

Functional Requirements for Mobile Data Terminal

1. The MDT should be affixed to the vehicle and should be able to interact with the control room by transmitting and receiving data through GPRS/3G/4G. The officers shall enter their details into it when they 'take over' duty. At this point they may also enter their IDs in order to record their attendance. The take-over shall include making appropriate text entries on the MDT of taking over of equipment, arms and ammunition, vehicle, fuel volume and kilometers on the odometer. For example, the staff shall indicate by input, the odometer reading of the vehicle and its location at the time of takeover. During the duty, the officer may change his status to meal break, tea break, available, attending to a Call for Service (CFS), etc.
2. The Dispatcher shall send CFS data to the Responding Units (RU) on its MDT and the Responding Units (RU) staff shall initiate the response by accepting the CFS on the MDT.
3. When instructed by the Computer Aided Dispatch (CAD), the MDT shall display graphical/ textual instructions to reach a location to respond to a CFS. It shall also work as a navigator and suggest the route(s). It shall also provide textual information to the RU about the CFS to be responded to. It shall

instruct the officer about the location to be adhered to as defined by the operations commander. There shall be several user-definable options for patrol charts i.e. a chart for week days, another for Sundays and holidays. The MDT shall also display relevant section of the map and display the location and status of other RUs. It shall show relevant layers when chosen. For example, it should show the location of police outposts, police stations, motor workshops, fuel stations, cinema halls, schools etc. The MDT should indicate the location where the RU has to locate itself if a contingency is declared.

4. It should be possible to transfer voice, multiple images and video from command centre to RUs and vice-versa.
5. The MDT should have a camera with video recording feature.
6. The vehicle mounted MDT should have integrated camera (with video) for recording the operations. e.g. pursuit driving operations. This is to avoid complex hardware integration and make officers job easy.
7. The MDT should have an audio recorder, which shall be used, among other applications, for recording and transmitting the Action Taken Reports (ATR), statement of informant, victim, injured, witness etc.
8. It should be possible for the RUs to propose entries into the GIS map from his MDT. These shall be vetted by the CAD administrator and after his approval shall become a part of the GIS map.
9. Some response units shall be outside the police department. e.g. fire services, private ambulances, cranes, salvage agencies. It should be possible to give them a client application for their mobile or desktop devices. These shall have very limited capabilities and access to the CAD.
10. There shall be multi-level security for all the devices remotely accessing the CAD. E.g. strong passwords, access to only predefined IPs, MAC numbers, etc.
11. The MDT shall also accept and transmit BOLO (Be On the Look Out).
12. It should be easily possible to install new software in future to expand the capability e.g. for service of summons, surveillance of criminals, courtesy calls to senior citizens, etc.
13. Standards of Ruggedness: The handheld MDT should adhere to MIL 810G and IP65. The vehicle mounted MDT should adhere MIL 810G and to IP65.

Features of MDT's

1. On screen keyboard with Punjabi, Hindi and English languages.
2. Daylight readable display: Daylight readability is one of the key prerequisites of this device as entire working is out of the office under open sky.
3. The screen of this device should be bright to ensure less human error during inputting data. (Especially while on the road in harsh environmental conditions.)

4. Latest technology: Along with embedded processing, latest windows / Android OS to give a lot of freedom for application development and deployment should be provided.
5. Remote update of OS and applications should be possible.
6. Rich and meaningful help files in Punjabi, Hindi and English should be available. Appropriate tool tips should also be available.
7. Voice recording should be possible.
8. Fully rugged as per MIL 810G & IP65.
9. The most important feature of a vehicle mounted device should be to sustain the vibration of the set up. The MDT along with the vehicle docking set up should be resistant to vibration & shock. It should ensure that any radio communication from the vehicle does not interfere with the computing device ensuring error free uptime for the solution.
10. This MDT would be installed in police patrol vehicles, is meant for in-vehicle use, and hence should be anchored to the vehicle for driver safety, device security, and user ergonomics. The MDT should follow specific installation protocols for proper ergonomics, power and communications functionality and would also include WAN modem, power-conditioning equipment, and WAN, WLAN, and GPS antenna for the vehicle.
11. Convertible feature: it should be possible to remove this device from the vehicle and use it as a Hand Held Mobile Rugged Tablet outside the vehicle as and when required, with built-in touch screen. This feature should provide versatility in terms of usage as the user can easily switch between standard vehicle mount and mobile tablet feature while on the move.
12. When used as a mobile tablet the battery should last for 6 to 8 hrs.
13. Whenever MDT is full charged, there should be a facility of Auto disconnect from charging till the battery level is 75%
14. High performance computing power & storage.
15. The device should be latest 3rd generation computing platform with high data storage capacity. This MDT should be a common platform for multiple computing applications and high compute power to ensure adequacy and scalability for future applications.

4.8 E-Governance

As part of e-governance services of Punjab, PMIDC is working on a common Mobile App and web services to enhance the existing G2C services all over the state. To achieve the same, following are the application components that are being developed for Municipal Corporations of Punjab.

1. Building Plan Management
2. Water & Sewage
 - New Connection
 - Disconnection
 - Billing
3. Property Tax- Assessment & Collection
4. Fire- License and NOCs
5. Trade Licenses
6. Compliances and Grievances for all utilities
7. Verification services
8. Birth & Death Certificate
9. State & ULB dashboards
10. Employee Payroll and Financial Accounts

MSI shall perform detailed requirement analysis for the components that shall be integrated with PMIDC common Mobile App including but not limited to the following for development of single app for citizens using the components of JICCC

- Smart Parking
- Solid waste management
- Integration of Jalandhar GIS map with PMIDC Mobile Application for location based complaints

4.9 Geographic Information System (GIS)

One of the goals of the smart city initiative is to create a single citizen interface where all data and applications are available on a GIS platform. An initial effort was conducted by Municipal Corporation to create the GIS database.

As part of smart city initiative, a separate RFP is being published for a full-fledged GIS infrastructure establishment and use the existing geodatabase with the following features:

- Use City level GIS platform, infrastructure & application as a foundation for Smart City solution, City Operation Centres & Command & Control Centres
- Build, implement & deploy city level GIS in short duration as an initial phase with immediate use for citizens and establish all the elements required for the list of components as per RFP
- Collaboration of various city stakeholders & departments together and to have a connect and engagement via a common GIS window for all operations
- Use GIS as spatial planning and analysis for various operation within city
- Use GIS as a Decision support system to prioritize actions
- To have a location based services to citizens of cities for better transparency & quick actions
- GIS based spatial and non-spatial queries for citizens and administrators and departmental stakeholders
- Provide administrators, citizens, tourists, businesses real time, and actionable information to aid their day-to-day decision-making

Existing layers of geospatial database:

TS Data Layers	Sec-1	Sec-2	Sec-3	Sec-4	Sec-5	Sec-6	Sec-7	Sec-8	Sec-9	Sec-10	Sec-11	Sec-12	Sec-13	Sec-14	Sec-15	Sec-16	Sec-17	Sec-18	Sec-19	Sec-20
Bank																				
Box																				
Bridges and Flyover																				
Bus Stand																				
Canal																				
Carriage Way																				
DGPS																				
Dispensary																				
Drainage																				
Dustbin																				
EB Poles																				
Electricity Poles																				
Electric Line																				
Fire Brigade																				
Footpath																				
Garbage Point																				
Hospital																				
Key Institutions																				
Land Marks																				
Mahholes																				
Mobile Towers																				
OFC																				
OHSR																				
Open Plot																				
Overhead Water Tank																				
Parks																				
Police Stations																				
Post Office																				
Railway Line																				
Road Centreline																				
School/College																				
Sector Boundary																				
Street Light																				
Telephone Poles																				
Temple Mosque																				
Tree																				
Toilet																				
Traffic Signals																				
Transformers																				
Vent Pipe																				
Water Tap																				
Zonal Office																				
Legend																				
Data/Layer Not Available																				
Available																				

Scope of work:

As part of this RFP, MSI shall study the integration requirements for the components mentioned below and integrate the components as applicable during the project tenure.

Objective:

Following are the objectives of GIS Integration.

1. GIS Map should be used as a common platform across all the solutions including Environmental, Sensors Monitoring, Intelligent Traffic Management, E-Governance, Utility Management system, Public Transport, Police Vehicles etc.
2. Appropriate geo referencing & geo tagging on the map should be done covering all relevant Smart elements in the RFP and various POI's such as public amenities, bus stops, bus routes, bin locations, transfer stations, street poles etc.
3. The component mapping should be multi layered keeping in vision the requirements for next 20 years.

4. GIS data modal need to be designed in accordance with Smart City solutions and need to be scalable and robust in nature so that it can meet any future need of smart solution and integration with future smart solutions and modules of city.
5. Alert, Events, Statuses for each smart element including hardware and software should be displayed on GIS Map.
6. The related Smart elements like Variable messaging system (VaMS) should also be displayed in the same layer for the application. Ex: Traffic Management, Environmental monitoring etc.
7. All government buildings and spaces should be geo tagged for the City of Jalandhar and shall be capable of data analytics based on GIS base map updates.
8. GIS data modal integrated should support domains, subtype, spatial rules and relationship, joins and spatial references etc.
9. GIS catalogue should be used to manage and maintain the GIS data modal. It must support database administration for user creation and management for GIS database.
10. **City Level GIS Portal:** GIS Web will include city portal for as a single window for accessing all the location based information. For more details, please refer e-governance section of RFP
11. Department specific search & query module should produce relevant output.
12. GIS maps must be integrated with GPS devices to locate real time position on GIS map & provide optimal route mapping.
13. SWM Assets mapping on GIS such as bins, transfer stations, landfill, garbage collection sites etc. Authority will provide SWM department related data.
14. There must be various analysis and work operations for Solid waste management from GIS application such as Geo fencing of waste bins, Geo fencing of vehicles, locate bins and bins location, signals, CCTV Surveillance cameras and provide planning & route optimization.

Indicative list of GIS based integration for City Analytics:

Component	Minimum GIS Analysis & Capabilities required as applicable
Solid Waste Management	<ul style="list-style-type: none"> ▪ The GIS system & Platform should support effective planning of schedules to better plan and service collection requirements. ▪ GIS system should support to reduce unwanted trips by optimal route planning leading to greater per vehicle productivity with full compliance to planned schedules. ▪ GIS system should enable identification of solid waste disposal sites

Component	Minimum GIS Analysis & Capabilities required as applicable
	<p>based on multiple criteria like slope, drainage, proximity to waterbodies, residential area etc. for efficient use of land and other natural resources within the city.</p> <ul style="list-style-type: none"> ▪ GIS system should give information to public about the date, time and other information of garbage collection area wise. ▪ GIS system must suggest the location for proposed bins in the city by GIS analytics for effective management of waste based on various factors such as populations, nearby hospitals and schools, areas that require cleaning etc. ▪ Web GIS system should support GIS based dashboards to showcase the results and information in the form of pie charts, bar charts, histograms, threshold bars, query ,highlight and selections etc.
Utility Water, Sewerage & storm water Network etc.	<ul style="list-style-type: none"> ▪ GIS system should be capable of modelling a water distribution network, mapping the location of Point of Sale, Isolation Trace of affected network area & customers, Illicit Discharge Trace, Service Qualification, optimize network routes to maximize revenue by considering locations, suggest alternate routing options and determine the impact on revenue streams, etc. ▪ GIS system should support designs creation for network expansions, Integration with SCADA, ERP systems, billing system, Metering system (smart meters), 3rd party Network Management systems for specific spatial analysis. ▪ The GIS system should be easily configurable to meet specific requirements like Network Isolation Trace, Service Qualification etc. without having to build them from scratch, and with the assurance of following best practices, and capable of extending based on requirements. ▪ GIS system must have operational dashboards that dynamically link to the water asset information's & gives the entire status of O&M. ▪ GIS system to perform the sewerage network tracing, Manhole inspection, Monitoring, Preventive maintenance, field crew navigation

Component	Minimum GIS Analysis & Capabilities required as applicable
	applications, field survey application and reports for repairs etc.
▪ Environmental Sensors / Air Quality Monitoring	<ul style="list-style-type: none"> ▪ GIS system should support to spatially map the air quality data, following statistical analysis to predict the values associated with spatial or spatiotemporal phenomena Primarily for environmental sensor reading analysis in order to decide if they pose a threat to environmental or human health and warrant remediation. ▪ GIS system should be capable of using proven deterministic methods of statistical Analysis to calculate unknown values of air quality: Inverse distance weighted, local polynomial, global polynomial, radial basis functions etc. ▪ The techniques should help to quantify the spatial autocorrelation among measured points and account for the spatial configuration of the sample points around the prediction location. ▪ GIS System should be capable to make a prediction— From the kriging weights for the measured values, calculate a prediction for the location with the unknown value. ▪ GIS system should be capable of accounting the error introduced by estimating the semivariogram model, by using many semivariogram models rather than a single semivariogram. ▪ It should be able to identify trends in the cluster of point densities to spatially locate the new, consecutive, intensifying, persistent, diminishing, sporadic, oscillating and historical hot and cold spots based on Getis-Ord Gi statistic P-Value & Z-Score for each feature in a dataset. ▪ GIS system based on the location analytics must find the areas that are causing the pollution like nearby industries and identifies the open green spaces where plantation can be improved for pollution reduction.
Provision for Property Tax and Land management	<ul style="list-style-type: none"> ▪ Property Tax /Land administration platform should seamlessly integrate with field operations and should securely connect to disparate

Component	Minimum GIS Analysis & Capabilities required as applicable
	<p>systems to maintain the integrity of survey data.</p> <ul style="list-style-type: none"> ▪ This GIS platform should support in creating and maintaining cadastral data and should streamline work processes and speeds the enrolment of new parcels including <ul style="list-style-type: none"> -Tax Parcel editing including the tools, workflow, topology, error checking, version management, and historic rollback that make mapping and public records tasks quick and easy. It should be able to identify GIS tax data errors based on set of rules and behaviours that model how points, lines, and polygons share coincident geometry. ▪ Support field data collection to collect data against a map or form-based data and integration with Enterprise cadastral system and track tax payment status per plot.
Routing, Intelligent Traffic System	<ul style="list-style-type: none"> ▪ It should help to maintain inventory of assets (roads, buildings, bridges etc.) along with asset details and condition data. ▪ It should support assigning and editing network features such as barriers, turns and unidirectional flow and should provide Multipoint routing ability. ▪ A network dataset is capable of modelling a single mode of transportation, 3D and Multimodal network datasets. ▪ The GIS system should help to track the location on real-time, in scheduling and determining the optimum number of vehicles required on the road, and optimal routing tools for multiple vehicles to reduce fuel consumption and therefore create a smaller carbon footprint. ▪ It should support to determine the best route assignment and order sequence. ▪ There should be analytics on the re-routing tools and the multimodal transportation system for moving point A to others by various communication methods like city bus, BRFTS, Metro etc. ▪ GIS system to highlight the passenger information system on the map that would be integrated with the PIS system of city bus. ▪ It should support to Store Coordinate Geometry Measurements to provide the results on a survey plan.

Component	Minimum GIS Analysis & Capabilities required as applicable
	<ul style="list-style-type: none"> ▪ It should support Linear referencing system to associate multiple sets of attributes to portions of linear features without requiring that underlying lines be segmented. ▪ System should support dynamic segmentation to compute the map locations of events stored and managed in an event table using a linear referencing measurement system and displaying them on a map. ▪ System should be able to identify the closest facility along the transportation network. ▪ System should be able to identify the suitable location based on maximising attendance, minimising impedance, maximum capacity or based on market share required to be covered.
Emergency Management Planning, Command centre control room operations	<ul style="list-style-type: none"> ▪ The Suite of applications should support preparation and response to emergency situations. ▪ To identify threats or current hazards, Define the impact to people and places, Plan, execute and monitor response activities, Communicate essential information to public etc. ▪ Leverage configurable applications to rapidly deploy decision support tools to simplify the implementation of data and maps to accurately determine potential impacts by fusing incident data with critical infrastructure, population densities, and other community values using spatial analysis tools like Flood Planning, Citizen Service Request, Impact Summary Map etc. to Support decision makers with dynamic and actionable information.
City Surveillance (Safety & Security Analysis)	<ul style="list-style-type: none"> ▪ City GIS must map CCTV cameras & integrate multiple sources of information, displays results on a map or satellite image, create a view shed area to visualize security camera coverage and plan the most efficient camera placement for security monitoring etc. ▪ It should support to analyse relationships between neighbourhood characteristics and incidents with respect to safety & security. ▪ It should be able to analyse the trend and represent the number of incidents that occurred in that area during a specific period, show the change in an area's incident rate etc.

Component	Minimum GIS Analysis & Capabilities required as applicable
	<ul style="list-style-type: none"> ▪ The system should provide a consistent method to measure concentrations of events over time by identifying trends in the cluster of point densities. To spatially locate the new, consecutive, intensifying, persistent, diminishing, sporadic, oscillating and historical hot and cold spots to identify areas with chronic problems and indicates the direction in which a particular incident may be shifting. ▪ GIS system must be capable of calculating the service area based on time and roads that need to block (Nakabandi) for catching thief's/criminals. ▪ GIS system must calculate and suggest the sites where police patrol vans are required based on the incident data to minimize the incident activities in the city. ▪ GIS System should be capable of maintaining data history, version management and conflict detection.

4.10 Helpdesk

a. City Operations Helpdesk

MSI shall provide the operational support for all the locations, through a suitable helpdesk system, to ensure that the solution is functioning as intended and that all problems associated with operation are resolved satisfactorily during the contract period. The MSI shall provide a web enabled helpdesk management system with SMS and email based alert system for the Helpdesk Call management and SLA reporting. MSI shall be required to setup a centralized helpdesk at the Jalandhar Integrated Command and Control Centre (JICCC).

MSI shall provision for the infrastructure necessary for managing the Help Desk including rent charges for Toll-free telephone line(s) at the Help Desk location. MSI shall provide multiple channels to log a complaint such as Toll-free lines, landlines, helpdesk tool, E-mail, direct walk-in etc. Outage of any component shall be calculated as a time between logging the call and closing the call.

A helpdesk is envisaged to be provided for the resolution of technical queries by internal users. Typical helpdesk activities (indicative) shall include, but not limited to:

1. Deployment of sufficient manpower to attend the helpdesk requests for extending technical support on hardware, network, application etc. to users
2. Deployment of web-based tool for the helpdesk
3. Provide Help Desk facility for agreed SLAs for reporting technical incidents / issues / problems with the system. Help desk facility shall be provided through Toll-free lines, landlines, helpdesk tool, E-mail, direct walk-in etc.
4. Implement a call logging system in line with the severity levels as per the SLAs. The Help desk shall log user calls related to system and assign an incident/ call ID number. Severity shall be assigned to each call as per the SLAs.
5. Track each incident / call to resolution.
6. Escalate the calls, to the appropriate levels, if necessary as per the escalation matrix agreed upon with Competent Authority/authorized entity
7. Analyse the incident / call statistics and provide monthly reports including but not limited to:
 - i. Type of incidents / calls logged
 - ii. Incidents / calls resolved
 - iii. Incidents / calls open
8. Helpdesk Solution shall further have the capability to upload frequently asked questions and solutions.

Helpdesk becomes the central collection point for service staff contact and control of the problem, change, and service management processes. This includes both incident management and service request management. This shall be the first level of support (L1).

It is also expected that a second level of centralized support (L2) shall also be maintained at the same location from where the various zones/wards can be serviced in case of problem escalation. If a problem is not resolved by telephone/help desk tool and the User declares the problem to be of an emergency nature, MSI shall dispatch a Field Service Staff member who shall provide On-site Support Service according to service levels given.

The Helpdesk shall act as a single point of contact for all users whether for service requests, incidents or problems. It shall encompass Helpdesk, Asset Management and Vendor Management. In addition, it shall offer a focused approach for delivering integrated Service Management and provide an interface for other functions in IT Services Continuity Management like Maintenance Contracts, Software Licenses etc.

MSI shall implement effective Helpdesk Management procedures to leverage the knowledge gained in providing faster and better solutions, create knowledge bases and prevent recurrence of problems.

Helpdesk Capacity

MSI is required to provide a minimum 8 seater helpdesk at Jalandhar Integrated Command and Control Centre (JICCC) during all operation hours as specified in the RFP. However, if the MSI believes that in order to meet the SLAs, additional capacity is required, the same may be provided by the MSI. It is also to be noted any supervisors required for the Helpdesk Operators shall be over and above the minimum operators mentioned

Shift Timings

Category	Shift	Type of Support	Type Support
Helpdesk at Integrated Command and Control Centre (JICCC) & (Police	Shift 1	On-premises	On-call
	Shift 2	On-premises	On-call
	Shift 3 (Night)	On-premises	On-call
Helpdesk at Jalandhar City	Shift 1	On-premises	On-call
	Shift 2	On-premises	On-call
	Shift 3 (Night)	On-Premises	On-call

The MSI shall operate the Central Helpdesk for the entire tenure of the Contract as follows:

Helpdesk Operators

The MSI is required to provide Operators at Helpdesk for operating and managing the Helpdesk as specified in this RFP. The Operators shall perform various activities including:

1. Understanding the query/issue in the reported request. Query could be related to the following:
2. Hardware including issues related to desktop/laptop, printer/multi-function device, local server, routers/switches

3. Application including login and password issues, accessing a particular module, navigation assistance, report generation assistance
4. Network including internet/intranet and end-user device connectivity
 - a. Providing information / clarification on the spot in case of an informational query or providing necessary troubleshooting assistance in case of a logged issue
 - b. In case of technical issues for which a resolution is not possible instantly, the operator shall submit the request into the system for escalation and further action by the MSI's team
 - c. Process all service requests, dispatch them to field personnel who shall perform the follow up

Field Support Staff

The MSI is required to provide Field Support Staff for undertaking all activities on field to complete a call logged by a User. MSI is expected to deploy enough number of Field Support Staff to ensure that SLAs as specified in the RFP are met.

IT / Non IT Infrastructure and application software for Helpdesk

The MSI shall be responsible for procurement, installation, commissioning and operations & maintenance of helpdesk including supply & installation of IT / Non IT infrastructure along with necessary application software (as per indicative BOM) required for the smooth functioning of the Central Helpdesk at both the location

b. Post Implementation Requirements:

Quality Assurance Plan

The Quality Assurance Management process will be implemented by the MSI in a structured and professional manner throughout various stages of the Project. It is intrinsically linked with the provision of safe and reliable systems since the application and control of applicable processes is the fundamental mitigation against systematic error. Achievement of ISO 9000 is the most common metric available to companies and an ISO 9001 compliant design methodology provides a high level of confidence that Quality Management is adequately implemented

System Configuration Management:

The system configuration management activity shall be carried out by the MSI and will comply with the principles depicted in the System Configuration Management Plan.

The MSI shall produce a System Configuration Management Plan to cover change control that occurs during the development phases and at the same time monitor the system configuration.

The System Configuration Management Plan shall address the configuration management in terms of configuration, change control, problem reporting, media control and appropriate configuration management tools.

Reliability Critical Items list should be made. Critical items are defined as System/Subsystem/Component, failures, which result into the highest disruption to service when ranked with other equipment in any system. This ranking will be based on the RAM (reliability, accessibility and manageability) analyses. Ranking severity will be considered for the number of instances, which would delay a service, due to the failure of the equipment. The length of the delay in any smart Jalandhar City schedule and the time taken to fix the failure would affect the criticality. The criticality of the item will also be based on the effect of that single item on the entire system.

The assessments include Failure Mode, Effects and Criticality Analysis (FMECA), Interface Hazard Analysis, Quantified Risk Analysis and quantitative analyses. It is recommended that the quantitative analyses be performed using Event Tree Analysis, Fault Tree Analysis or availability simulation modelling:

Class	Types of failures and incidents	Definitions
4	Significant	The failure leads to an incident that requires evacuation or immediate attention to people, while restoration of the operation could take a long time, or lead to a delay greater than 30 min.
3	Major	The failure leads to a disturbance of the operation with a significant loss of missions degrading regularity and “offered service”. A delay greater or equal to 3 min but less than 30 min is suffered.
2	Minor	The failure leads to a disturbance of the operation with a delay. A delay greater or equal to 1 min but less than 3 min is suffered.

1	Negligible	The failure has no immediate consequence on the pursuit of the missions but may lead to an intervention in corrective maintenance.
---	------------	--

Helpdesk/Contact Centre Solution

Automated Call Distribution Software

- ACD system (Hardware & Software) shall be provided in 1:1 Hot Standby configuration.
- The ACD system shall be able to handle call & IP Phone capacity defined.
- System should support skill base routing, multiple group support, priority handling and Queue status indicator. It is desirable that calls to certain trunk groups or to certain dialled numbers be assigned a higher priority than other calls and that calls which overflow from another split be queued ahead of other calls.
- System should support 50 (Fifty) call centre agents on a single server
- Single system should be able to administer 100 (hundred) agents
- Call overflow: The system should support call overflow routing e.g. if there is a queue in particular ACD group and another group is sitting idle, system should be able to transfer the calls to another group based on the settings defined by the administrator.
- Skill Assignment and Preference Levels: The proposed system must be able to assign individual skills to each call taker/agent (i.e. Bilingual, training or experience level, product knowledge, customer knowledge, etc.). Individually assigned skills must be able to be ranked and rated in terms of priority, proficiency or preference.
- Virtual Seating or Free Seating - The proposed system must support the concept of virtual seating. Call takers/agents can log-on from any "soft phone" instrument within the system. Call takers/agents on the proposed system will be logically defined, rather than requiring a "soft phone" extension and termination. Each Call taker/agent and supervisor on the system must have an individually assigned log-on identification number, which permits individual statistics to be collected by the ACD management information system. Multiple log-on events by the same individual during a work period at different terminals must be tracked individually as one "shift".
- The system should support assigning multiple skill sets (minimum 120) to an agent without degradation of the overall system capacity.
- Route calls to remote call centres based on agent skill availability.

- Prioritized call routing — It shall be possible to define Agent Preference options
- ACD System should be able to support integrated self-service applications.
- ACD System should be able to run defined workflow via HTTP request.
- In addition to the above, The ACD system should have the following features:
 - Expert Agent Selection (EAS)
 - Expert Agent Selection – Preference Handling Distribution (EAD-PHD)
 - Least Occupied Agent (LOA)
 - Reason Codes for AUX Work & Log-Off
 - Skill Level and Expert Agent Distribution
 - ISDN Network Call Redirection (NCR)
 - Service Observe of Logical Agent
 - Service Level Maximizer (SLM)
 - Forced Agent Logout from ACW
 - ASA (Average Speed of Answer) Routing
 - The offered voice system should have an integrated call centre functionality, both IP and non-IP and It should also support both IP and non-IP agents simultaneously
- The system should support load balancing of calls among multiple ACDs.
- The offered system should redirect unanswered calls.
- Offered system should support to provide the capability to the supervisors for logout agents from their own voice terminal without having to go to the agent's desk & it could be possible from a remote location.
- The proposed system should support a multisite call centre environment with multiple distinct sites as a single virtual call centre operation. It should also have a capability to allocated call between sites based upon agent skills, agent availability, queue times, and other criteria.
- The offered ACD system should be able to collect request information, such as a zip code or account code, before the call is sent to an agent and then route the call based upon that information.
- Proposed system could use the estimated wait time or average speed of answer to make routing decisions.
- The offered system should predict the estimated wait time for various split/skills and pick the best destination for a call to avoid excessive wait times and subsequent overflow. It should support predictive wait time routing
- Call routing program have a capability to connect the caller to an Interactive Voice Response (IVR) system while the call remains in queue for an agent. The incoming call should not lose its place in

queue when the call is routed to voice applications, audio text announcements, or other IVR applications.

- The system should promote agent fairness relative to equitable agent call distribution for multi-skilled agents. The system should be able to distribute calls to agents based on ACD work occupancy instead of most idle or longest current idle time.
- Both agents and supervisors should be notified via the telephone indicators when thresholds are reached for individuals and groups.
- The offered system should have a capability for agents to record personalized greetings that can be played to the caller prior to connection to the agent.
- The offered system should support for service level call routing. Like for each call type in terms of “answer X% of this type of calls within Y seconds” and will your ACD routing algorithms use our specified X & Y service level factors to route and deliver specific calls accordingly to meet the specified objectives.

CTI - Computer Telephony Integration Software

- The CTI shall be provided with 1:1 Hot Standby configuration to avoid any single point of failure.
- The CTI system shall be able to handle call & IP Phone capacity defined above.
- The CTI platform shall be able to provide the caller's CLI information. It shall be possible to send & populate agent's PC with CLI information.
- The offered CTI platform shall support a set of APIs.
- The CTI link shall be able to pass events and information of agent states and changes in agent states as well as incoming calls to the computer applications, e.g., if the customer calls from the same no. from which he had called earlier (registered/unregistered), the CTI platform shall be able to automatically fetch and display at least last 5 service requests details for that customer.
- The CTI shall maintain the accounting and authorization logs of the users accessing the components of the telephony system. The logs shall include information users who have logged-in into the system and the specific commands entered by them.
- It shall have web-based GUI console for administration, configuration & management of the system, Real-time information/alerts and reports regarding health status e.g. up/down status, performance & resource utilization statistics etc. of the system shall be available through this console.

Voice Recording System for Agent Calls - Softphone Software

Recording:

- The call recording solution (Hardware & Software) shall be provided in hot standby configuration.
- The solution must be able to record IP phone communication via the LAN, without employing a passive or active IP sniffing on the network.
- The recording solution must provide a single universal license that can support recording on all phones including analog phone, digital phone, IP phone, IP soft-phone.
- The solution must be able to record encrypted IP phone communication via the LAN.
- The solution should also be able to record IP, Digital & analog endpoints
- Should record inbound ACD calls and outbound dialler calls.
- Should be able to support Master-Slave configuration in case of large deployments
- support for Centralized or decentralized search and replay of calls
- "Tag" or classify calls with user-defined labels for simplified search and replay

Quality Recording:

- The solution shall provide scalable screen recording.
- The solution should allow for voice only, data only, or voice and data recording based on specific event triggers.
- The solution should support selective recording based upon user-defined business rules
- The solution should have the capability to record based on a particular schedule (for example, record all calls on Tuesday from 9:00 - 11:00 AM for agent XYZ).
- The system should show the status of the agents; which agents are logged on.
- The solution should allow for the automatic refresh of the logged on agent display.
- The solution should be able to provide real-time agent monitoring.
- The solution should provide an optional desktop application to allow agents to initiate and /or terminate recording (Record on Demand)
- System should support Rules-based recording

Reporting:

- Standard out-of-the-box reports generation should be possible.
- The system should be able to customize the reports
- The reporting system shall be part of an industry standard platform, or it should be a propriety product.

- Reports should be scheduled for automatic delivery to email or a file directory.
- Both text and graph reports shall be offered.

Evaluation of Agents (scoring)

- This should include adding questions, changing weightings and changing values.
- Evaluate multimedia calls and application use
- The solution should allow the user to create, without vendor customization, multiple grading templates using questions provided by the user.
- The solution should have the capability of inserting notes on a per-question basis and a summary note into the grading form.
- Easy to create evaluation forms
- Recording supported for wide range of contact centre needs including inbound and outbound calls, phone, email and web chat
- The solution should produce scorecards with multiple Key Performance Indicators (KPIs).
- The solution should be able to show trends based on historical performance.
- Individual scorecards should give an overview of individual agent performance, supervisor group performance, manager's group's performance, overall contact centre(s) performance and enterprise contact centre performance.

Analytics:

- It should be able to integrate other forms of metadata.
- The system should be able to be extended to include additional metadata.
- The data should be stored in an industry standard, non-proprietary format.
- It should support encrypted audio.

IP Phone - Softphone Software

- The IP phones should be of the same make as that of IP PBX supplied by the bidder.
- The IP Phone shall have an interactive and user-friendly alphanumeric display to make use of the key phone very simple.
- The IP Phones shall support connection of Headset.
- The IP Phone shall have LED/LCD Indicator for Call Waiting and Message Waiting.
- It shall be possible to set preferences such as Display Contrast and Ring Types.

Voice Broadcasting Software.

This may be the integral part of CAD software or Master System Integrator (MSI) may purchase the separate tool as per the below mentioned requirement and later integrate with CAD solution

Broadcasting (BOLOs)	
1	BOLOs should be sent to: <ul style="list-style-type: none"> ▪ Any CAD workstation/terminal ▪ Any personnel by name ▪ Groups of personnel by name, unit and/or terminal ▪ All units on a specified event ▪ Combinations of the above
2	Should have ability to associate a BOLO to an Event number
3	Should have association of the BOLO to an Event number results in the automatic population of the location information in the Broadcast dialog
4	Should have ability to associate a BOLO to a case number
5	BOLOs should be created without relating to an event
6	Should have ability to create a Broadcast (BOLO) in association with an event and place the event in a Held status in one function

Telephony System (IP PBX System and Gateway) - Answering Service Software

- It should be possible for the IP phone to be connected on the same line which is connected to the computer i.e. Single wire to desk.
- The system software version offered should be the latest release as on the date of supply of EPABX as available globally.
- The call processing, Signalling & networking components of the offered system shall be based on open standards.
- The system architecture should allow for incremental application additions to the enterprise without modification to existing feature server software
- The PBX shall be provided in 1:1 Hot Standby mode to avoid any single point of failure. The PBX servers shall work in 1:1 Hot standby configuration in such a manner that if one server fails the second server is able to take the complete load of calls automatically (without any manual intervention) without dropping any existing calls (IP, TDM & PRI).
- The PBX and gateway shall be rack mountable.
- The system shall allow outbound calling from the IP Phones.
- The system shall support local announcements and music on hold.
- The software shall provide GUI based interface for configuration and management of the system.

- The system shall maintain the accounting and authorization logs of the users accessing the components of the telephony system. The logs shall include information about users who have login into the system and the specific commands entered by them.
- It shall be possible to schedule tasks. The tasks could be one or more operations that the user can specify to run at a predetermined date and time.
- It shall provide reports about station alarms, trunk analysis, processor occupancy, system capacity etc.

Helpdesk/Contact Centre Executive/User/Operator System

Sl. No.	Minimum Specifications
1	It should provide consistent user interface across multiple media types like fax, SMS, telephone, email, and web call back.
2	The executive's desktop should have a "soft-phone" – an application that enables standard telephony functions through a GUI.
3	It should provide the executives with a help-desk functionality to guide them to answer a specific query intelligently.
4	It should also provide an easy access to executives to previous similar query which was answered successfully.
5	It should also be possible to identify a request to be a similar request made earlier.
6	It should be possible for executives to mark a query as complex/typical and put in to database for future reference by other agents.
7	It should be possible for executives to escalate the query.
8	System should be able to integrate with e-mail / SMS gateway so that appropriate messages can be sent to the relevant stakeholders after the interaction and any updates thereon.
9	Should intelligently and automatically responds to email inquiries or routes inquires with skills based routing discipline to agents.

5 Annexure - Project Implementation Timelines, Deliverables and Payment Schedule

a) Project Implementation Timelines

The implementation timelines for the project components are as given below.

Sl. No.	Phase	Timeline
1	Issuance of Letter of Intent	A
2	Submission of Performance Bank Guarantee	A + 30 days
3	Signing of Contract with MSI	A + 30 days = T
4	Completion of Project Inception Phase incl. Mobilization of Team	T + 1 month
5	Completion of Requirement Phase, including Feasibility Study and Site Survey	T + 3 months
6	Completion of Design Phase & Report	T + 5 months
7	Installation of HW/Infrastructure, SW Phase & Report	T + 9 months
8	Completion of Integration	T + 10 months
9	UAT, FAT, STQC, etc.	T + 11 months
10	Go -Live (G)	T + 12 months = G
11	Operation & Maintenance	G + 4 years

b) Project Deliverables

S.No	Milestone	Deliverables	Timelines (in months)
	Phase I	Project Panning	T+1 months
1	Project Planning	1. Detailed Project Plan 2. Survey and Detailed Design of all the solutions components 3. Design Approvals 4. Required Civil Infrastructure Plan & Approval	T+1 months
	Phase II	Project Implementation	T+10 months
2	Delivery Of BOM	1. All the BOM mentioned hardware and soft wares should be procured and delivered 2. Stock Entry of Hardware and Verification of Hardware by JSCL.	T+5 months
3	Implementation completion	1. Weekly and Monthly Progress Reports 2. Hardware Installation and configuration	T+10 months

		<ol style="list-style-type: none"> 3. Software Development 4. Pilot Deployment 5. Prototype Acceptance and Factory Acceptance Testing 6. Final Deployment and Documentation 7. System Integration. 8. Testing-Performance, Scalability, Systems Integration, Stress Testing, Security Testing, Systems Acceptance Test, etc. 9. Develop Training Materials 	
	Phase III	Acceptance Testing & Go-Live	T+12 months
4	Testing & Go-Live	<ol style="list-style-type: none"> 1. User Acceptance testing 2. Final Acceptance Testing 3. Training & Change Management 4. User Training 5. Mobilization of required staff 6. Operational System Acceptance 7. JICCC, DC, DR certifications Go-Live 	T+12 months
	Phase IV	Operations & Maintenance Phase	T+48 months
5	Operations & maintenance	<p>MSI has to follow the SLA's defined during the maintenance phase. MSI will be solely responsible for the deliverables. SLA Compliance Reports, Audits</p> <p>Note: The following table with mile stones is indicative. MSI can have a separate plan in the interest of completing the project in time. For details of deliverables please refer to Project Management section in this document.</p>	T+48 months

c) Payment Schedule

S. No.	Scope of Work	Timelines	Payment

1	Phase I Project Planning	T1= T + 1 Months	5% of CAPEX value against Bank guarantee or equivalent
2	Phase II Implementation- Delivery of entire BoM	T2= T1 + 5 months	20% of CAPEX value on delivery of hardware
3	Phase II Implementation- completion	T3= T1 + 10 Months	25% of CAPEX value on the commissioning of hardware
4	Phase III Acceptance Testing & Go-live	T1 = T + 12 months	26% of CAPEX value
5	Operations & Maintenance phase for a period of 48 months from the date of Go Live of the last solution	T1 + 48 Months	Equal quarterly instalments (1.5%) of Capex and 6.5% of OPEX quoted value

Note:

- a. The request for payment shall be made to the AUTHORITY in writing, accompanied by invoices describing, as appropriate, the services performed, and by the required documents submitted pursuant to general conditions of the contract and upon fulfilment of all the obligations stipulated in the Contract.
- b. Due payments shall be made promptly by the AUTHORITY, generally within 60 (Sixty) days after submission of an invoice or request for payment by MSI after Approval & Sign Off of the Milestone by AUTHORITY.
- c. The currency or currencies in which payments shall be made to the MSI under this Contract shall be Indian Rupees (INR) only.
- d. All remittance charges shall be borne by the MSI.
- e. In case of disputed items, the disputed amount shall be withheld and shall be paid only after settlement of the dispute.
- f. Any penalties/ liquidated damages, as applicable, for delay and non-performance, as mentioned in this RFP document, shall be deducted from the due payments of the respective milestones.
- g. Taxes, as applicable, shall be deducted / paid, as per the prevalent rules and regulations
- h. The above payment milestones shall be deemed to be achieved upon sign-off of relevant and respective deliverables by the Authority or its appointed agencies.

6 Annexure –Bill of Materials

The list of items mentioned hereunder is indicative. The Bidder shall consider the components and quantity to fulfil the RFP and project requirements in totality.

a. Integrated Command & Control Centre (ICCC) and Data Centre (DC)

Sl. No	Particulars	Unit	Qty
A	ICMCC - Hardware		
1	Video Wall (DLP LED)- Main Control Room (7 X 3) Cube - 50" each	Nos	21
2	3-Screen Operator Workstation	Nos	4
3	2-Screen Operator Workstation	Nos	8
4	1-Screen Operator Workstation	Nos	20
5	Laptop - Core i7	Nos	12
6	Keyboard Joystick	Nos	4
7	High End Network Printers (MFC)	Nos	1
8	Projector for Meeting Rooms with Screen	Nos	2
9	Multi-Functional Printer	Nos	5
10	I.P. Phones	Nos	40
12	Video Conferencing Solution	Set	1
13	Rack - 42U (Intelligent Rack)	Nos	2
14	Rack Servers (Appl - 8, Analytics -2, NMS & Network -2, DHCP - 1, DB Server -1 , ASA-2, Syslog - 1, Antivirus-1, Security -2)	Nos	23
15	SAN Switch 24 port	Nos	2
16	Secondary storage – Tape drive – 30 days	Nos	1
17	LTO 7 Tapes - 6 TB	Nos	250
18	SAN Storage (2 PB)	Nos	1
19	Leaf Switch	Nos	4
20	Fabric Controller	Nos	1
21	Spine Switch	Nos	2
24	Core Router	Nos	2
25	Internet Router	Nos	2
26	Distribution Switch	Nos	4
27	L3/Core Switch	Nos	2

28	L2 Switch (48 ports)	Nos	2
29	Internal & External Firewall (IPS (Intrusion Prevention System) /IDS (Intrusion Detection System)	Nos	2
30	Advanced Malware Sandboxing	Nos	1
31	Server Load Balancer+ Link Load Balancer(LLB)+ Web Application Firewall(WAF) Appliance+DDOS	Nos	2
32	Network Behavior Analysis System	Nos	1
33	Network Access Control & Authentication	Nos	1
34	Web Security System (URL Filtering/Caching)	Nos	2
35	24 Core rack mounted LIU with all accessories including fibre, patch card etc.	Nos	1
36	48 Core rack mounted LIU with all accessories including fibre, patch card etc.	Nos	1
37	Fire Alarm & Suppression System for entire ICMCC	Lump sum	1
38	Rodent Repellent System for entire ICMCC	Lump sum	1
39	Desktop PC for Network Room	Nos	2
41	IP Based MFP Printer for Network Room	Nos	1
42	Printers and scanners for ICMCC	Set	1
43	Biometric Access Control System	Nos	6
44	Consumables	Lump Sum	
45	Electricity Connection	Lump sum	
46	Electricity Charges	Lump Sum	
47	False ceiling & Lighting cost	Lump Sum	
48	Lan Cabling and any other passive components.	Lump Sum	
49	Diesel Charges	Lump Sum	
50	ICCC Furniture Cost	Lump Sum	1
TOTAL			
B	ICMCC - Software		
1	Video Wall Controller & Application	Nos	1
2	Video Management Software	Nos	1

3	ICCC+ City Operations Platform (IoT)	Nos	1
4	Integrated Mobile Application for all PAN City Components	Nos	1
5	Anti-Virus Software and HIPS for ICMCC	Lot	23
6	Antivirus Software and HIPS for all physical servers	Nos	23
7	Server OS	Nos	23
8	Enterprise Management System (EMS) Software + Helpdesk	Nos	1
9	RDBMS	Nos	2
10	Integration Bus	Nos	1
11	API Gateway	Nos	1
12	Backup software	Nos	1
13	Identity and Access Management	Nos	1
14	Virtualization Software Licenses for 4 Physical Servers with two CPU each	Nos	40
15	Integration of PAN City Components	Lump sum	1
16	DR Management Software	Nos	1
17	SMS Gateway	Nos	1
18	Disaster Management Application (Natural disaster)	Nos	1
19	Building Management software	Nos	1
TOTAL			
C	Internet Bandwidth at ICMCC, DC, Helpdesk, Viewing Centre		
1	Internet Bandwidth at ICMCC	Lump sum	1
2	DC to DR P2P Link (100 MBPS)	Lump sum	1
3	Fiber LAN Connectivity between ICCC & Viewing Centres (1 GBit) incl. switches and repeaters	Lump sum	3
D	Non It- Hardware		
1	Internal Surveillance System (CCTV)	Lump sum	1
3	Site Preparation Cost	Lot	1
4	Air conditioning (Duct AC for JICCC)	Nos	1
5	Diesel Genset - 250 KVA	Nos	1
6	Online UPS - 60 KVA (Minimum) with battery	Nos	2
7	Hand Set	No.	10
8	IVRS Server	No.	1
9	CTI Server	No.	1
10	Automatic Call Distributor Server	No.	1
11	Dialer	No.	1
12	Voice Logger	No.	1
13	IP PBX	No.	1

E	Non It- Software		
1	Automated Call Distribution Software	Lot	1
2	Computer Telephony Integration Software	Lot	1
3	Answering Service Software	Lot	1
4	Interactive Voice Response Software	Lot	1
5	Softphone Software	Lot	1
6	Voice Broadcasting Software	Lot	1
7	Server Operating System	No.	1
8	Integration with e-Governance mobile applications by PMIDC	Lump sum	1

b. Intelligent Traffic Signalling System

SI. No	Particulars	Unit	Qty
A	Traffic Junctions Components		
1	Adaptive Traffic Control System (ATCS) Compatible Controller	Nos	9
2	ATCC	Nos	2
3	Countdown timer (EN Certified)	Set	44
4	Galvanized Cantilever Poles	Nos	44
5	Galvanized Standard Poles	Nos	20
6	Galvanized Gantry Poles	Nos	4
7	Traffic Light Aspects	Nos	11
8	Junction Box/Cabinets	Nos	11
9	Access Switch (24 port)	Nos	11
10	RLVD	Nos	44
11	ANPR	Nos	102
12	SVDS	Nos	2
13	Public Address System	Nos	25
14	Emergency Call Box	Nos	5
15	ANPR LPU	Nos	102
16	E-Challan Hand held devices	Nos	50
B	Support Accessories		
1	UPS, Battery (1 KVA)	Nos	11
2	SITC (System Installation, Testing & Commissioning)	Nos	11
3	Earthing	Nos	11
4	Rugged Enclosure (for Switch, UPS etc.)	Nos	11
5	Electricity Meter with rugged enclosure	Nos	11
C	Software System		
1	ATCS Software	License	1
2	E-Challan Application and Integration	Bundled	1
3	ATCC	Nos	1
4	ANPR software	Nos	1

D	Site Related		
1	Civil Work	Nos	11

c. CCTV Surveillance

SI. No	Particulars	Unit	Qty
A	CCTV Surveillance Systems		
1	PTZ Camera with IR Facility	Nos	15
2	Fix Box cameras	Nos	981
3	Bullet Cameras	Nos	50
4	Face Recognition cameras	Nos	10
B	Support Accessories		
1	Poles for PTZ Cameras	Nos	15
3	Straight Poles	Nos	981
4	UPS (1 KVA)	Nos	183
5	Rugged Enclosure (for Switch, UPS etc.)	Nos	183
6	Electricity Meter with rugged enclosure	Nos	183
7	Site Preparation (including electrical wiring, digging, UTP, Power Cabling, furnishing, Installation etc.)	Lump sum	183
8	POE+ Switch 16 Port	Nos	183
C	Software System		
1	Video Analytics Software	Nos	1
2	Face Recognition System	Lump sum	1
3	NERS & CCTNS Integration including Connectivity	Lump sum	1

d. Network Backbone

SI. No	Particulars	Unit	Qty
1	MPLS Link in ring topology for Cameras deployed at different locations in City for 1200 cameras (4GBPS)	Lump sum	1

e. Disaster Recovery (DR)

SI. No	Particulars	Unit	Qty
A	System Software		
1	Server OS	Lump sum	1

2	RDBMS	Lump sum	1
3	Virtualization Software	Lump sum	1
B	Cloud		
1	DR (VMs, Storage, Network) - 5 years	Lump sum	1
C	DR setup		
1	Installation and configuration	Lump sum	1

f. Viewing Centres

SI. No	Particulars	Unit	Qty
A	Satellite - IT Infrastructure		
1	LED Screen - 60"	Nos	3
2	Workstation Desktop with OS	Nos	3
3	LAN Switch	Nos	3
B	Support System		
1	Site Preparation (Electrical, LAN Cabling, Earthing, Minor refurbishments, Installation, etc.)	Nos	3
2	UPS	Nos	3

g. Variable Messaging System

SI. No	Particulars	Unit	Qty
A			
1	VMS board	Nos	25
	VMS controller	Nos	25
2	Mounting structure for VMS	Lump sum	25
3	Electricity	Lump sum	25
4	VMS Application	Nos	1
5	VMS Cabinet IP 65 Compliant	Nos	25
6	Site Preparation (Power, Meter, UPS, Fitment Components, Installation etc.)	Nos	25

h. Emergency Response System

SI. No	Particulars	Unit	Qty
A	Hardware for Vehicles		
1	Vehicle Tracking Unit	Nos	49
2	Mobile Data Terminal	Nos	49
3	Installation & Configuration	Nos	49

i. Environment Sensors

SI. No	Particulars	Unit	Qty
1	Environmental Sensors + Application	Nos	5
2	Multi-Color LED Board	Nos	5
3	Site Preparation (Power, Meter, UPS, Fitment Components Installation etc.)	Nos	5

j. Body Cameras

SI. No	Particulars	Unit	Qty
1	Body Cameras	Nos	20
2	Body Camera Software	Nos	1
3	Body Cameras Docking station	Nos	1