PUDUCHERRY SMART CITY DEVELOPMENT LIMITED

# REQUEST FOR PROPOSAL FOR SELECTION OF SYSTEMINTEGRATOR FOR DESIGN, DEVELOPMENT, SITC, O&M FOR 05 YEARS OF INTEGRATED COMMAND & CONTROL CENTER(ICCC) & OTHER ASSOCIATED ACTIVITIES FOR PUDUCHERRY SMART CITY AREA

## VOLUME 2 – SCOPE, FUNCTIONAL & TECHNICAL SPECIFICATION

**Original RFP NO: RCIL-2023-PDY-Smart City-RFP-01 DATED: 01.06.2023**
**Corrigendum: RCIL-2023-PDY-Smart City-RFP-01 (Modified) Dated 27-07-2023**

Table of Contents

## 1 Disclaimer

The information contained in this Request for Proposal document ("RFP") whether subsequently provided to the bidders, ("Bidder/s") verbally or in documentary form by RailTel Corporation of India Limited (henceforth referred to as "RailTel" in this document) or any of its employees or advisors, is provided to Bidders on the terms and conditions set out in this Tender document and any other terms and conditions subject to which such information is provided.

This RFP is not an agreement and is not an offer or invitation to any party. The purpose of this RFP is to provide the Bidders or any other person with information to assist the formulation of their financial offers ("Bid"). This RFP includes statements, which reflect various assumptions and assessments arrived at by RailTel in relation to this scope. This Tender document does not purport to contain all the information each Bidder may require. This Tender document may not be appropriate for all persons, and it is not possible for RailTel and their employees or advisors to consider the objectives, technical expertise and particular needs of each Bidder. The assumptions, assessments, statements and information contained in the Bid documents, may not be complete, accurate, adequate or correct. Each Bidder must therefore conduct its own analysis of the information contained in this RFP and to seek its own professional advice from appropriate sources.

Information provided in this Tender document to the Bidder is on a wide range of matters, some of which may depend upon interpretation of law. The information given is not intended to be an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law. RailTel accepts no responsibility for the accuracy or otherwise for any interpretation of opinion on law expressed herein.

RailTel and their employees and advisors make no representation or warranty and shall incur no liability to any person, including the Bidder under law, statute, rules or regulations or tort, the principles of restitution or unjust enrichment or otherwise for any loss, cost, expense or damage which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, reliability or completeness of the RFP, and any assessment, assumption, statement or information contained therein or deemed to form part of this RFP or arising in any way in this Selection Process.

RailTel also accepts no liability of any nature whether resulting from negligence or otherwise howsoever caused arising from reliance of any Bidder upon the statements contained in this RFP. RailTel may in its absolute discretion, but without being under any obligation to do so, can amend or supplement the information in this RFP.

The issue of this Tender document does not imply that RailTel is bound to select a Bidder or to appoint the Selected Bidder (as defined hereinafter), for implementation and RailTel reserves the right to reject all or any of the Bidders or Bids without assigning any reason whatsoever.

The Bidder shall bear all its costs associated with or relating to the preparation and submission of its Bid including but not limited to preparation, copying, postage, delivery fees, expenses associated with any demonstrations or presentations which may be required by RailTel or any other costs incurred in connection with or relating to its Bid. All such costs and expenses will remain with the Bidder and RailTel shall not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by a Bidder in preparation for submission of the Bid, regardless of the conduct or outcome of the Selection process.

## 2 Definitions and Acronyms

| Terms | Acronyms |
|---|---|
| AAA | Authentication, Authorization, Accounting |
| ABD | Area Based Development |
| AI | Artificial Intelligence |
| AMC | Annual Maintenance Contract |
| AP | Access Points |
| API | Application Programming Interface |
| AQM | Air Quality Monitoring |
| ANPR | Automatic Number Plate Recognition |
| ATCS | Adaptive Traffic Control System |
| BOM | Bill of Material |
| BEC | Bidders Evaluation Committee |
| BG | Bank Guarantee |
| CC | Capital Cost |
| CCTV | Closed Circuit Television |
| CEO | Chief Executive Officer |
| CPU | Central Processing Unit |
| CSP | Cloud Service Provider |
| DB | Data Base |
| DC | Data Centre |
| DD | Demand Draft |
| DG | Diesel Generator |
| DR | Disaster Recovery |
| DRDM | Department of Revenue and Disaster Management |
| DWC | Double Wall Corrugated |
| ECB | Emergency Call Box |
| EMD | Earnest Money Deposit |
| EMS | Element Management System |
| FAT | Factory Acceptance Test |
| FMS | Facility Management Services |
| GIS | Geographical Information Systems |
| GI | Galvanized Iron |
| GPS | Global Positioning System |
| GST | Goods and Services Tax |
| PSCDL | Puducherry Smart City Development Limited |
| HDD | Horizontal Drilling |
| HDPE | High Density Polyethylene |
| HOD | Head of Department |
| ICCC | Integrated Control and Command Center |
| ICT | Information and Communication Technology |
| IOT | Internet of Things |
| IP | Internet Protocol |
| ISP | Internet Service Provider |
| IT | Information Technology |
| ITMS | Integrated Traffic Management System |
| INR | Indian Rupee |
| IVR | Interactive Voice Response System |
| KPI | Key Performance Indicator |
| LOA | Letter of Acceptance or Letter of Award |

| Terms | Acronyms |
|---|---|
| LAN | Local Area Network |
| LoI | Letter of Intent |

| Terms | Meaning |
|---|---|
| MoU | Memorandum of Understanding |
| MOUD | Ministry of Urban Development, GOI |
| SI | Master System Integrator |
| NPV | Net Present Value |
| NPW | Net Project Worth |
| OEM | Original Equipment Manufacture |
| O&M | Operations & Maintenance |
| OFC | Optical Fiber Cable |
| PA | Public Address |
| PAS | Public Address System |
| PAT | Prototype Acceptance Test |
| PABX | Private Automatic Branch Exchange |
| PBG | Performance Bank Guarantee |
| PDD | Proposal Due Date |
| PDU | Power Distribution System |
| POA | Power of Attorney |
| PoC | Proof of Concept |
| PoE | Power over Ethernet |
| PoP | Point of Presence |
| PQ | Pre-Qualification |
| PTZ | Pan Tilt Zoom |
| PV | Present Value |
| PWD | Public Work Department |
| QCBS | Quality cum Cost Based Selection |
| RFP | Request for Proposal |
| RLVD | Red Light Violation Detection |
| ROW | Right of way |
| RI | Right to Inspect |
| SCM | Smart Cities Mission |
| SCP | Smart City Proposal |
| SI | System Integrator |
| SITC | Supply Installation Testing Commissioning |
| SLA | Service Level Agreement |
| SOP | Standard Operating Procedures |
| SVD | Speed Violation Detection |
| SSD | Solid State Drive |
| TOR | Top of the Rack |
| TQ | Technical Qualification |
| TRV | Total Revenue |
| UAT | User Acceptance Testing |
| UPS | Uninterrupted Power Supply |
| VA | Video Analytics |
| VAPT | Vulnerability Assessment and Penetration Testing |
| VM | Virtual Machine |
| VMD | Variable Message Display |
| VMS | Video Management System |

**Definitions**

| Term | Definition |
|---|---|
| Client | DRDM / PSCDL |
| MSI cum PMC /Authority/ Tender Inviting Authority | RailTel Corporation of India Ltd |
| System Integrator | Selected Bidder with whom the contract agreement is signed against this RFP. |

# 3 Overview

## 3.1 Introduction

Puducherry, formerly known as Pondicherry, gained its significance as "The French Riviera of the East" after the advent of the French colonialization in India. Puducherry is the Tamil interpretation of "new town" and mainly arrived from "Poduke", the name of the marketplace as the "Port town" for Roman trading, way back in 1st century as mentioned in the 'The Periplus of the Erythraean Sea'. The settlement was once an abode of many learned scholars as evidently versed in the Vedas, hence also known as Vedapuri.

Puducherry Smart City Participated in the Government of India Launched Smart City Mission challenge in which Puducherry City was qualified as Smart City in 3rd round of Smart city Challenge keeping The Vision is to **"Transforming Puducherry into a global tourism destination byleveraging its heritage, cultural, spiritual, and educational advantages. Enhance the quality of life of the citizens by providing efficient urban mobility, smart civic infrastructure, smart service delivery and participative decision making."**

## 3.2 Vision

Transforming Puducherry into a global tourism destination by leveraging its heritage, cultural, spiritual, and educational advantages. Enhance the quality of life of the citizens by providing efficient urban mobility, smart civic infrastructure, smart service delivery and participative decision making."

Based on the above formulated vision, Smart City Proposal was focused on the following

opportunities and Challenges:

a) Livelihood Opportunities Through Promotion of Tourism

b) Protection of Heritage and Preservation of the Unique Features of the City

c) Urban Poverty Alleviation through Affordable Housing

d) Urban Mobility, Traffic Decongestion and Safety & Security of Citizens

e) Better Delivery of Citizen Services with accountability

## 3.3 Project Background

The vision of Puducherry Smart City is to drive citizen centricity through improvements in City Operations, improve efficiency of municipal services and promote a better quality of life for residents. In order to achieve these Puducherry Smart City Development Limited desires to foster the development of a robust ICT infrastructure that supports digital applications and ensures seamless oversight of city-wide operations.

The key objective of this project is to establish a collaborative framework where input from different functional departments of Puducherry Municipal Corporation and other stakeholders such as transport, fire, police, e-governance, etc. can be assimilated and analyzed on a single platform; consequently, resulting in aggregated city level information. Further, this can be

converted to actionable intelligence, which would be propagated to relevant stakeholders and citizens.

Puducherry Smart City Development Limited (PSCDL) has entrusted implementation of works to the Department of Revenue and Disaster Management (DRDM), Puducherry. The DRDM has engaged RailTel as MSI-cum-PMC for the implementation of the project who will float tender, finalize tender with the approval of DRDM/PSCDL and execute the work under the Smart City mission which will include ICCC and Smart Elements like, Intelligent Traffic Management System, City Surveillance, Smart Poles, Smart Kiosk, Environmental sensors, Variable Message Display, Public Address System, Public Wi-Fi, OFC Network, Incident Management and Urban Flood Plain Management.

## 3.4 Objective of the Project and RFP

### 3.4.1 Objective of the Project

a) The DC & DR will be connected with various city level ICCCs and various applications of the city from where feeds are to be received (except video feeds). It will host command center application platform for all Smart City projects. It will also host other common applications like integrated analytical layer / BI engine. Eventually all the smart components / applications deployed in the cities will be integrated with the common platform layer for managing smart city operations using the Open Application Programmable Interface (API) Structure.

b) ICCC is required to be scalable for hosting more applications and services in future for managing smart cities more effectively. ICCC will help in managing the utilities for Centre Business District (CBD) areas of smart cities and in future capable of managing utilities of entire Puducherry urban through city ICCC. It is also planned to have a Citizen Mobile Application for providing various services to the citizens of the UT of Puducherry. The Citizen Mobile Application will serve as a single unified platform for the citizens to engage with the government, avail citizen centric services (G2C & B2C services), register municipality related complaints, receive issue resolution, access live city feeds through the city dashboard, learn about governance schemes, projects, and initiatives.

c) The four main components of the planned ICCC platform are: Citizen Collaboration, Grievance Redressal, Citizen Service Delivery (G2C & B2C services) and City Dashboard. The Citizen Mobile Application will receive grievances and inputs from both citizen and the Government, using multiple channels (including external social media) to drive the different redressal services, and in turn disseminate information using external media and the platform itself as channels. All the discussion topics, surveys, polls, blogs are specific to discussion groups. Hence, separate Government departments can create, and moderate different discussion groups and the discussion topics, surveys, polls can be created within these discussion groups and moderated by the concerned department using the admin console. The solution also boasts of a robust analytical engine & dedicated team to monitor the collaboration platform and stakeholders about the citizen sentiment/feedback on various discussion topics/polls on regular intervals.

d) The Enhancement and integration of existing E-Governance platform with ICCC is also in the scope of SI. The SI is required to enhance the current application and add the missing modules of E-Governance application which are required for seamless operations for all the departments of the UT of Puducherry. The proposed ICCC for Puducherry smart city will have physical capacity up to 50% of current plan for future activities like expansion of services and its infrastructure based on the agreed plans of PSCDL/DRDM.

### 3.4.2 Objective of the RFP

1. In line with the above vision and an understanding of the pulse of citizens, following smart city components are proposed to be executed vide this RFP:

a) Intelligent Traffic Management System

b) Creation of online/mobile based platform to facilitate tourists & visitors

c) City level application and Smart Dashboard

d) Command & Control Centre with Data Centre (DC) and cloud hosted Data Recovery (DR) which will be an advanced integrated system to operate and manage multiple city service operations.

e) Smart Kiosks.

f) Smart poles with CCTV, Wi-Fi, Air Quality Monitoring (AQM), Smart Street lighting, digital billboard, Emergency call box, Public address system.

g) OFC

h) Flood sensor, Environmental Sensor, Variable Message Display, Public Address System, Emergency Call Box

i) City Wide Surveillance system

2. Through this RFP, RailTel with the approval of client intends to select System Integrator (SI) to:

a) Carry out location specific feasibility survey in consultation with different stakeholder units of the Union Territory of Puducherry like DRDM, Police Department, Transport Department, Puducherry Municipality, Electricity Department, Public Works Department, Town and Country planning, Science and Technology etc., at the locations to be covered under the Smart City projects jointly with RailTel.

b) Project period for SI would start with effect from issuance of work order to roll out of the project and its five-year maintenance period.

c) Design, Develop, Implement, Roll-out and Maintain Governance Application and infrastructure.

d) Design, Develop & Maintain city and state level Network highway with ITMS, City Surveillance with Video Analytics, Smart Poles and OFC network.

e) Build/implement/operate Data Center and Disaster Recovery Center for all the smart city projects outlined above.

f) Design, develop and maintain the Integrated Command and Control Center (ICCC) and associated activities at the proposed location (to be finalized in consultation with different stakeholder units of the Union Territory of Puducherry) with city-based controls and analytics and a state-of-the-art Integrated

Command and Control Center (ICCC). The scope of State level ICCC infrastructure should be such that it may be expanded to integrate smart city components and modules in future.

g) The Common Data Center and Disaster Recovery Center for the Puducherry Smart City shall be a platform for management for the operations of the proposed smart city projects as well as all currently operational E-Gov and smart city initiatives in the UT of Puducherry. The city specific ICCC shall be helpful in managing the smart operations and emergency response in the locations/wards to be covered under the Puducherry Smart City project.

h) Integration of the existing and future ICT based urban solutions (in coming future during the project period) and ICCC solution of Puducherry Smart City Development Ltd.

i) Design, Develop & Maintain city and state level Network highway with Smart Traffic & Transport system, City Surveillance with Video Analytics & Kiosks system.

3. This RFP provides a high-level overview of the technology approach for setting up a common DC/DR for the city based ICCC and includes in-depth details of the functional roles of system components of PAN city application, and the interactions between roles, to achieve an end-to- end system design and project objective. The SI will be responsible for the following:

a) Design, Development, Implementation, Operation & Maintenance of ICCC and associated Projects at Puducherry, its roll out, and integration with existing smart city applications/E-Gov platforms.
b) Intelligent Traffic Management System
c) Creation of online/mobile based platform to facilitate tourists & visitors
d) City level application and Smart Dashboard
e) Command & Control Centre with DC and cloud hosted DR which will be an advanced integrated system to operate and manage multiple services of the smart city infrastructure.
f) Smart Kiosks.
g) Smart poles with CCTV, Wi-Fi, Air Quality Monitoring (AQM), Smart Street lighting, digital billboard, Emergency call box, Public address system.
h) OFC
i) Flood sensor, Environmental Sensor, Variable Message Display, Public Address System, Emergency Call Box
j) City Wide Surveillance system

The system is to be designed taking into consideration the future scalability and integration with upcoming systems.

The system shall help to meet the following objectives:

- Security and Safety
- Improved & Smooth Traffic Movement in the City
- Effective Monitoring
- Improved Responsiveness
- Improved Management

Ensuring safety and security in fragile settings remains among the department's key

objectives in addition to handling crisis management during serious incidents, the list of strategic objectives include:

| | |
|---|---|
| Security and Safety | • Live monitoring of critical infrastructures, city entry & exit points, important locations/ public places in city area like area near to railway stations, airport, bus stops and other public places through surveillance camera.<br>• Live monitoring and control of Traffic Signals, Live monitoring of over speeding vehicles, live monitoring of vehicles passing through important locations of the city including entry and exit points.<br>• Live alerts in case of an event/ incident.<br>• Help to identify, apprehend and prosecute offenders.<br>• Monitoring of suspicious people, activity, vehicles, objects etc. with respect to protecting life & property and maintaining law and order in the city. |
| Improved Responsiveness | • Access to Police by the Citizens for quick and effective response, improved visibility and transparency.<br>• Better Management of Security breaches based on alerts received from system.<br>• Provide assistance to emergency services and fast turn-around time. |
| Effective Monitoring | • Address detection of hot listing vehicles.<br>• Assist in management and policing of large-scale events (political, religious etc.).<br>• Aid to investigation by Police Department by integration of analytic tools.<br>• Providing evidence for criminal and civil action in the courts. |
| Improved Traffic Management | • Address the manual Traffic Signaling in the city.<br>• Optimizing the traffic movement with help of Adaptive Traffic Signal Control |
| Improved Management | • Help in maintaining Law & Order situations.<br>• Help in improving traffic discipline. |

## 4 Project broad scope

### **4.1** Overview

The Overall aim is to select System Integrator (SI) for the Puducherry smart city project area that would be responsible to provide an end-to-end ICT Solutions for the works mentioned in para 3.4.2(3).

### **4.2** Services

The SI will design and develop concept of Smart City works and services, get it implemented / executed, rollout and including operation & maintenance period for 05 years on a turnkey

basis.

**4.3** Responsibilities

The SI would be responsible for designing in following packages mentioned below:

a) Design, Development, Implementation, Operation & Maintenance Central ICCC along with DC at Puducherry

b) Puducherry Smart City rollout and integration with Central ICCC

c) Establishment of DR center and its integration with the ICCC, & DR

d) Deploy:

i. City Surveillance system - CCTV/PTZ camera with video analytics capabilities
ii. Intelligent Traffic management system - Adaptive Traffic Control System (ATCS), Red Light Violation Detection (RLVD) and Automatic number-plate recognition (ANPR), Automatic Traffic Counter & Speed Violation Detection (SVD)
iii. Environmental sensors, Flood sensor
iv. E governance - Citizen Services application
v. GIS platform integrated with Command-and-Control Center
vi. Variable Message Board (VMD),
vii. Smart Poles with Emergency Call Box, Public Announcement system, Smart street lighting, digital billboard, public Wi Fi, etc.
viii. Smart Kiosk
ix. Emergency call box, Flood sensor, Public address system
x. OFC network.

e) Provide Operation & Maintenance services (O&M), including warranty & IT Helpdesk services for a period of five (05) years from Go-Live.

f) The SI shall provide City network backbone through OFC fiber. The provisioned network infrastructure shall be designed in a manner, which shall be capable to carry all the key services that shall be implemented in due course by the authority.

g) In order to achieve the convergence with other city level projects, the Integration with existing/proposed ICT systems as below are also envisaged, Water/sewerage SCADA, Electrical SCADA, e- Health, Public Bike Sharing System, Transport Monitoring center, ERSS (Dial 100/112).

h) Necessary civil and electrical interior infrastructure of the building for the City ICCC is to be developed through this project. The ICCC building shall be provided by the Puducherry Authority.

**4.4** Establishment of ICCC

Under the Smart City initiative, it is envisaged to establish an Integrated Command & Control Centre (ICCC) Data Centre, Disaster Recovery, Intelligent Traffic Management system, Smart Elements and Smart Parking Management System shall be deployed & commissioned at Puducherry in real time which shall be the single & dedicated place for integrating, implementing, monitoring, controlling & commanding all City-Wide Smart ICT for line departments.

**4.5** Elements

Elements of Smart City are as follows but not limited to: -

a) Integrated Command & Control Centre (ICCC)

b) Data Centre (DC) & Disaster Recovery Centre (DR)

c) Intelligent Traffic Management System (ITMS)

i. Red Light Violation Detection (RLVD)
ii. Speed Violation Detection (SVD)
iii. Auto-Number Plate Recognition System (ANPR)
iv. Adaptive traffic control system (ATCS),
v. Other analytics including Violation of Helmet, seatbelt rules, triple riding on bikes, stop line violation, wrong side movement detection etc.
vi. E-Challans integration

d) City wide CCTV surveillance

e) Smart Elements

i. Smart Kiosk
ii. Public Address (PA) System / Emergency Call Box (ECB)
iii. Variable Messaging Display (VMD)
iv. Environmental Sensors for AQM
v. Flood Sensors

f) Any other E-Governance Application or Citizen facing application

g) Creation of online/mobile based platform to facilitate tourist and visitors

h) City level application and smart dashboard

i) Smart poles with CCTV, Wi-Fi, Air Quality Monitoring (AQM), Smart Street lighting, Digital billboard, Emergency call box, Public address system.

j) OFC network.

k) Integration with other ICT systems of the Smart city.

**4.6** Network Backbone

The connectivity between the field/end devices and the ICCC over its own network fiber backbone. The network availability would be monitored through a Network Operations Centre with implementation of a robust EMS, which will be housed along with the Integrated Command and Centre. The SI will be responsible to deploy the Optical Fibre backbone for the requirement for connectivity. Seamless and resilient connectivity required for the following but not limited to:

a) Managed Service - End devices to Data Centre
b) Internet Bandwidth
c) DC DR Connectivity
d) DC Backhaul Bandwidth
e) VPN Remote Connectivity

**4.7** Smooth & efficient operation of ICCC

The SI is to further ensure that all the smart city components and devices are connected to the Data Centre, DR and Command Control Centre in a reliable and resilient mode for smooth& efficient operation of the ICCC. 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.

**4.8** Connectivity to DC & DR

The SI is expected to have performed 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 Puducherry Smart City ICT Solutions and duly factorize those in while preparing a response to this RFP.

**4.9** Security & Monitoring of all ICT infrastructure

SI must make all the necessary provisioning for security of all ICT hardware's along with network backbone at DC, DR and Edge devices and their monitoring from the Central ICCC at Puducherry.

**4.10** Project Activities

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 for the proposed project using Hi-Tech solutions.

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

a) Project Management
b) Survey and Detailed Design of all smart solutions components
c) Prototype Acceptance and Final Acceptance Testing
d) Software Development
e) System Integration
f) Testing & Pilot Deployment
g) Training
h) Change Management
i) Final Deployment & Documentation
j) Operational System Acceptance Tests
k) Comprehensive Operations and Maintenance of 5 years after Go-Live
l) Facility Management Staff

4.10.1 Implementation Phase:

Implementation of ICCC for Puducherry Smart City along with implementation of Citizen Mobile Application and Integration of Existing E-Governance platform.

a) Activities related to Common Data Center and Data Recovery Center for the Smart City project along with implementation of Citizen Mobile Application and Integration of Existing E-Governance platform. Implementation of common applications on DC & DR and integration as per the agreed Functional Requirement Specification (FRS), Software Requirement Specification (SRS) and Standard Operating Procedure (SOP).

b) Creation of city specific interface for accessing the common applications.

c) Integration of city specific applications with common command center platform.

d) Facilitating user acceptance testing and conducting the pre-launch security audit of applications

e) 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.

f) Planning, implementation and integration of all the necessary modules of Citizen Mobile Application

4.10.2 Activities related to Smart City & ICCC Puducherry

i. Physical Setup of ICCC as per the layout agreed with the DRDM/PSCDL. This includes activities like false flooring, false ceiling, partitions, network cabling, electric fitting, Online UPS (built in storage), DG Set, auto on-off lighting system and other facilities as mentioned above along with required furnishing of the complete DC facility
ii. A Centralized Helpdesk and a Situation room will only be setup in ICCC
iii. IT and Non-IT Infrastructure installation, development, testing and production environment setup
iv. Safety and security of IT and Non-IT Infrastructure
v. Housekeeping facility for ICCCs.
vi. Software Application customization, data migration, integration with third party services/application
vii. Preparation of User Manuals, training curriculum and training materials
viii. Role based training(s) on the Smart City Solutions
ix. SoP implementation, Integration with City GIS Platform, Integration of solutions with Command-and-Control Center
x. Network connectivity establishment and configuration between DC & DR, City ICCC, existing applications (which are to be integrated with DC & DR and City ICCC).
xi. User training and roll-out of solution
xii. Integration of the various services & solution with DC & DR and ICCC platform
xiii. Submit Monthly Progress reports as per the defined format to DRDM along with invoices.
xiv. Submit Joint Monthly Progress reports after approval as per the format defined to DRDM along monthly progress report on common DC and DR along with total invoices.
xv. Go-Live of City ICCC will happen in this phase only, where complete setup of the ICCC will be required to be done along with complete integration with minimum 1 service.

4.10.3 Post Implementation Scope for the Operation and Maintenance Phase

a) Activities related to Common Data Center and Disaster Recovery Center for SmartCities

i. Operations and maintenance of DC & DR facility.
ii. Annual technical support for all hardware and software components for the O & Mperiod
iii. Overall maintenance of the DC & DR facility and continuity of operations as perService Level Agreement (SLA).

b) Activities related to City ICCC

i. Deploying manpower at city level ICCC for solution maintenance and monitoring support which includes change request management, bug tracking and resolution, production support, performing version and patch updates
ii. Integration of various services of the city based on the requirements of the city
iii. Annual technical support for all hardware and software components for the O & M period
iv. Preventive, repair maintenance and replacement of hardware and software components as applicable under the warranty and AMC services during the contract period
v. Provide a Helpdesk and Incident Management Support at State level till the end of contractual period
vi. Recurring refresher trainings for the users and Change Management activities
vii. Provide facility, information and required access to DRDM/PSCDL/Municipal Corporation or its authorized agency for doing various kinds of Audits as and when required
viii. Preventive, repair maintenance and replacement of non-ICT components as applicable under the warranty and AMC services during the contract period
ix. LAN at ICCC
x. Overall maintenance of the ICCC facility and continuity of operations as per SLAs
xi. Overall maintenance of housekeeping and physical security at ICCC, DC & DR
xii. Provide necessary security to the ICCC premises and its setup during the period of contract
xiii. Submit Monthly Progress reports as per the defined format to DRDM along with invoices
xiv. Submit Joint Monthly Progress reports after approval as per the format defined by DRDM/ PSCDL along monthly progress report on common DC and DR along with total invoices.

### 4.10.4 Expectations from Integrated Command and Control Center Platform

ICCC platform shall be the 'heart' of the Smart City of Puducherry that assists in enhancing efficiencies of city operations and management of all smart cities. It provides a holistic view of all city operations allowing monitoring, control and automation of various functionalities at an individual system level along with enabling cross-system analytics.

This application will be required to be installed on the common data center and disaster recovery center for smart cities. This application platform will be common to all cities with different instances of each city.

The business requirements that the Integrated Command and Control Center Application Platform shall achieve are:

a) Shall enable cross-system and cross-agency coordination to monitor, operate and manage the city in an integrated manner
b) Shall enable different agencies and departments of State and Cities to monitor and utilize information of other departments for delivering services in an integrated and more efficient manner
c) All systems being provided as part of this RFP and by others (mentioned in this RFP) shall be integrated with Command Center Application as per the requirements of the Project.
d) The platform shall enable various visualization and analytics of city operations to improve decision making. These analytics shall be achieved via cross-system integration of various systems and as per the standard operating procedure (SOPs) discussed and agreed upon with the Client. Analytics shall include both prescriptive, predictive analytics and cognitive analytics.
e) Command Center Application shall provide reporting capabilities for city administrators

to keep record of city operations

f) Command Center Application shall ensure that integrity and confidentiality of all information gained is always secure
g) Command Center Application platform shall be the integration point at which data from across the city converges for processing. This shall allow all information to be managed within the same network, eliminating many communication problems that are faced by working in siloes
h) Command Center Application shall provide shift-based operations for an overall 24x7 support
i) Map and integrate all systems to city specific GIS platform being provided as part of this RFP
j) The system shall be scalable to accommodate future growth and support hardware and software additions and upgrades.

k) Command Center shall leverage information provided by multiple city systems to support an integrated, seamless, proactive and comprehensive response mechanism for day-to-day city operations and challenges. The platform shall provide a combination of system layers that when combined shall make use of Data, ICT and ITS infrastructure, advanced computing, analytics, and visualization to enhance the city's intelligence. In addition, it shall provide the tools for the city decision makers to better manage the services they provide to its citizens.

l) There are several functions and systems that shall be managed out of the Command Center Application. Depending on the type of systems and functions, they shall be monitored and/or controlled from the Command Center Application and will have the option of sharing a feed to another agency as required via the platform. This shall integrate all the City Systems procured under the Smart City Mission, which include systems procured through this project and system which are/will be procured as other projects.

Note: Responsibility of integration is of the SI, whereas SI for other application which is to be integrated, SI will be responsible for providing interface layer / API / Software Development Kit (SDK) in its system for doing the application. Authorities will be responsible for getting required interface layer / API / SDK for particular application from respective department (whose application is required to be integrated with ICCC interface) for SI to integrate with Common Command Center Application Expectations from Data Center and Data Recovery Center of ICCC.

4.10.5 Expectations from DC & DR

a) DC & DR is required to host & save data related to common command center and applications hosted in ICCC environment.
b) DC & DR will not host any smart application (implemented in smart cities) which is being integrated with command center application. This smart application (which is being integrated with command center application) is responsibility of the respective vendor / SI of the city who is managing the particular application implementation and rollout.
c) DC & DR will also host common applications like Integration Layer, Analytical Layer, Enterprise Management Software (EMS), Knowledge Management (KM), Information & Cyber Security applications, etc. required for Command Center Applications and ICCC working.
d) DC & DR will save data coming from the applications hosted in datacenter of ICCC

Puducherry

e) DC & DR should be able to receive information (ex: from the field devices) and send the information to the ICCC platform or visualization layer.
f) DC & DR will only save log of the transactions performed with common command center application.
g) DC & DR will also have dashboard views of the applications (integrated with command center application) for historical data as required by the city.

4.10.6 Manpower and resources

The SI has to deploy all resources including manpower (project manager and his team with sufficient number of assistants) and setup office in Puducherry within 15 days from the date of issuance of work order.

**4.11** SI's Obligations:

a) SI obligations shall include all the activities as specified in this RFP. It shall be SI's responsibility to ensure the proper and successful implementation, performance and continued operation of the proposed solution in accordance with and in strict adherence to this RFP.

b) SI shall adhere to the Smart City Mission (SCM) guidelines issued by the MoHUA and the advisories issued by SCM, MoHUA from time to time on the implementation of ICCC by Smart Cities.

c) SI shall also satisfy the minimum functional and technical requirement, service level agreement conditions, as specified in this RFP.

d) In addition to the aforementioned, SI shall provide services to manage and maintain the said system and infrastructure as mentioned in the RFP.

e) Department of Revenue and Disaster Management, Puducherry reserves the right to interview the team composition that shall be deployed as part of the project team. If found unsuitable, the DRDM may reject the deployment of the personnel.

f) SI is encouraged to propose equipment which are compliant with "Make in India" initiative.

g) Department of Revenue and Disaster Management, Puducherry reserves the right to require changes in personnel which shall be communicated to RailTel.

h) SI shall provide the project team necessarily comprising the following key resources namely Project Manager, ICCC/ Command Center Expert, Solution Architect, Security Infrastructure expert, GIS expert, Data Management expert /Analyst, Business Analyst / Use-case/SoP expert, Network Architect, and Server/ Storage & Database Expert only after assessment and approval of DRDM/PSCDL.

i) SI with the prior approval of Department of Revenue and Disaster Management/PSCDL may make additions to the project team. SI shall provide Department of Revenue and Disaster Management, Puducherry with the resume of Key Personnel and provide such other information as the DRDM may reasonably require through RailTel. The Authorities also reserves the right to interview the personnel and reject, if found unsuitable. In case of change in its team members, for any reason whatsoever, SI shall also ensure that the exiting members are replaced with at least equally qualified and professionally competent members.

j) SI should submit profiles of only those resources who shall be deployed on the project.

Any change of resource should be approved by the tenderer and compensated with equivalent or better resource. The Authority may interview the resources suggested by SI before their deployment on board. It does not apply in case of change requested by the tenderer.

k) In case of change in its team members, SI shall ensure a reasonable amount of time overlap in activities to ensure proper knowledge transfer and handover / takeover of documents and other relevant materials between the outgoing and the new member.

l) SI shall ensure that their Team is competent, professional and possesses the requisite qualifications and experience appropriate to the task they are required to perform under this RFP. SI shall ensure that the services are performed through the efforts of their Team, in accordance with the terms hereof and to the satisfaction of the tenderer. Nothing relieves SI from its liabilities or obligations under this contract to provide the Services in accordance with the RFP and SI shall be liable for any non-performance, non-compliance, breach or other loss and damage resulting either directly or indirectly by or on account of its Team.

m) SI shall be fully responsible for deployment / installation / development/ laying of network fiber and integration of all the software and hardware components and resolve any problems / issues that may arise due to integration of components.

n) SI shall ensure that the OEMs supply equipment/ components including associated accessories and software required and shall support SI in the installation, commissioning, integration and maintenance of these components during the entire period of contract. SI shall ensure that the OEMs supply the software applications and shall support SI in the installation / deployment, integration, roll-out and maintenance of these applications during the entire period of contract. It must clearly be understood by SI that warranty and maintenance of the system, products and services incorporated as part of system would commence from the day of Go-Live of system as a complete Smart city solution including all the solutions proposed. SI would be required to explicitly display that they have a back-to-back arrangement for provisioning of warranty and maintenance support till the end of contract period with the relevant OEMs. The annual maintenance support shall include patches and updates the software, hardware components and other devices.

o) Factory visits may be required by the Authorities at the cost of SI to verify the claims of the SI.

p) Site visits to any of the operating Command Centre / Data Centre developed by SI at cost to SI may be required by client to verify the claims of the SI.

q) All the software licenses that SI proposes should be perpetual software licenses. The software licenses shall not be restricted based on location and DRDM should have the flexibility to use the software licenses for other requirements if required.

r) Authorities reserve the right to review the terms of the Warranty and Annual Maintenance agreements entered into between SI and OEMs and no such agreement/contract shall be executed, amended, modified and/or terminated without the prior written consent of the tenderer.

s) An executed copy of each of such agreements/contracts shall, immediately upon execution be submitted by SI to the Authorities.

t) SI shall take approval of the PSCDL board/DRDM/ RailTel for sub contract.

u) SI shall follow all the codal formalities while executing the work.

v) If a product is de-supported by the OEM for any reason whatsoever, from the date of Acceptance of the System till the end of contract, SI should replace the products/solutions with an alternate that is acceptable to the tenderer at no additional cost to the tenderer

and without causing any performance degradation.

w) The Licenses will be in the name of DRDM only.

**4.12** SI's Reporting Obligations:

a) SI shall monitor progress of all the activities related to the execution of this contract and shall submit to the Authorities, progress reports with referenceto all related work, milestones and their progress during the implementationphase.
b) Formats for all above mentioned reports and their dissemination mechanismshall be discussed and finalized along with project plan. The Authorities onmutual agreement may change the formats, periodicity and disseminationmechanism for such reports.
c) Periodic meetings shall be held between the representatives of theAuthorities and SI once in every 15 days during the implementation phase todiscuss the progress of implementation. After the implementation phase isover, the meeting shall be held as an ongoing basis, as desired by Authorities,to discuss the performance of the contract.
d) SI shall ensure that the respective solution teams involved in the execution ofwork are part of such meetings.
e) All the goods, services and manpower to be provided / deployed by SI underthe Contract and the manner and speed of execution and maintenance ofthe work and services are to be conducted in a manner to the satisfactionof DRDM's representative in accordance with the Contract.
f) Authorities reserves the right to inspect and monitor/ assess the progress/performance of the work / services at any time during the course of the Contract. Authorities may demand and upon such demand being made, SIshall provide documents, data, material or any other information which Authorities may require, to enable it to assess the progress/performance of the work / service.
g) At any time during the course of the Contract, Authorities shall also have theright to conduct, either itself or through another agency as it may deem fit, an audit to monitor the performance by SI of its obligations/ functions inaccordance with the standards committed to or required by the Authoritiesand SI undertakes to cooperate with and provide to the Authorities any otheragency appointed by the Authorities, all Documents and other details asmay be required by them for this purpose. Such audit shall not include SI'sbooks of accounts.
h) Should the rate of progress of the works or any part of them at any time fallbehind the stipulated time for completion or is found to be too slow to ensurecompletion of the works by the stipulated time, or is in deviation to Tenderrequirements/ standards, the Authorities' representative shall so notify SI inwriting.
i) SI shall reply to the written notice giving details of the measures they proposeto take to expedite the progress so as to complete the works by the prescribed time or to ensure compliance to RFP requirements. SI shall not beentitled to any additional payment for taking such steps. If at any time itshould appear to the Authorities representative that the actual progress ofwork does not conform to the approved plan SI shall produce at the requestof the Authorities representative a revised plan showing the modification to the approved plan necessary to ensure completion of the works within thetime for completion or steps initiated to ensure compliance to the stipulatedrequirements.
j) The submission seeking approval by the Authorities of such plan shall notrelieve SI of any of his duties or responsibilities under the Contract.
k) In case during execution/implementation of works, the progress falls behind

schedule or does not meet the Tender requirements, SI shall deploy extra manpower/ resources to make up the progress to meet the RFP requirements. Plan for deployment of extra man power/ resources should betaken care by SI. SI shall prepare and distribute Service level performancereports in a format by Authorities.

l) The reports shall include "actual versus target" Service Level Performance, a variance analysis and discussion of appropriate issues or significant events. Performance reports shall be distributed to the Authorities.

m) Also, SI may be required to get the SLA reports audited by a third party auditor under its responsibility with necessary approval from Authorities. All related cost will be borne by SI.

# 5 Project Scope of Work

## 5.1 Assessment, Site Survey and Project Plan

After signing of contract, the SI needs to deploy team locally proposed for the project and ensure that a Project Inception Report is submitted to the Authorities which shouldcover following aspects. The SI shall first carry out a detailed survey to identify & finalizethe locations, requirements vis-a-vis proposed solutions.

a) Names of the Project Team members, their roles and responsibilities

b) Approach and 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) Risks the SI anticipates and the plans they have towards their mitigation

e) Detailed project plan specifying dependencies between various project activities / sub-activities and their timelines

f) The SI shall conduct a comprehensive study to establish the key performance indicators (KPIs) for the project. The KPIs of the study shall be included in the survey.

g) The SI shall study the existing business processes, functionalities, existing management systems and applications including MIS reporting requirements. Additionally, the SI should provide detailed designs specifying the following:

i) Post completion of Survey the SI shall consult the various Stake Holder of the project, in consultation with the Authorities, and finalize the locations for execution. Upon freezing the locations for execution, the SI shall detail out the final functional requirement system for each of the proposed ICT intervention and get a sign off from the user department and the Authorities.

ii) Post finalization of the SRS and FRS the SI shall submit a High-Level Design Document which shall cover the broad architecture and a solution document for each of the proposed ICT intervention.

iii) The HLD will comprise of the compute, storage and the OS requirements.

iv) Post HLD, the SI shall be submitting the Low-Level Design Document with the good for construction drawing, network connectivity drawing, LPU details, if any, API for integration, communication protocol etc.

v) Upon approval of LLD by the Authority the SI shall implement the said ICT intervention.

vi) Software Requirement Specification (SRS), Test cases and conducting the PAT/FAT of the project.

vii) Location of all field systems and components proposed at the junctions, (KML /KMZ file plotted on GIS platform like google earth etc.)

viii) Location of Network Provider's Point of Presence (PoP)

ix) Design of Cables, Ducts routing, digging and trenching

x) Electrical power provisioning.

### 5.2 Documents/ Drawings Submission after Award of Contract

SI shall submit documents and drawings as mentioned below within One (1) Months after award of contract for review and approval from Client/ Consultant. Following are the minimum list of documents and drawings to be submitted, however, SI shall not restrict himself to the same and it is in the obligation of the SI to submit all supporting documents, detailed drawings as requested by Client/ Consultant during engineering and execution stage.

#### 5.2.1 Stage 1: Design engineering

a) Design basis report and individual system block diagram.
b) Overall system architecture and flow diagrams
c) Design calculation sheets for all systems
d) System and location wise Equipment list along with GIS coordinates
e) System and location wise Load list/ power requirement
f) System and location wise UPS load list System and location wise Heat load calculation list
g) Technical specifications and datasheets for all systems.
h) Standard Operating Procedures (SOPs) for Integrated Command & Control Center (ICCC).
i) Key Performance Indicators (KPIs) for each system.

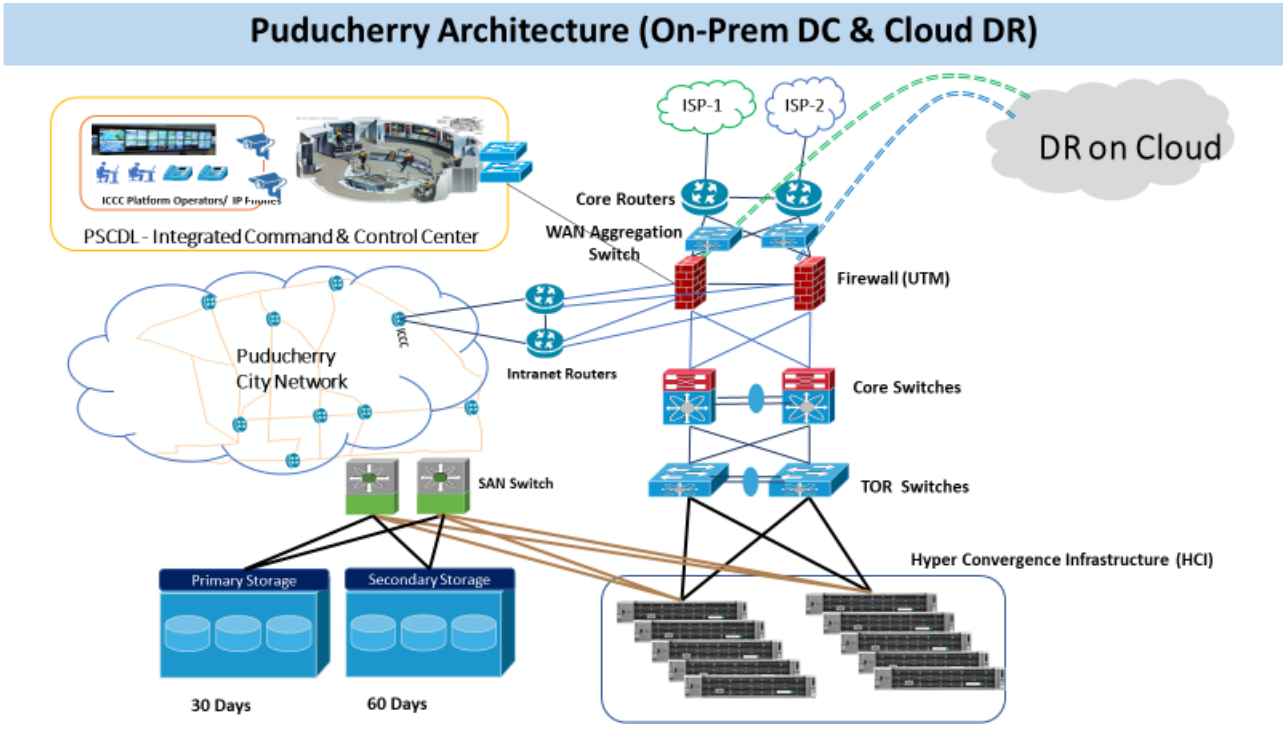
#### 5.2.2 Stage 2: Project execution

a) General arrangement drawings.
b) Job execution schedule
c) Equipment general arrangement, internal wiring and third-party integration provision
d) QAP and FAT/ SAT procedures
e) System/ equipment Installation/ erection drawings.
f) Installation manuals

### 5.2.3 Stage 3: Post commissioning

a) As-built drawings
b) Training manuals and schedules.
c) Operation and maintenance manuals.
d) Spares list (recommended spares, commissioning spares and operation spares)

### 5.3 Finalization of Detailed Technical Architecture




## Applications Architecture

**On-Prem DC**

- VMS Application:
  -Video Storage (first 30 Days in Primary Storage and 31st day to 90th Day in Secondary Storage)
- ICCC Application (5 Year Data)
- ITMS (5 year Data)
- VA (5 Year data)
- All other IoT Apps (All Data)
- EMS/NMS

**Cloud DR**

- ICCC Application (5 Years Data)
- ITMS (5 Years Data)
- VA (5 Years Data)
- All other IoT Apps (5 Years Data)

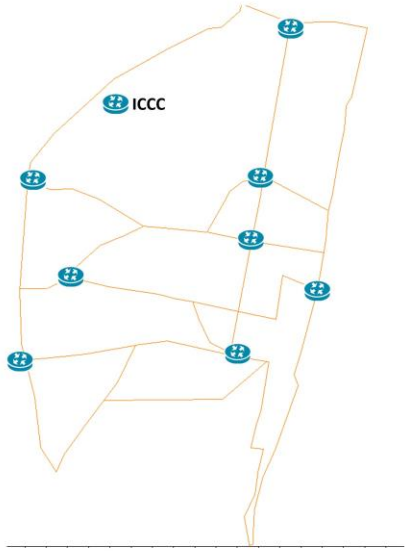
**On-Prem DC:**

- On-Prem DC Applications should be deployed in HA.
- Should consider EMS resources for Staging/TnD.
- On-Prem DC All Applications data should be in HCI and continuous video storage should be in external primary/secondary storage.
- DC Applications local back up should be in external storage system.

**Cloud DR:**

- Cloud DR Applications should be deployed without HA.
- In case of on premise DC fails, applications from cloud DR should work seamlessly or with minimum configuration changes.
- After on Premise DC restoration, incremental data in Cloud DR and On-Prem DC data should synchronized.

## Typical City Network Architecture




While implementing the ICT intervention the SI shall adopt the following:

a) **Scalability** - The system should also support both vertical and horizontal scalability. There must not be any system-imposed restrictions on the upward scalability in number of field devices, or other smart city components. The Applications proposed for various vertical solutions shall be capable of handling 50% growth for the next 5 years. SI shall clearly quantify the expansion capabilities of the application software without incurring additional cost.

b) **Availability** -. The SI shall make the provision for high availability (N:N or N:1) for all the services of the system. Redundancy has to be considered at the core components level.

c) **Security-** The architecture must adopt an end-to-end security model that protectsdata and the infrastructure from malicious attacks, theft, natural disasters etc. SI must make provisions for security of field equipment as well as protection of the software system from hackers and other threats. 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. There should also be an endeavour to make use of the SSL/VPN technologies to have secured communication between Applications and its end users.

   Field equipment installed through this Project would become an important public asset. During the contract period of the Project the SI 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.

   The security services used to protect the solution shall include: Identification, Authentication, Access Control, Administration and Audit and support for industry standard protocols. 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. The overarching requirement is the need to comply with ISO 27001 standards of security. The application design and development should comply with OWASP top 10 principles. All the field devices will be
X.509 certified for compliance to policy change management and to ensure that there is no default password.

d) **Manageability -** Ease of configuration, ongoing health monitoring, and failure detection are vital to the goals of scalability, availability, and security and must beable 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 extentpossible

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 theirprofile and registration, the system shall enable single-sign on facility to apply forvarious services, make payments, submit queries /complaints and check.

h) **Support for PKI based Authentication and Authorization-** The solution shall support PKIbased Authentication and Authorization, in accordance with IT Act 2000, using the Digital Certificates issued by the Certifying Authorities (CA). In particular, 3 factorauthentications (login id & password, biometric and digital signature) shall be implemented by the SI for officials/employees involved in processing citizen services.

i) **Interoperability Standards-** Keeping in view the evolving needs of interoperability, especially the possibility that the solution shall become the focal point of delivery ofservices, 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 SI shall ensure that the application developed is easily integrated with the existing applications. The code does not build a dependency on any proprietarysoftware, particularly, through the use of proprietary 'stored procedures' belonging to a specific database product. The standards should:

1. 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
2. Be of leading industry standards and /or as per standards mentioned in the technical specifications

**j) Application Architecture**

1. The applications designed and developed for the departments concerned must follow best practice and industry standards. In order to achieve the high level of stability and robustness of the application, the system development life cycle 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. Standards should (a) at least comply with published e- Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and (b) be of leading industry standards and /or as per standards mentioned in the technical specifications

2. The modules of the application are to be supported by the Session and TransactionManager for the completeness of the request and response of the client request.The system should have a module exclusively to record the activities/ create the logof activities happening within the system / application to avoid any kind ofirregularities within the system by any User / Application.
3. SI shall design and develop the Smart City System as per the Functional and Systemrequirement specifications finalized.
4. The Modules specified will be developed afresh based on approved requirement.

### 5.4 Site Clearance Obligations and Other Relevant Permissions

#### 5.4.1 Survey And Commencement of Works

Prior to starting the site clearance, the SI shall carry out survey of field locations, for buildings, structures, fences, UG utilities' – Power Cables & WaterPipelines, OFC Network of other Operators, Trees, existing installations, etc. TheAuthorities shall be fully informed of the results of the survey and the amountand extent of the demolition and site clearance shall then be agreed with the Authorities. Restoration will be the responsibility of the SI. Right of Way and Track rent will be borne by PSCDL/DRDM.

#### 5.4.2 Existing Traffic Signal system

The infrastructure of existing traffic signal systems including the aspects, controllers etc. will be dismantled and replaced with the new systems whichare proposed and required under the scope of this project. The dismantled infrastructure shall be delivered at the designated location of PSCDL/DRDM without damage at no extra cost.

#### 5.4.3 Electrical Works and Power Supply

The SI shall directly interact with PSCDL/DRDM for provision of mains power supply at all locations for ICCC field systems. The SI shall be responsible to pay the electricity bills including connection charge, meter charge, recurring charges etc. to the PSCDL/DRDM directly. SI shall have to submit the challanof bill submission to PSCDL/DRDM. PSCDL/DRDM will reimburse the amount deposited by the SI after verification in next billing cycle.

### 5.5 Miscellaneous:

a) Authority shall assist in obtaining all necessary go ahead, legal permissions, NOC (No Objection Certificate) from various departments to execute the project. SI shall have to identify and obtain necessary legal / statutory clearances for erecting the poles and

installing cameras, for provisioning ofthe required power, etc. SI shall provide & manage all necessary paper workto pursue permission from respective authorities. Commercial/legal fees / RoW charges shall be applicable to Authority for obtaining the necessary permissions.

b) The SI shall provide all material required for mounting of components such ascameras and other field equipment. All mounting devices for installation of CCTV cameras such as mounting bracket, Lens, Weather proof housing, Pole,Junction Box, Power Supply, Cables, accessories, etc. 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.

c) All the equipment, software and workmanship that form a part of the serviceare to be under O&M from the SI throughout the contract period.

d) SI shall also get comprehensive insurance from reputed insurance company for the project duration for all the equipment's / components installed under this project.

e) SI shall ensure all the equipment's installed in the outdoor locations are vandal proof and in case the equipment's get damaged /stolen for reasonswhatsoever, it shall repair/replace the same in the specified time as per SLAsat no extra cost to the Authority. All such costs shall be factored in the comprehensive insurance of field equipment for the duration of the contract.

f) Preventive maintenance shall be carried out once in a quarter along with corrective maintenance and also when calls are placed by Authority or itsdesignated agency.

g) In addition to above, the SI shall be fully responsible for all maintenanceactivities for the period between installation of equipment and roll-out of the system.

h) During implementation, if observed that any camera / field equipment requires change in the field of view / orientation, it shall be done by SI withoutany extra cost.

i) In case of request for change in location of field equipment post installation,the same shall be borne by Authority at either a unit rate as per commercialsor a mutually agreed cost.

### 5.6 Design and Implementation of Integrated Command & Control Center System

The SI should ensure the successful implementation of the proposed ICCC Project as per the scope of services described below. SI shall implement and deliver the following systems and capabilities linked ICCC.

i. City Surveillance system - CCTV/PTZ camera with video analytics capabilities

ii. Intelligent Traffic management system - Adaptive Traffic Control System (ATCS), Red Light Violation Detection (RLVD) and Automatic number-plate recognition (ANPR) & Speed Violation Detection (SVD)
iii. Environmental sensors, E governance - Citizen Services application
iv. GIS platform integrated with Command-and-Control Center
v. Variable Message Board (VMD),
vi. Smart Poles with Emergency Call Box, Public Announcement system, Smart street lighting, digital billboard, public Wi Fi, etc.
vii. Smart Kiosk
viii. Emergency call box, Flood sensor, Public address system
ix. OFC network.

### 5.7 Design, Supply, Installation & Commissioning of the Field Equipment

The Scope includes Supply, Installation, commissioning and Customization (as required) of various field systems which include Integrated Traffic Management System (ITMS) at Traffic Junctions, City Surveillance System, Smart Poles, Smart Kiosk, VMDs, DC & DR and other IT infrastructure required for successful operations of the ICCC project.

Based on the approved Survey report, the SI will undertake the system configuration and customization in line with the changed, improved or specific requirements of the Authorities including:

**5.7.1.** The implementation methodology and approach must be based on the global best practices in-order to meet the defined Service Levels during the operation.
**5.7.2.** Best efforts have been made to define major functionalities for each sub- system of ICCC system. However, SI should not limit its offerings to the functionalities proposed in this RFP and is suggested to propose any functionality over and above what has already been given in this tender with no additional cost.
**5.7.3.** The SI shall design the field level equipment architecture to ensure maximum optimization of network equipment, poles, cantilever, mounting infrastructures, power supply equipment including, electric meters and junction box.
**5.7.4.** Finally approved/accepted solution for each component of ICCC project shall be accompanied with "System Configuration" document and the same should be referenced for installation of ICCC systems at Junctions/Locations that are identified within the scope of this project.
**5.7.5.** The SI shall be required to submit a detailed installation report post installation of all the equipment at approved locations. The report shall be utilized during the acceptance testing period of the project to verify the actual quantity of the equipment supplied and commissioned under the project.
**5.7.6.** The SI shall be responsible for obtaining all permissions/ NOC and approvals necessary to install the ICCC systems components as per the approved design.

The sub-systems included as part of the ICCC project which are required to be implemented and integrated are given in the subsequent sections.

### 5.8 City Surveillance System – (CCTV Camera)

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

5.8.1. 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 the Puducherry Smart City authority.

5.8.2. A detailed survey shall be conducted, by the SI along with a team of Authority and the Puducherry 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 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 SI and submitted to Authority in the form of a detailed site survey report along with other details for its approval.

5.8.3. The SI shall install Surveillance System Cameras for CCTV monitoring and management at all locations across Puducherry city mentioned in the respective annexure.

5.8.4. The SI shall undertake due diligence for selection and placement of surveillance cameras to ensure the optimized coverage of the traffic junction and other locations along with all associated junction arms, accuracy of the information captured on the field and for rugged operations.

5.8.5. The SI shall design, supply, and install the surveillance cameras as defined in the RFP; all wiring connections for the system shall be installed by the SI. The SI shall supply all of the necessary equipment for the camera operations including camera housings and mountings, camera poles, switches, cabling, and shall make the final connections to the junction box.

5.8.6. The SI shall be responsible for providing the entire necessary IT infrastructure for monitoring, recording, storage & retrieval of the video streams at ICCC or any otherlocation as specified in the RFP.

5.8.7. System shall provide inter-operability of hardware, operating system, software, networking, printing, database connectivity, reporting, and communication protocols. SI 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 Authority. Indicative list of the field level hardware to beprovided by SI is as follows:

5.8.8. Cameras (Fixed Box Cameras, PTZ Cameras etc.)

5.8.9. Dome camera for the indoor applications – POP sites monitoring

5.8.10. Industrial Grade Switches

5.8.11. Outdoor Cabinets

5.8.12. Pole for cameras / Mast

5.8.13. Outdoor Junction box

5.8.14. UPS

5.8.15. Networking and power cables and other related infrastructure

5.8.16. SI 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 SI while installing / commissioning cameras are as follows:

5.8.17. Ensure surveillance objective is met while positioning the camera such that the requiredfield of view is being captured as finalized in field survey.
5.8.18. Ensure camera is protected from the on-field challenges of weather, physical damageand theft.
5.8.19. Make proper adjustments to have the best possible image / video captured.
5.8.20. Ensure that the pole is well placed for vibration resistance adhering to the road safetynorms.

5.8.21. Appropriate branding or color coding (Police/Authority Branding) of poles and junctionboxes, to warn mischief mongers against tampering with the equipment at the junction.
5.8.22. The functional requirements and technical specifications provided in this RFP are indicative and carry guiding rule. The SI is free to offer products and solutions which meetrequirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards & best practices adopted in the industry. The SI is encouraged to design an Optimized solution which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical requirement inthe RFP may be considered if it is required for meeting current & future requirements during the contract period. The SI is fully responsible for the specified outcome to be achieved.
5.8.23. For more details on technical and functional specifications of Surveillance Cameras, SIshould refer to Section: 6.0 for Functional and Technical specifications.

**5.9 Integrated Traffic Management System (ITMS)**

The broad scope of work to be covered under ITMS sub module will include thefollowing, but is not limited to:

5.9.1. Preparation of Solution Architecture for Adaptive Traffic Control System (ATCS) as per the BOQ for installation of traffic signaling systems.
5.9.2. Installation of Vehicle Detectors, Controllers, Traffic Light Aspects, Poles, Cantilevers, Junction Box and other required accessories at Traffic Junctions for successful operation of the ITMS project for Puducherry Smart City.
5.9.3. Integration of ITMS field infrastructures with the proposed ITMS software application.
5.9.4. Configuration of traffic signal at each of the junction along with development of signal control plan for individual operations, coordinated signal plan for the junction in sync with the area wide signal plan for different operating conditions. The operating conditions may include different peak and off-peak conditions, special events, contingency plans etc.
5.9.5. The functional requirements and technical specifications provided in this RFP are indicative and carry guiding rule. The SI is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards & best practices adopted in the industry. The SI is encouraged to design an Optimized solution which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical requirement in the RFP may be considered if it is required for meeting current & future requirements during the contract period. The SI is fully responsible for the specified outcome to be achieved.

5.9.6. For more details on technical and functional specifications of ITMS, SI should refer to Section # 6.0 for Functional and Technical specifications.

**A. Traffic Violation Detection System**

The broad scope of work to be covered under this sub module will include thefollowing, but is not limited to:

*a.* The SI shall install the Traffic Violation Detection System at traffic junctions across the city. This system shall capture the infractions of Red light and stop line violations at these junctions.

*b.* The SI shall design, supply, and install the Traffic Violation Detection System as defined in the RFPs, all wiring connections to the traffic signal controllers and to the camera platforms shall be installed by the SI. The SI shall supply all of the necessary equipment for the camera and detection system, including but not limited to: computers, ancillary camera equipment, camera housings, camera poles, warning signs and shall make the final connections to the camera.

*c.* The solution proposed by the SI shall seamlessly integrate with the existing E-Challan system proposed under the scope of this project. RAILTEL / DRDM/ PSCDL shall facilitate to get access to the Vaahan and Sarathi database. Bidder shall be required to access the same through use of appropriate APIs.

*d.* The SI shall be responsible for providing all the necessary IT infrastructure for analysis, storage & retrieval of the infraction information at ICCC or any other location as specified in the RFP.

*e.* The functional requirements and technical specifications provided in this RFP are indicative and carry guiding rule. The SI is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards & best practices adopted in the industry. The SI is encouraged to design an Optimized solution which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical requirement in the RFP may be considered if it is required for meeting current & future requirements during the contract period. The SI is fully responsible for the specified outcome to be achieved.

*f.* For more details on technical and functional specifications of Traffic Violation Detection system, SI should refer to Section: 6.0 for Functional and Technical specifications.

**B. ANPR System**

The broad scope of work to be covered under this sub module will include thefollowing, but is not limited to:

a) The SI shall install the ANPR Cameras at every entry & exit points of the city onmajor highway and ITMS junctions/locations across the city. This system shall automatically capture the license number plate of the vehicle at these junctions.

b) The SI shall design, supply, and install the ANPR camera system as defined in theRFPs, all camera accessories such as IR Illuminators, camera housing and mounting shall be installed by the SI. The SI shall supply all of the necessary equipment for the camera and local processing system, including but not limited to: computers, local storage, and ancillary camera equipment, camerapoles, warning signs and shall make the final connections to the camera.

c) The SI shall be responsible for providing all the necessary IT infrastructure for detection, analysis, storage & retrieval of the number plate information at ICCC or any other location as specified in the RFP.
d) The functional requirements and technical specifications provided in this RFPare indicative and carry guiding rule. The SI is free to offer products and solutionswhich meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards & best practices adopted in the industry. The SI is encouraged to design an Optimized solution which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical requirement in the RFP may be considered if it is required for meeting current & future requirementsduring the contract period. The SI is fully responsible for the specified outcometo be achieved.
e) For more details on technical and functional specifications of ANPR Cameras,SI should refer to Section: 6.0 for Functional and Technical specifications.

**C. RLVD System**

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

a) The SI shall install the RLVD Systems at traffic junctions across the city. This system shall capture the infractions of Red light and stop line violations at these junctions.
b) The SI shall design, supply, and install the RLVD system as defined in the RFPs, allwiring connections to the traffic signal controllers and to the camera platformsshall be installed by the SI. The SI shall supply all the necessary equipment for thecamera and detection system, including but not limited to: computers, ancillary camera equipment, camera housings, camera poles, warning signs and shall make the final connections to the camera.
c) The SI shall be responsible for providing all the necessary IT infrastructure fordetection, analysis, storage & retrieval of the number plate information at ICCC or any other location as specified in the RFP.
d) The solution proposed by the SI shall seamlessly integrate with the existing E-Challan system proposed under the scope of this project. RAILTEL / DRDM/ PSCDL shall facilitate to get access to the Vaahan and Sarathi database. Bidder shall berequired to access the same through use of appropriate APIs.
e) The functional requirements and technical specifications provided in this RFP are indicative and carry guiding rule. The SI is free to offer products and solutionswhich meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line withapplicable standards & best practices adopted in the industry. The SI is encouraged to design an Optimized solution which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical requirement in the RFP

may be considered if it is required for meeting current & future requirementsduring the contract period. The SI is fully responsible for the specified outcome tobe achieved.

f) For more details on technical and functional specifications of RLVD Cameras, SIshould refer to Section: 6.0 for Functional and Technical specifications.

**D. Speed Violation Detection (SVD) System**

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

i. SVD camera will be installed on major highways of the city.
ii. Primarily, SVD will be at major locations along with real time visual indications of speed violation on LED display board.
iii. System will be able to record the vehicle speed with proof of video/photograph andevent time and date.

The SI shall design, supply, and install the SVD system as defined in the RFPs, all wiring connections to the traffic signal controllers and to the camera platformsshall be installed by the SI. The SI shall supply all the necessary equipment for thecamera and detection system, including but not limited to: computers, ancillarycamera equipment, camera housings, camera poles, warning signs and shall make the final connections to the camera

**E. E-Challan Devices**

The SI is required to supply devices for junctions to integrate in to the existing e- Challan application for spot challan issuance.

The functional requirements and technical specifications provided in this RFP are indicative and carry guiding rule. The SI is free to offer products and solutions whichmeet requirements of the RFP focusing on the outcome, future scalability, security,reliability and adherence to specified SLA under this RFP, in line with applicablestandards & best practices adopted in the industry. The SI is encouraged to designan Optimized solution which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical requirement in the RFP may be considered if it is requiredfor meeting current & future requirements during the contract period. The SI is fullyresponsible for the specified outcome to be achieved.

**5.10 Lightning-Proof Measures**

The SI shall comply with lightning-protection and anti–interference measures for system structure, equipment type selection, equipment earthing, power, signal cables laying. The SI shall describe the planned lightning-protection and anti – interference measures in the As-Is report. Lightning arrester for all pole shall be erected for the entrance cables of power line, video line, data transmission cables. Signal separation of low and high frequency; equipment's protective field shall be connected with its own public equal power bodies; small

size/equipment signal lightning arrester shall be erected before the earthling. The Internal Surge Protection Device for Data Line Protection shall be selected as per zone of protection described in IEC standards. Data line protection shall be used for security system, server data path and other communication equipment.

**5.11 Earthing System**

All electrical components are to be earthen by connecting two earth tapes fromthe frame of the component ring and will be connected via several earth electrodes. The cable arm will be earthen through the cable glands. The entireapplicable IT infrastructure i.e. field locations/traffic junctions or command centreshall have adequate earthing. Further, earthing should be done as per Local statenational standard in relevance with IS standard.

i. Install the earthing devices for the equipment, including lightning earthing, protection earthing and shielded earthing. All earthing shall meet the related industry standards.

ii. The earthing cable shall be installed in a secure manner to prevent theft and shall be rustproof. Earthing down lead and the earthing electrode shall be maintenance free.

iii. Earthing should be done for the entire power system and provisioning should be there toearth UPS systems, Power distribution units, AC units, etc. so as to avoid a ground differential. RAILTEL / DRDM/ PSCDL shall provide the necessary space required to prepare the earthing pits.

iv. All metallic objects on the premises that are likely to be energized by electric currents should be effectively grounded.

v. There should be enough space between data and power cabling and there should notbe any cross wiring of the two, in order to avoid any interference, or corruption of data.

vi. The earth connections shall be properly made.

vii. A complete copper mesh earthing grid needs to be installed for the server farm area,every rack needs to be connected to this earthing grid. A separate earthing pit needs tobe in place for this copper mesh.

viii. Provide separate Earthing pits for Servers, & UPS as per the standards.

**5.12 Junction Box / Outdoor Cabinet, Poles and Cantilever**

i. The SI shall provide the Junction Boxes, poles and cantilever to mount the fieldsensors like the cameras, traffic sensors, traffic light aspects, active networkcomponents, controller and UPS at all field locations, as per the specificationsgiven in the RFP.

ii. Each intersection shall be fitted with outdoor cabinets dimensioned to host allequipment necessary to operate enforcement systems and traffic surveillance systems as defined in this RFP.

iii. SIs shall reserve additional room in the intersection controller cabinet to accommodate the future system requirements

iv. 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. Boxesshall be dustproof and impermeable to splash-water. They shall be suitable for the Puducherry's environmental conditions.

v. The cabinets shall be of robust construction and shall include 3-point security- locking mechanisms to prevent unauthorized access to the field equipment

vi. The Junction Box for UPS with Battery bank needs to be considered separately.

vii. It should be noted that the SI should design the Junction box keeping in mindthe scalability requirements of the project.

viii. Temperature and Humidity Control: All enclosure compartments shall be equipped with a natural convection air circulation system via provision of aircirculation filters that shall not require maintenance and shall allow free circulation of air inside the enclosures to prevent overheating as well as thebuild-up and effects of humidity and heat, without permitting the entry of elements that might endanger system operation.

ix. SI shall ensure that all the hardware is placed inside the junction boxes that could withstand temperatures prevalent in Puducherry throughout the year.

x. At selected traffic junctions, if the existing infrastructure of poles and cantilevers can be used for mounting/installing the traffic light aspects then RAILTEL / DRDM/ PSCDL shall facilitate to obtain NOC from respective department forinstallation by the SI. However, SI will be responsible for obtaining all the necessary permissions etc. The details of traffic junctions/locations are providedin Annexure VIII under Section of 12.0

xi. The SI shall ensure that all installations are done as per satisfaction of Authority.

xii. For installation of CCTV Cameras, PTZ Cameras etc. SI shall provide appropriate poles & cantilevers and any supporting equipment. SI shall be required to supply, install, configure and integrate surveillance cameras at the identified locations and thereafter undertake necessary work towards their commissioning.

xiii. SI shall ensure that the poles erected to mount cameras are good, both qualitatively and aesthetically

xiv. SI shall use the industry leading practices while positioning and mounting thecameras 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.

xv. The poles shall be installed with base plate.

xvi. Base frames and screws shall be delivered along with poles and installed by the SI.

xvii. In case the cameras need to be installed beside or above the signal heads, suitable extensions for poles need to be provided and installed by the SI so thatthere is clear line of sight.

xviii. SI 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 and Variable Messaging Sign boards

xix. SI shall provide structural calculations and drawings for the approval of Authority. The design shall match with common design standards/ IS Codes as applicable under the jurisdiction of Authority/authorized entity.

xx. SI shall coordinate with concerned authorities / municipalities for installation.

xxi. Poles and cabinet shall be so designed that all elements of the field equipmentcould be easily installed and removed.

xxii. SI shall ensure that physical look of the installation area returns to neat & tidy conditions after installation of poles, cantilevers etc. The placement shall bedesigned keeping in mind the normal flow of vehicular traffic and pedestrianmovement is not disturbed.

### 5.13 Power & UPS - for Field Locations

i. SI Shall coordinate with Energy distribution Company for provision of power for field installations. Desired energy meters shall be installed in the junction box at appropriate locations. Energy consumption costs shall be borne by SI duringimplementation and O&M Period which will be reimbursed by RAILTEL / DRDM/PSCDL at actual.

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

iii. SI shall carry out a study and identify locations to provide UPS backup, depending upon power situation across city, to meet the camera and other field equipment's uptime requirements.

iv. SI shall install UPS at the identified intersections in secure, tamper-proof housingin corrosion resistant cabinets.

v. SI shall ensure that the UPS is suitably protected against storms, power surgesand lightning.

vi. SI shall provide UPS for efficient heat dissipation without air conditioning. It shallbe able to withstand temperatures prevalent in the Puducherry throughout the year.

### 5.14 Civil and Electrical Works

i. SI shall be responsible for carrying out all the civil work required for setting up allthe 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

ii. SI shall provide electricity to the cameras through the aggregation point. Sincethis component has dependency on approval from local authorities, it is recommended that SI plans this requirement well in advance & submits theapplication to the concerned electricity distribution agency with requisite fees, as applicable.

iii. SI shall carry out all the electrical work required for powering all the componentsof the system

iv. Electrical installation and wiring shall conform to the electrical codes of India.

v. SI shall make provisions for providing electricity to the cameras (PTZ and Fixed) via SJB (Surveillance Junction Box), housing the UPS/SMPS power supply, withminimum backup as defined in this RFP,

vi. For the wired Box cameras, SI shall provision for drawing power through PoE(Power over Ethernet), while PTZ cameras shall be powered through PoE+ /dedicated FRLS power cable laid separately along with STP cable.

vii. Registration of electrical connections at all field sites shall be done in the nameof Authority.

viii. SI shall house the electricity meters inside the power cabinet as mentioned inthe controller Cabinet section as above.

ix. Electricity Charges for implementation and O&M period for all the systems has to be borne by the SI and cost of electricity will be reimbursed on monthly basisto SI by RAILTEL / DRDM/ PSCDL.

### 5.15 Cabling Infrastructure

i. The SI shall provide standardized cabling for all devices and subsystems in the field.
ii. SI shall ensure the installation of all necessary cables and connectors between the field sensors /devices assembly, outstation junction box, for pole mounted field sensors /devices the cables shall be routed down the inside of the pole and through underground duct to the outstation cabinet.
iii. All cables shall be clearly labeled with indelible indications that can clearly be identified by maintenance personnel. The proposed cables shall meet the valid directives and standards.
iv. Cabling must be carried out per relevant BIS standards. All cabling shall be documented in a cable plan by the SI.

**5.16 Responsibility Matrix - Overall**

| # | Key Activities | Successful Bidder | Puducherry authority | RAILTEL & PSCDL | Infra OEMs | Electricity | Other Utilities | Other Depts | PMO/SI | Existing ICT |
|---|---|---|---|---|---|---|---|---|---|---|
| Project Inception Phase | | | | | | | | | | |
| 1 | Project Kick Off | R/A | C | C | C | I | I | I | C | I |
| 2 | Deployment of manpower | R/A | C | C | C | I | I | I | C | I |
| Requirement Phase | | | | | | | | | | |
| 3 | Assess the requirement of IT Infrastructure and Non IT Infrastructure | R/A | C | C | C | C | C | C | C | C |
| 4 | Assessment of Business processes | R/A | C | C | C | I | I | C | C | I |
| 5 | Assessment of requirement of Software requirements | R/A | C | C | I | I | I | C | C | I |
| 6 | Assess the Integration requirement | R/A | C | C | C | C | I | C | C | C |
| 7 | Assess the connectivity requirement all locations (including Building) | R/A | C | C | C | I | I | C | C | I |
| 8 | Assessment the Network laying requirement | C | C | C | R/A | I | I | C | C | I |
| 9 | Assessment of training requirement | R/A | C | C | I | I | I | C | C | I |
| Design Phase | | | | | | | | | | |
| 10 | Formulation of Solution Architecture | R/A | C | C | C | I | I | C | C | I |
| 11 | Creation of Detail Drawing | R/A | C | C | C | I | I | C | C | I |
| 12 | Detailed Design of Smart City Solutions | R/A | C | C | C | I | I | C | C | I |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 13 | Development of test cases (Unit, System Integration and | R/A | C | C | C | I | I | C | C | I |
| | User Acceptance) | | | | | | | | | |
| 14 | Preparation of final bill of quantity and material | R/A | C | C | C | C | I | C | C | I |
| 15 | SoP preparation | R/A | C | C | C | C | C | C | C | I |
| Development Phase 1 & 2 | | | | | | | | | | |
| 16 | Helpdesk setup | R/A | C | C | I | I | I | I | C | I |
| 17 | Physical Infrastructure setup | R/A | C | C | I | I | I | I | C | I |
| 18 | Procurement of Equipment , edge devices, COTS software (if any), Licenses | R/A | C | C | I | I | I | I | C | I |
| 19 | IT and Non IT Infrastructure Installation | R/A | C | C | I | I | I | I | C | I |
| 20 | Development, Testing and Production environment setup | R/A | C | C | I | I | I | I | C | I |
| 21 | Software Application customization (if any) | R/A | C | C | I | I | I | I | C | I |
| 22 | Development of Bespoke Solution (if any) | R/A | C | C | I | I | I | I | C | I |
| 23 | Data Migration | R/A | C | C | I | I | I | I | C | I |
| 24 | Integration with Third party services/application (if any) | R/A | C | C | I | I | I | I | C | I |
| 25 | Unit and User Acceptance Testing | R/A | C | C | I | I | I | I | C | I |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 26 | Implementation of Solutions | R/A | C | C | I | I | I | I | C | I |
| 27 | Preparation of User Manuals , training curriculum and training materials | R/A | C | C | I | I | I | I | C | I |
| 28 | Role based training(s) on the Smart City Solutions | R/A | C | C | I | I | I | I | C | I |
| Integration Phase 1 & 2 | | | | | | | | | | |
| 29 | SoP implementation | R/A | C | C | C | C | C | C | C | I |
| 30 | Integration with GIS | R/A | C | C | C | C | C | C | C | I |
| 31 | Integration of solutions with Command and Control Centre | R/A | C | C | C | C | C | C | C | I |
| Go –Live Phase 1 & 2 | | | | | | | | | | |
| 32 | Go Live | R/A | C | C | I | I | I | I | C | I |
| Operation and Maintenance | | | | | | | | | | |
| 33 | Operation and Maintenance of IT, Non IT infrastructure and Applications | R/A | C | C | I | I | I | I | C | I |
| 34 | SLA and Performance Monitoring | R/A | C | C | I | I | I | I | C | I |
| 35 | Logging, tracking and resolution of issues. | R/A | C | C | I | I | I | I | C | I |
| 36 | Application enhancement | R/A | C | C | I | I | I | I | C | I |
| 37 | Patch & Version Updates | R/A | C | C | I | I | I | I | C | I |
| 38 | Helpdesk services | R/A | C | C | I | I | I | I | C | I |

R/A = Responsible/Accountable

C = Consulted

I = Informed

### 5.17 Project Deliverables

| # | Key Activities | Deliverables |
|---|---|---|
| **1** | Project Kick Off | Project Plan |
| **2** | Deployment of manpower | Risk Management and Mitigation Plan |
| **3** | Assess the requirement of IT Infrastructure and Non-IT Infrastructure | Functional Requirement Specification document |
| **4** | Assessment of Business processes | System Requirement Specification document |
| **5** | Assessment of requirement of Software requirements | Requirements Traceability Matrix |
| **6** | Assess the Integration requirement | Site Survey Report |
| **7** | Assess the connectivity requirement of all locations (including Building) | |
| **8** | Assessment of network laying requirement | |
| **9** | Assessment of training requirement | |
| | | HLD documents |
| | | LLD documents |
| | | Application architecture documents |
| | | Technical Architecture documents. |
| | | Network Architecture documents. |
| | | Logical and physical database design. |
| | | Logical and physical infra-architecture |
| **11** | Creation of Detail Drawing | Data dictionary and data definitions. |
| **12** | Detailed Design of Smart City Solutions | GUI design (screen design, navigation, etc.). |
| **13** | Development of prototype (Unit, System Integration and User Acceptance) | Test Plans |
| **14** | Preparation of final bill of quantity and material | SoPs & KPIs |
| **15** | SoPs & KPIs preparation | Change management Plan |

| | | |
|---|---|---|
| **16** | Helpdesk setup | IT and Non-IT Infrastructure Installation Report |
| **17** | Physical Infrastructure setup | Training Completion report |
| **18** | Procurement of all IT & Non-IT equipment's | Application deployment and configuration report |
| **19** | IT, Non-IT and Cloud-based Infrastructure | Unit Testing Report |
| | Installation | |
| **20** | Development, Testing and Production environment setup | Functional Testing Report |
| **21** | Development of Software Application and customization (if any) | |
| **22** | Integration of Third party services/application (if any) | |
| **23** | Unit Testing | |
| **24** | Implementation of Solutions | |
| **25** | Preparation of User Manuals, training curriculum and training materials | |
| **26** | Role based training(s) on the Smart City Solutions | Integration Testing Report |
| **27** | SoP & KPIs implementation | |
| **28** | Integration with Smart Components | Completion of UAT and closure of observations report |
| **30** | Integration of solutions with Integrated Command and Control Centre | |
| **31** | Integration Testing | |
| **32** | User Acceptance Testing | |
| **33** | Go Live | Go-Live Report |
| **34** | Operation and Maintenance of IT, Non-IT infrastructure and Applications | Detailed plan for monitoring of SLAs and performance of the overall system |
| **35** | SLA and Performance Monitoring | Fortnightly Progress Report |

| | | |
|---|---|---|
| **36** | Logging, tracking and resolution of issues. | Monthly SLA Monitoring Report and Exception Report |
| **38** | Patch & Version Updates | Issues logging and resolution report |
| **39** | Helpdesk services | |

### 5.18 Project Timelines – Phase wise

| Sr. No. | Stage | Key Deliverables | Time Schedule (In month (M) / Days) |
|---|---|---|---|
| 1 | Phase1(Implementation period) | Project Management, Supply, Installation, Testing and Commissioning of ICCC and other associated activities including Go-Live. support at the time of execution and the entire project is to be rolled out on or before the T1 stage. | T0+ 6M=T1 |
| 2 | Phase 2(O & M period) | Operation and Maintenance of ICCC and other associated activities and SLA calculation. | T1+60M=T2 |
| 3 | Phase 3 | Once the project is over including O&M for five years with the adjustment of flaws, dues, penalties etc. for Handover. | T2+2M |

**T0: Date of issue of LoA/PO.**

* If the there is any delay in the implementation of the project due to the delay of SI, then the SI shall not be paid for the delay timeline & penalty may also be imposed as per penalty clause.

**5.19 Project Timelines – Component wise**

| Project Component | Deliverables | Timeline (Max Limit) | Value of Penalty |
|---|---|---|---|
| Deployment of Resources | Successful Deployment of All Resources as per project requirement | T/0+2 weeks | After T/0+2 weeks, a penalty of 2% per week on the amount to be released thereof up to the maximum value of 10% on the amount to be released. However, Delay beyond three (03) weeks would lead to termination of contract. |
| Implementation of Project | Implementation on of different milestone of the Project, i.e., the project is to be roll out in full-fledge with all certification, clearances on or before T/0+180 days | T/0 + 180 Days | After T0+180 days, a penalty of 5% on the amount to be released on completion of same milestone value per week up to the maximum value of 10% on the amount to be released on completion of same milestone. However, Delay beyond two (2) weeks would lead to termination of contract. |
| Progress Reports | Monthly Progress Reports during the implementation on period and during the O&M period | By 5th of each succeeding month | After 5th of succeeding month, a penalty of Rs. 1000 per day with a capping of Rupees 1 lakh. |
| Project Deliverables | User Acceptance Test (UAT) completion and other completion certificates enabling roll Out | T/0+180 days | After 15 days of T/0+180 days, a penalty of1 lakh per day with a capping of 15 lakh. Delay beyond 60 days would lead to termination of contract. |

T/0: The date of issuing of LOA/PO to SI

**The maximum Penalty is capped at 10% of the overall Contract value.**

If any financial penalty imposed on RailTel by Puducherry Authorities during the contract period due to non-performance/non-compliance shall be borne by SI as per the above table. In addition SI has to borne the SLA penalties / any other deductions by the Puducherry Authorities.

**5.20 Project Defect Liability Period (DLP) / Warrantee of Product & Services**

Bidder shall be responsible for Operation and Maintenance of each component(HW, SW, SW Patches, Upgrades and Service) related to this RFP for period of Five (5)-Years after final acceptance testing and handover to client.

- All hardware items should to be quoted with 5 years replacement warrantyfrom OEM and onsite support and services.
- All software/subscription/licenses should be quoted with 5 years warranty,updates, upgrades (wherever applicable), support and services from OEM"

## 6. Functional Requirement and Technical Specifications

The functional requirements and technical specifications are provided in the belowsections. The SI is free to offer products and solutions which meet requirements of theRFP focusing on the outcome, future scalability, security, reliability and adherence tospecified SLA under this RFP, in line with applicable standards & best practices adopted in the industry. All specified parameters mentioned in the scope/technicalrequirement in the RFP may be considered for meeting current & future requirementsduring the contract period. The SI is fully responsible for the specified outcome to beachieved for the project. Some of the basic prerequisites that bidder shall fulfill the under this RFP are mentioned below;

i. All hardware items shall be quoted with 5 years advance replacement warranty from OEM/Supplier/Manufacturer and onsite support and services.
ii. All software/subscription/licenses should be quoted with 5 years warranty, updates,upgrades (wherever applicable), support and services from OEM.
iii. Manufacturer Authorization Form should be submitted for each item clearlymentioning the items for which the bidder is authorized to quote.
**iv. OEM undertaking that the quoted product will not become end of sale within next 12 months.**
**v. OEM undertaking that the quoted product will not become end of support/end of life for next 5 years.**
**vi. OEM undertaking that they have not been blacklisted by any Govt./PSU in India.**
vii. Bidder should submit complete Bill of Materials for each item
viii. Incorrect/Incomplete Bill of Material may lead to rejection of bid.
ix. OEM of all active IT components should have online portal to raise tickets for supportand services.
x. Product serial numbers of all IT active components should be available in the OEMonline portal for ease of maintenance and support.
xi. OEM should have end user web interface to log case with product serial number.
**xii. Malicious Code Certificate:**
(Both Bidder and OEM should submit following certificate along with the bidocument):

"This is to certify that the Hardware and the Software being offered, as part of the contract, does not contain Embedded Malicious code that would activate procedures to:

a. Inhibit the desires and designed function of the equipment.
b. Cause physical damage to the user or equipment during the exploitation.
c. Tap information resident or transient in the equipment/network.

The firm will be considered to be in breach of the procurement contract, in case physical damage, loss of information or infringements related to copyright and Intellectual Property Right (IPRs) are caused due to activation of any such malicious code in embedded software."

**Details of Key Modules**

### 6.1 Integrated Command and Control Centre

The Integrated Command and Control Centre (ICCC) serves to collate and standardize data from various sensors for subsequent analytics and visualization together with initiating requisitealerts and standard operating procedures (SOPs) in terms of responding to incidents. Theplatform should support and be open for community development requirement and will beextended to citizens

as and when required.

**Proposed Solution**

- Monitor and utilize information of other departments for delivering services in an integrated and more efficient manner.
- Use of Big Data, ICT and infrastructure, advanced computing, analytics, and visualization to enhance the city's intelligence.
- Capturing real time information through sensors, cameras, GPS devices and citizen feedback/input.

**a) Envisaged Benefits**

For Authorities,

- Efficient planning and control mechanisms
- Seamless integration
- Addressing issues based on real time data insights
- Better administration with real-time access to data across interventions.For Citizens,
- Citizen Engagement System - Citizen Services application – Open Data Collaboration Platform for Better citizen services in a timely manner
- Improved user satisfaction

Integrated Command & Control Center capable of communicating, correlating, collaborating with other city systems, departments such as emergency response forces, utilities (energy, water and sewage), transportation, city surveillance, citizen engagement platform, Traffic Enforcement System, etc.

To improve citizen service delivery through seamless integration and proactive monitoringof departmental services, and to provide Integrate command and control center (ICCC) to Puducherry Smart City Development Ltd.

The Long term objective of ICCC is to establish a collaborative framework where input from different functional departments of PSCDL and other stakeholders such as City Corporation, City Development, Town Planning Department, transport/RTO, fire, police, e-governance etc. can be assimilated and analyzed on a single platform; consequently resulting in aggregated city level information. Further, this aggregated city level information can be converted to actionable intelligence, which would be propagated to relevant stakeholders and citizens.

As a first step is to design and commission ICCC to provide a common picture by assimilating data coming from various field devices/sensors related to traffic, surveillance, variable message signboard, Public Address System and other smart components installed on the field.

Objective is also to provide visualization / monitoring of ground situation through CCTV feed, standard operating procedures and provide support in effective decision making and response in real time manner.

6.1.1. Integrated City Operation Platform

The ICCC Platform should serve as a foundation for building the technology base of the smart city and should harness advances in digital technologies in IoT, Big Data, BI, AI, Mobile and

GIS. The Software Suite should cover a Digital platform to integrate the various urban systems and Pre -integrated Application software covering Integrated Command

and Control Center, Mobile workforce Management, Citizen Engagement . It should also act as a central system through which the city administrators can monitor and operate the various city services intelligently and efficiently.

The proposed Smart City Software Suite should at the minimum support the following services and capabilities.

| Services | Capabilities |
|---|---|
| **Seamlessly connect & monitor urban systems** | 1. It should be able to connect, collect and process data from various urban systems and detect anomalies.<br>2. It should provide an easy-to-use interface to onboard and provision sensor data and data from various applications systems |
| **Analyze data in real time and automate core processes** | 1. It should enable Intelligent automation of the workflows based on anomalies detected including actuating devices/systems and work with AI/ML system for predictive actions.<br>2. It should enable the operator to configure various types of SOPs and automate the processes |
| **Drive in-line departments operational efficiency through AI** | 1.It should support ready to deploy Smart Cities AI/ML applications for various domains to drive efficiency across various in-line departments.<br>2.It should be integrated with a tool to support composing the data, building ML models and deploy them as APIs to be used by various AI/ML applications. |
| **Build 360º situational awareness for operations** | 1. It should enable effective management of City Operations through a Integrated Command and Control Center Application System.<br>2. It should enable handling of major events and incidents that occur in the city by unifying the data from the various systems and creating a common operating picture for Situation Management. |
| **Empower city workforce with insights to respond faster** | 1. It should be integrated with Unified Workforce managementApplication system so that City Workforce across all departments can be integrated and equipped with Mobile App to efficiently run their day today activities.<br>2. It should provide complete visibility to the events and real time insight to take action faster by the workforce. |
| **Deliver civic services digitally to citizens** | 1. It should be integrated with Citizen Engagement Application System to engage with and allow citizens to raise grievances and avail civic services digitally.<br>2. The Application should support delivery of the services through grievance Case Management System, City Mobile App and City Portal integrated with Chatbot |
| **Enable community driven innovation through open data** | It should be integrated with Open Data Collaboration Platform and provide an open data-sharing platform to foster community driven innovation and to enable communities to access data and build third-party applications to deliver more services. |

| ICCC Specifications | | | |
|---|---|---|---|
| **Sl No** | **Parameters** | **Requirements** | **Compliance** |
| | | | **(Yes / No)** |
| Make : | | | |
| Model : | | | |
| 1 | Data Acquisition from Sensors/Devices | The digital platform should be a pre-integrated with IoT and AI capabilities, thus enabling the city with actionable intelligence. | |
| 2 | | The platform should be able to integrate with any type of sensor platform being used for the urban services irrespective of the technology used. The Platform shall be agnostic to communication channels such as LoRA, ZigBee, GPRS, Wi-Fi, IP Camera | |
| 3 | | It supports a secured multitenant layer to acquire and validate data collected (push/pull) from the sensor and transform rough data into valid, verified, possibly corrected data. | |
| 4 | Edge Analytics | It should preprocess the data in real-time from the sensors using Edge computing capability. | |
| 5 | | The Platform should provide integration support with low code,, highly secured integration with edge devices . | |
| 6 | | ICCC application should enable local and real-time analytics on the continuous streams of data from vehicles, systems, appliances, devices and sensors of all kinds | |
| 7 | | The ICCC Application should integrate with domain specific IoT Edge application which should be working, even it gets disconnected from the IoT Edge Application cloud backend. It needs to store messages that would go upstream and saves them until the device reconnects. Also, it should be able to authenticate modules and child devices so that they can continue to operate. | |
| 8 | | The Edge Analytics from domain specific applications should work in conjunction with centralized analytics systems at ICCC, it should further provide efficient time analytics across the whole IoT ecosystem. | |

| | | | |
|---|---|---|---|
| 9 | | ICCC should integrate with Domain specific Edge Applications which are made up of two components that work independently: | |
| 10 | | 1. IoT Edge modules with containers that runs the Domain specific IoT Edge services | |
| 11 | | 2. Domain specific Modules deployed to IoT Edge devices and executed locally on those devices. The IoT Edge Management should run on each IoT Edge device and manage the modules deployed on each device. | |
| 12 | Network Protocol Adoption | It should support bi-directional communication between platform and the sensor system. | |
| 13 | | It should be network and protocol agnostic. | |
| 14 | | The platform should be able to collect and aggregate data in real time from on-field sensors/Edge Infrastructure like Bin Sensors, Water Sensors, Environment Sensors, Access Sensors, and Actuators etc. | |
| 15 | | The Platform should support industrial protocols like OPC UA BACNET (can be achieved through OPC UA, Modbus, IEC and Serial communication) and IOT (LoRA, MQTT, Stomp, AMQP etc.). | |
| 16 | | The Platform shall integrate with domain specific applications which include a broad range of Device Integration services for establishing the I/O interface to field devices such as RTU's, PLC's, IBMS etc. systems with bi-directional control. Similarly, it should seamlessly integrate with IoT devices/Sensors/gateways and applications. | |
| 17 | | The Platform should provide the user with the ability to change the encryption keys, without any interruption to the operation of the system. | |
| 18 | | The Platform should set up individual identities and credentials for each of the connected devices and help retain the confidentiality. | |
| 19 | Backbone Messaging | The Platform should have a Backbone Messaging System like Kafka for building horizontally scalable real-time data pipelines to receive, store, route and deliver messages. | |
| 20 | | Platform shall contain Plug and play approach to integrate with diverse M2M Protocols/ (IOT protocols ) | |

| | | | |
|---|---|---|---|
| 21 | System | The backbone messaging system, should be highly durable to handle all the incoming messages and it should be able to prioritize and allow the message to jump the queue based on the priority. | |
| 22 | Data Normalization | The Platform shall automate the steps required to analyse data from IoT devices. It should transform and enrich IoT data before using it for real-time analytics and time-series data storage for analysis. | |
| 23 | | It should support transformation of messages from native protocol of devices to a common format and should have data transformation adaptors to perform better analytics on runtime. | |
| 24 | | It should be agnostic to sensor technologies and integrate with various types of sensor platform. | |
| 25 | | The Platform should allow normalization of all the in-coming data from different devices of various OEMs. | |
| 26 | | The data Normalization approach shall be using Visual programming (no code or low code) that helps the administrator to provision various types of sensors and devices and normalize the data. | |
| 27 | | With the help of the built-in ETL platform, the platform shall cleanse the data, transform and load the data to create an error free data pool, and provide secure access to that data using data API(s) to application developers. | |
| 28 | | The Smart City digital platform should be pre-integrated with API & ESB Integration System/ API management system that enables various smart city applications to be integrated covering existing and proposed new applications in a seamless manner and provide service automation. | |
| 29 | | API Management System shall support various integration methods through - API, Sockets, OPC UA (SCADA API), APIs, etc. | |
| 30 | API Management | The platform should enable contextual information and correlation across domains and verticals (Multiple vendor and Multi-sensor in future | |

| | | | |
|---|---|---|---|
| 31 | System | The API & ESB subsystem/API management system shall cover - API gateway, Key Manager, API Portal, ESB and Analytics & Monitoring. | |
| 32 | | API Management System shall be capable of supporting policy enforcement for API subscriptions, application creation, etc. with the help of customizable workflows. | |
| 33 | | API Management System shall have custom behaviour capability on lifecycle transitions from cradle to grave: create, publish, block, deprecate, and retire | |
| 34 | | Normalized APIs for the City Application domains should be available (Parking, Outdoor Lighting, Traffic, Environment, Urban mobility etc.) to monitor, control sensor and/or actuators functionality to enable app developers to develop apps on the platform. For example, Lighting APIs: Vendor agnostic APIs to control Lighting functionality | |
| 35 | | API Management System should possess Cross collaboration APIs: Enabling contextual information and correlation across domains and verticals (Multiple vendor and Multi-sensor in future) | |
| 36 | API Gateway | The platform should enable decentralized API management policies | |
| 37 | Key Manager | The platform should authenticate and authorize API requests from any client or device types that requests the resource servers which are operating on traditional and microservice architectures. | |
| 38 | API Portal | The API portal shall be the repository of standard APIs for consumption by any third-party applications/ sub-systems | |
| 39 | | Normalized APIs should be available to carry out integration with other platforms/applications | |
| 40 | | Enables City and/or its partners to write software adaptors based on the API(s) provided by device vendors and have the ability to control, monitor and collect the data from these street devices | |
| 41 | | API Management System should support API composition, protocol and data transformation | |

| | | | |
|---|---|---|---|
| 42 | Manage and Scale API Traffic | API Management System should be capable of enforcing rate limiting and dynamic throttling based on usage quotas and bandwidth quotas | |
| 43 | | API Management System should be able to protect API backends with limit throttling capability | |
| 44 | | API Management System should possess extremely high-performance pass-through message routing capability with minimal latency | |
| 45 | Monitor and Monetize | API Management System shall be able to publish API usage to a pluggable analytics framework (Analytics framework includes - requests, responses, faults, throttling, subscriptions and self-sign ups etc.) | |
| 46 | | API Management System should be capable of monitoring SLA compliance | |
| 47 | | API Management System should be able to integrate with centralized Logging and Monitoring platform to provides the following services: | |
| 48 | | API Management System shall have Statistical graphs for API latency and API usage comparison to monitor API and application performance | |
| 49 | | API Management System shall have the ability to analyze logs pertaining to application errors, API deployment stats, Login errors, number of API failures and access token errors | |
| 50 | | API Management System track consumer analytics per API, per API version, per tier and per consumer usage | |
| 51 | | API Management System should have configurable payment schemes to monetize API usage through policies | |
| 52 | Services and Protocol Support | API Management System should possess integrated ESB solution / API management system capability of ensuring pluggable approach to Smart City Applications | |
| 53 | | API Management System should have pre-configured connectors across various Smart City Solution vendor, payments gateways, CRM, ERP, social networks or legacy systems | |

| | | | |
|---|---|---|---|
| 54 | | API Management System should support formats & protocols such as JSON, XML and SOAP etc. | |
| 55 | | API Management System should support Network transport protocols such as HTTP, HTTPS, WebSocket. | |
| 56 | | API Management System should have adapters to COTS systems such as SAP BAPI and IDoc, IBM WebSphere MQ, Oracle AQ and MSMQ | |
| 57 | Route, Mediate and Transform Data | API Management System should possess following routing capabilities such as header based, content based, rule-based and priority-based routing | |
| 58 | | API Management System should possess mediation capability to support all Enterprise Integration Patterns (EIPs), database integration, event publishing, logging & auditing and validation | |
| 59 | | API Management System should possess payload transformation capability. | |
| 60 | API & Interface Security | The access to data should be highly secure and efficient. | |
| 61 | | Access to the platform API(s) should be secured using API keys. | |
| 62 | | API Management System should support security standards: OAuth 2.0, HTTPS over SSL, and key management help protect the data across all domains. | |
| 63 | | API Management System 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. | |
| 64 | | API Management System should be capable of having security policies ensured for all APIs exposed which would | |
| 65 | | Restrict API access tokens to domains/Ips, | |
| 66 | | Validate APIs payload contents against a schema | |

| | | | |
|---|---|---|---|
| 67 | Control Access and Enforce Security | Ensure all API access to the system rely only on OAuth2 standard | |
| 68 | | Ensures Integrated Identity Server for application registration, OAuth2 token generation & validation | |
| 69 | | API Management System should be capable of blocking the subscription for an administrator and to restrict a complete application | |
| 70 | | API Management System should be capable of configured Single Sign-On (SSO) using SAML 2.0 for easy integration with existing web apps | |
| Data Processing Layer | | | |
| 71 | Complex Event Processing Engine | The Smart City digital platform should be pre-integrated with Complex Event Processing System with BPM enabling the configuration of the Policy, alarm management and execution of SOPs. The system shall provide extensive capabilities in detecting anomalies and also correlating anomalies across various city domains. | |
| 72 | | The Complex Event Processing sub-system should be cloud ready that captures events from the Platform and diverse data sources, processes the data, executes complex conditions, and acts on the same through predefined Business process and rules. | |
| 73 | | The Complex Event Processing sub-system shall allow the city to create complex analytics on sensor data with Adaptive Intelligence | |
| 74 | | The Complex Event Processing sub-system shall have a drag and drop functionality using which rules can be applied to a single stream of data or multiple streams from interconnected sensor systems. | |
| 75 | | The Complex Event Processing sub-system shall process and scale to handle millions of events in real time with in the time range of 1 to 5 seconds. | |

| | | | |
|---|---|---|---|
| 76 | | The Complex Event Processing sub-system shall support streaming and complex event processing types such as filters, streaming aggregations, patterns, non-occurrence, anomaly detection, Aggregative Functions (window based, or Start Based, Group based), Joins (works with Windows) Pattern, Sequence, Geo Spatial and etc. | |
| 77 | | The Complex Event Processing sub-system shall have Out of the box support for event sources from the Platform like HTTP, TCP, Kafka, JMS, MQTT, Email, File, RabbitMQ and social media platforms etc. | |
| 78 | | The Complex Event Processing sub-system shall support for in-memory data storage and rich data integration via out-of-the-box store connectors for RDBMS like MSSQL, Oracle, MySQL, Maria, Postgres, MongoDB, HBase, Cassandra, Solr, Redis, Elasticsearch and Hazelcast etc. | |
| 79 | | It should provide an integrated development environment to develop Object Model (OM) which defines the elements and the relationships | |
| 80 | | It should be able to deal with the change in operational systems based on the operator's decision | |
| 81 | | The Complex Event Processing sub-system shall Integrate with REST services and clients to retrieve live analytics and stored data and access management services. | |
| 82 | | The Complex Event Processing sub-system should allow Application to | |
| 83 | | Generate alerts based on thresholds | |
| 84 | | IF, Then Else analysis - Based on input | |
| 85 | | The Complex Event Processing sub-system should calculate aggregations over a short window (time, length, session, unique, etc) or a long time period | |
| 86 | | Average, Sum etc | |

| | | | |
|---|---|---|---|
| 87 | | The Complex Event Processing sub-system should perform Analytics based on geo spatial data which includes | |
| 88 | | Alert based on geo boundaries - Geo Fencing | |
| 89 | | Distance Travelled | |
| 90 | | Speed | |
| 91 | | The Complex Event Processing sub-system should calculate aggregations over long time periods with seconds, minutes, hours, days, months & years granularity | |
| 92 | | Correlate data while finding missing and incorrect events | |
| 93 | | Detect temporal event patterns | |
| 94 | | Analyse trends (rise, fall, turn, tipple bottom) | |
| 95 | | Run pre-treated machine learning models (PMML, TensorFlow) | |
| 96 | | Learn and predict at runtime using online machine learning models | |
| 97 | | It should support Static rule processing, Context specific rule processing, | |
| | | Dynamic rule processing, Decision making through synchronous stream processing, Query tables, Windows and Aggregation. | |
| 98 | | It should serve the following value propositions, | |
| 99 | | - Ability to respond to real-time data with intelligent & automateddecisions | |
| 100 | | - Should provide an environment for designing, developing, anddeploying business rule & event applications | |
| 101 | | - Should provide an integrated development environment to develop Object Model (OM) which defines the elements and the relationships | |
| 102 | | - Should be able to deal with the change in operational systemsbased on the operator's decision | |
| Data Analytics Layer | | | |

| | | | |
|---|---|---|---|
| 103 | Analytics Engine | The Smart City digital platform OEM should be pre-integrated with analytics engine to enable necessary insights and analytics. | |
| 104 | | The Analytics sub-system should be an AI-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. | |
| 105 | | The platform shall be pre-integrated with analytics to perform multi-dimensional analysis on incidents data supporting business intelligence and machine learning capabilities that enable delivery of pre-packaged analytics applications like dashboard, reports, advanced analytics - disaster management, social analytics, etc. | |
| 106 | | The Platform shall be integrated with analytics engine, and which shall support following capability. | |
| 107 | | The Analytics sub-system should support multiple Data Sources. Min below standard data sources should be supported from day 1 – CSV, TSV, MS Excel, NoSQL, RDBMS | |
| 108 | | The Analytics sub-system should be able to discover, compare, and correlate data across heterogeneous data sources to unravel the patterns that are previously hidden. At a broader level system shall support following tasks: | |
| 109 | | Connect to a variety of data sources | |
| 110 | | Analyze the result set | |
| 111 | | Visualize the results | |
| 112 | | Predict outcomes | |
| 113 | | The Analytics sub-system should be capable of performing descriptive, predictive, and also prescriptive analytics wherever applicable. | |
| 114 | | The Analytics sub-system should have capability to analyse data in motion to display the alerts in real-time and store the data in centralized database for future trend analysis. | |

| | | | |
|---|---|---|---|
| 115 | | The Analytics sub-system should be capable of developing predictive analytics based on the requirements of the city. Domains can range from Solid Waste, Transport etc. | |
| 116 | | The Analytics sub-system should provide with end user access ranging from ETL, integration of data from structured & unstructured data sources, intelligence with simulation and modelling and interactive dashboards with ad-hoc query, integration with spreadsheets, proactive alerting, Scorecards and so on. | |
| 117 | | The Analytics sub-system should provide capabilities to create KPIs to measure progress and performance over time and graphically communicate strategy & strategic dynamics using Strategy maps, Cause and Effect diagrams, and Custom views. Intuitive and dense visualizations must be available. | |
| 118 | | The Analytics sub-system should help simulate what if scenarios. It should help visualize assets/resources at risk due to the pending/ongoing incident, should render impacted region on a GIS/2D map. The solution should help build the list of assets, their properties, location and their interdependence through an easy-to-use Graphical User Interface. Solution should highlight not only the primary asset impacted but also highlight the linked assets which will be impacted. | |
| 119 | | The subsystem should be capable of providing time-shifted or offline analytics on the archived data. | |
| 120 | | It should provide capabilities for the analysis to run autonomously, refreshing data and re-analyze the situation continuously across a complex set of variables. | |
| 121 | Analytics Engine Visualizations | Analytics sub-system should provide visualizations dashboard. | |
| 122 | | In the visualization workspace, it should allow to change visual attributes of a graph. | |
| 123 | | User should not be allowed to alter the graph/visualization definition. | |
| 124 | | In the visualization workspace, user should be able to do the following operations: | |
| 125 | | - Change the graph/visualization type | |
| 126 | | - Print the graph | |

| | | | |
|---|---|---|---|
| 127 | | - Export the graph | |
| 128 | | - Narrow down on the value ranges | |
| 129 | | - Toggle the axis labels | |
| 130 | | - Integrate with other 3rd party applications seamlessly | |
| 131 | Sentiment Analytics | The Analytics sub-system shall have the capability to provide sentiment analytics of configured key words/accounts through internet crawling through the platform. Ability to categorize key issues/topics/words in real time on social media platform (Instagram ,Twitter, Facebook, Website Discussion Forums, News Papers) which are contributing to negative/positive perception among citizens. | |
| 132 | AI Data Pre-Processing | Platform should enable machine learning with big data, providing the ability to obtain valuable insight from large amounts of structured, unstructured and fast-moving data | |
| 133 | | Platform should enable organization and labelling of data by the intelligent methods of alignment and indexing | |
| 134 | | Platform should be capable of handling missing data | |
| 135 | | Platform should support data cleaning operations. | |
| 136 | ML Libraries | Platform should be capable of native support for asynchronous execution of collective operations and peer-to-peer communication | |
| 137 | | Platform should allow user to export models in the standard file formats (Pickle, H5, ONNX) | |
| 138 | | Platform should enable fast, flexible experimentation and efficient production through a hybrid front-end, distributed training and ecosystem of tools & libraries | |
| 139 | Model Store and Service | Platform should allow the user to convert ML model to a bitstream, store it in disk and reloaded at any point of time. | |
| 140 | | Platform should allow the user to do real time and batch predictions using the models | |

| | | | |
|---|---|---|---|
| 141 | | Platform should create an API wrapper around the predicted model and should be capable of deploying it as a web-service | |
| Common Enabling System | | | |
| 142 | Business Process Management | The Smart City digital platform shall have the capability of integration with Business Process Management (BPM) sub-system that would enable the process automation, delegation, parallel workflows, etc. | |
| 143 | | It should be capable of handling parallel process flows, that would carry out all possible combinations including split, merge and cross reference of processes. | |
| 144 | | It should also enable the user to delegate or assign an activity to individuals or teams. | |
| 145 | GIS Map Support | Platform must provide ability to configure various geo-spatial data from different providers including but not limited to City GIS systems | |
| 146 | | Platform must provide ability to support different geo spatial formats from commercial and open geospatial standards. | |
| 147 | | System should support integration with any Map API services like Google, Esri, Open Street, etc. It should be possible to visualize all the Assets (Sensor, Devices, Vehicles, Cameras, other city resources) on map. | |
| 148 | | It should be possible to visualize all the Assets (Sensor, Devices, Vehicles, Cameras, other city resources) on map. | |
| 149 | | The Assets must be provided as layers with ability to switch these layers and visualize the assets of only selected layers. | |
| 150 | | The GIS Maps should provide interactive visualization of travel time and traffic based on the sensor data and data ingested from 3rd party sources. | |
| 151 | | It should allow the operator to execute dynamic messaging across the city through the sign boards to inform the citizens in real time. | |

| | | | |
|---|---|---|---|
| 152 | | GIS Platform shall support GIS Maps in following file format PDF, JPG, PNG, Vector PDF Map , Web Map Service (WMS), GeoJson defined by the Open Geospatial Consortium (OGC), Google Map-aerial; terrain, Bing Map, aerial, satellite, hybrid, ArcGIS/ESRI and Open Platform GIS Applications. | |
| 153 | | GIS platform should provide a picture-in-picture map view capability, | |
| 154 | | Upon the availability of GPS positioning of a file, the user should be able to quickly alternate between the video and map view within the video player | |
| 155 | | The application must be able to ingest and present either a static location (e.g., for a fixed camera) or dynamic location (e.g., for mobile cameras) that allows users to validate the location where the video was recorded at the time of the event | |
| 156 | Location engine | Map services and geospatial coordinates: Shall provide the geographical coordinates of specific facilities, roads, and city infrastructure assets. | |
| 157 | | Geospatial calculation: Shall calculate distance between two, or more, locations on the map | |
| 158 | | Location-based tracking locates and traces devices on the map | |
| Security | | | |
| 159 | | The Platform should set up individual identities and credentials for each of the connected devices and help retain the confidentiality | |
| 160 | | The Platform should provide mutual authentication and support encryption at all points of connection, so that data is never exchanged between devices and IoT Platform without a proven identity. | |
| 161 | | To maintain the integrity of the system, the Platform shall allow the user to selectively revoke access rights for specific devices as needed. | |

| | | | |
|---|---|---|---|
| 162 | IoT Security | To ensure the flexibility for the device vendor, the platform should allow the user to create Authentication and Authorization policies based on device profile level, it shall also support the below policies: | |
| 163 | | a) Standard Authentication | |
| 164 | | b) Custom Authentication | |
| 165 | | c) x.509 Certificate based Authentication | |
| 166 | | Standard Authentication should comprise of Time-based password for the device to ensure that in case the device gets compromised, it can only utilize the token for the defined time. | |
| 167 | Security-IoT Device Identity Registry | All IoT Device connecting to the IoT Platform shall be secured through strict device Identity Policies and token-based authentication | |
| 168 | | The Platform shall Support AES 128, 256 Based Payload Encryption. | |
| 169 | | The Platform shall have Per device authorization policies to ensure zero data leak tolerance. | |
| 170 | Security-User Identity and Access Management | Role based access shall be enforced for all application activities. | |
| 171 | | The Platform should support LDAP to be used as an additional data store for user management and authentication. | |
| 172 | | Shall have Single Sign on and Multi factor authentication for secure user access to application services | |
| 173 | Data Security & Integrity | Data Governance / Role Based Access Control: The Platform should support data governance & stewardship model, in which roles, responsibilities are clearly defined, assigned, implemented, documented and communicated | |
| 174 | | Data Protection / Production Data integrity: The Platform should support procedure in place to ensure production data shall not be replicated or used in non-production environment | |
| 175 | | Data Protection / Data at rest: The Platform should support encryption for tenant data at rest (on disk/storage) | |

| | | | |
|---|---|---|---|
| 176 | | Data Retention: The Platform should support capabilities to enforce tenant data retention policies | |
| 177 | | Data recover & restore: The Platform should support capability to recover and restore data in case of a failure or data loss. | |
| 178 | | Data disclosure & privacy: The Platform should disclose data attributes, elements collected from source. All the attributes should be disclosed & appraised to data owner. With appropriate approval from City authority, Platform should have ability to encrypt sensitive data element at rest. | |
| 179 | Configuration of Data Security Features | The Platform shall have the ability to configure user access and authorization control to provide specific set of information/data/application control to designated or authorized set of users. For E.g.: Ability to restrict water department operation team to view water billing data (if not authorized). | |
| 180 | Cybersecurity framework and security | A Cybersecurity framework as per guidelines of MoHUA should be integrated with ICCC aimed at building a secure and resilient application for citizens and stakeholders of Smart City. The framework comprising of policy, procedures, and guidelines should be designed to protect the application and information; build capabilities to prevent and respond to cyber-attacks; and minimize damages through cyber-attacks. | |
| 181 | Data Governance | The Platform shall be Integrated with data governance to ensure only authorized owner have permission to read / write data into the system. | |
| 182 | | The Platform shall allow storage encryption to prevent illegal data and behavioral tracking activities | |
| 183 | | The Platform shall assure data quality in terms of accuracy, accessibility, consistency, completeness and updating. | |
| 184 | | The Platform shall Govern all aspects of API Access services including data service descriptions, data consumption, service usage, service discovery, service lifecycle management and service policy | |
| 185 | | Monitoring - all the data access from the application shall be logged and monitored | |
| 186 | | The Platform shall integrate with a centralized logging and Monitoring platform which integrates with all part of platform services for Audit and performance monitoring. | |

| | | | |
|---|---|---|---|
| 187 | Centralized Logging & Monitoring Platform | The Centralized Logging and Monitoring sub-system should be integrated with all smart city application and the IoT platform to give the user an operational view | |
| 188 | | The logging and monitoring system should be able monitor the application/platform infrastructure for performance with time series view of: | |
| 189 | | - Up time | |
| 190 | | - CPU Utilization | |
| 191 | | - Network Utilization (Bytes received per second, Bytes sent persecond, Packet drops and Timed out connection) | |
| 192 | | - User connection count | |
| 193 | | - Disk connection count | |
| 194 | | - Process Count | |
| 195 | | - Total threshold count | |
| 196 | | Platform should keep track of sensor last seen date and time and be able to detect disconnected sensors & raise alarms | |
| 197 | | The Platform shall allow time shifted analytics with the log data. | |
| 198 | | The user should be enabled to control all the platform service from a single system, the control operation includes | |
| 199 | | - Service Restart | |
| 200 | | - Update Configuration | |
| 201 | | The system should allow user to get detailed SLA monitoring along with SLA report | |
| Provisioning and Administration Tool | | | |
| 202 | | The ICCC platform shall provide solution for enabling end to end Platform Administration which includes Asset Management, Rule Configuration & Workflow Management. | |
| 203 | | The solution shall have a view of all the sensors connected to the platform with their health status for real time monitoring. | |
| 204 | | The solution shall support secure device onboarding process with bulk uploading options. | |
| 205 | | The solution shall enable remote device management capabilities via API. | |

| | | | |
|---|---|---|---|
| 206 | Provisioning & Service Management | The solution shall support remote health monitoring and managing capability | |
| 207 | | The solution shall be capable of sensor health abnormality detection and automated workflow execution with integrated workforce app. | |
| 208 | | The solution should provide icon-based user interface on the GIS map to report non-functional assets. | |
| 209 | | The solution should also provide a single tabular view to list all assets along with their availability status in real time. | |
| 210 | | The solution should allow maintenance personnel to manage and plan incoming work requests and automatically generated work from preventive maintenance programs. | |
| 211 | | The solution should provide proactive maintenance alerts (by analysing live data and historic maintenance data) | |
| 212 | | The solution should provide accurate and up to date warranty tracking from the date of commissioning, product lifecycle management, alerts on warranty expiry dates for devices/ sensors | |
| 213 | | The solution shall provide all the capability to provision the sensor/device, normalize, create policy, SOP and build the necessary workflow for deployment. | |
| 214 | | The solution should provide access or restrict access to user group for any actuators/devices. | |
| 215 | | The Asset Management functionality of the tool should enable to manage events such as generating service order request for faulty and disconnected. | |
| 216 | | Asset Management should be capable of policy configuration such as preventive maintenance scheduling based on asset maintenance frequency, installation date, Schedule asset shut down or restart on pre-defined date and time | |
| 217 | | Asset Management should have capability of pre-defined SOPs such as Notify service provider in case of asset failure | |
| 218 | | Intentionally left Blank | |
| 219 | | Asset Management should support creating check list for field work force units for performing asset maintenance | |
| Machine Learning Builder capability | | | |

| | | | |
|---|---|---|---|
| 220 | Machine Learning Builder | ML Learning Builder should provide an environment to build machine learning models through low-code/no-code visual toolkit for developing, deploying, and operating enterprise AI ML driven applications. | |
| 221 | | The system also supports traditional ML models, time series forecasting, and deep learning. | |
| 222 | | There shall be a tool for the city administrators to create analytics / predict outcomes, when necessary, the tool provided shall allow the user to develop models for analytics using the necessary data available to the user. | |
| 223 | | The Machine Learning Tool should have an easy-to-use, visual interface that gives users the access to data exploration. | |
| 224 | | The Machine Learning Tool shall support data input from multiple data Sources for data accumulation. | |
| 225 | | The Machine Learning Tool supports ready to use ML Pipeline for prediction, recommendation, | |
| | | optimization, forecasting, Natural Language Processing, Anomaly detection. | |
| 226 | | The Machine Learning Tool should support users to choose from multiple Machine Learning Model types like (Not limited to:) | |
| 227 | | - Auto ML: Users can select this option and the system automatically selects the Algorithm based on best accuracy | |
| | | - Manual ML: Users can select Algorithms manually and provideparameters based on the selected Algorithm | |
| 228 | | - Geo ML: Users can select ML Algorithms especially built forGeospatial Data. | |
| 229 | | Users can Export files in multiple data formats (CSV, PDF, Excel etc.) | |
| 230 | | The Machine Learning Tool shall allow the users to load disparate data sources and join, filter, and wrangle data, all without having to write queries. | |
| Dashboard | | | |
| 231 | Configurable Dashboard | Configurable Dashboard should help in reducing the customization time for building the dashboard. | |
| 232 | | Configurable Dashboard should provide a single web interface for configuring the data source to visualize the data using various visuals available | |

| | | | |
|---|---|---|---|
| 233 | | Application should allow to connect various data sources for fetching the data. The Configurable Dashboard shall provide the user to connect with any data source provided in the application for fetching the data and later can be configured in the widgets | |
| 234 | | Standard Dashboard templates should be available for various Smart City Domains- Surveillance, Traffic, Environment, Parking, Waste Management, Energy, Buildings | |
| 235 | | The application should provide GIS based visuals for geospatial analysis. | |
| 236 | | The application should allow user to configure the basic settings, colour theme, etc. which need to get updated throughout all the widgets built | |
| 237 | | The application will allow user to create widgets or similar which can be used for building the dashboard. Once the widget configuration is done, the same widget can be used in multiple dashboards without the need to create multiple times | |
| 238 | | The user should be able to fetch the data from the saved data source and configure the dataset for the selected widget. | |
| 239 | | The user should be able to view the configured widgets which user can bring a common place and create the layout as per the need. | |
| 240 | | The user should be able to save the dashboard and can get shareable link which can be used to embed the dashboard in any application | |
| 241 | | The user should be able to create a KPI defined on top the connected data source. If the KPI has been met, a pre-defined process should be executed. | |
| 242 | | ICCC Application shall integrate with other Smart City Applications/E-Governance Platform | |
| 243 | | a) Smart parking system | |
| 244 | | b) Intelligent Traffic Management System - Adaptive Traffic Control<br>System (ATCS), Red Light Violation Detection (RLVD) and | |
| | | Automatic number-plate recognition(ANPR), Automatic Traffic Counter and Classifier (ATCC) & Speed Violation Detection (SVD) | |
| 245 | | c) City Surveillance system - CCTV/PTZ camera with video analyticscapabilities | |
| 246 | | d) Environment management system - Environmental sensors | |

| | | | |
|---|---|---|---|
| 247 | | e) Variable Message Board (VMD), | |
| 248 | | f) E governance - Citizen Engagement System - Citizen Servicesapplication – Open Data Collaboration Platform | |
| 249 | | g) Storm Water level Monitoring system | |
| 250 | | h) Smart Street Lighting system - Smart Street light controllers(CCMS) | |
| 251 | | i) GIS platform integrated with Command-and-Control Center | |
| 252 | | j) Smart Poles with Emergency Call Box, Public Announcementsystem, Smart Street lighting, digital billboard, public Wi Fi, etc. | |
| 253 | | k) Information Kiosk | |
| 254 | | l) OFC network. | |
| 255 | | m) The Integration with existing/proposed ICT systems as below are also envisaged, Water/sewerage SCADA, Electrical SCADA, e- Health, Public Bike Sharing System, Transport Monitoring centre,ERSS (Dial 100/112). | |
| 256 | General Capabilities | The application should: | |
| 257 | | - help the city operators to run the city efficiently by integrating allthe alarms and provides an easy-to-use GUI interface (web & client server) | |
| 258 | | - help manage: alarms, map-based visualization of the city assetsand events, execute SOPs and coordinate the operations; | |
| 259 | | - provide 360-degree situational awareness and insights acrossurban functions to city administrators. | |
| 260 | | Based on the incident type, system shall open the activities that need to be carried out for the incident. The SOP shall provide the actions like notification, correlate, dispatch, and close incident. This activity should be defined in the administrator system for each type of incident. This activity will be either manual or automated. | |
| 261 | | It should be integrated with a real-time KPI dashboard that will provide 360-degree situational awareness of the various urban system operations and efficiency. | |

| | | | |
|---|---|---|---|
| 262 | Alarm Management | The alarm management module should: | |
| 263 | | a) enable the ICCC to service all alarms generated automatically by the city digital platform for operators to visualize the alarms, create incidents and dispatch city workforce for action. | |
| 264 | | b) provide the details about each alarm received from the varioussub-systems integrated. | |
| 265 | | c) provide the operator details regarding the source of the alarm,type of alarm, generated time, priority, and elapsed time to takeappropriate action. | |
| 266 | | d) provide advanced map & video visualization for situationawareness. | |
| 267 | | e) provide an easy use GUI that is simple to operate. | |
| 268 | | f) operator to view various types of alerts in a single place andvalidate the alerts for further processing. | |
| 269 | GIS Visualization | The application shall provide map-based visualization for all the details of the alarms and enable the operator in decision making. | |
| 270 | | Application enables visualization of all the assets (camera, access control, lighting) on the GIS map as a layer. | |
| 271 | | Unique identification (icon /symbol) should be provided for each of the asset types. | |
| 272 | | The application shall allow health status (functional /non-functional) of assets to be identified using colour code. | |
| 273 | | All field resources (vehicles /field workforce) should be location enabled and mapped to the GIS with unique identification (icon /symbol). | |
| 274 | | Each of the asset shall be created as a layer on the map and can be turned ON /OFF by the operator depending upon the alarm type and incident use case. | |
| 275 | | The application shall enable operator to search assets based on the type and jurisdiction and enables operator to object based interactive building floor plan, parking lot layouts, bus inside, etc. | |
| 276 | Video | The application shall provide video-based visualization of all the associated cameras for the alarms in matrix view and enables the operator in decision making. | |
| | | Selection of cameras can be based on the following: | |

| | | | |
|---|---|---|---|
| 277 | Visualization | a) Map based selection | |
| | | b) Jurisdiction/ camera selection from the camera list alert thedetails of the alerts | |
| 278 | | The application should: | |
| 279 | General Capabilities | 1. provide a 360-degree view of the situation lifecycle covering Preparedness, Response, Recovery and Mitigation. | |
| 280 | | 2. provide a portal for all the major incidents/events and help in coordinating and managing response. | |
| 281 | | 3. help monitor, control, and effectively take measures to save lives and properties during any situation. | |
| 282 | | The system should have intelligence of the emergency policies and procedures for streamlined information sharing among multiple agencies. | |
| 283 | | The application should provide a rich GUI based web console through which the administrators can monitor and respond intelligently and efficiently to a situation. | |
| 284 | | The application should have the capability to integrate with industry standard video management systems, video analytics and unified communication to support advanced situational awareness. | |
| 285 | | The application should provide a single view of all the active situations to the operator in the home screen and the status of the associated events against each situation such as the time for completion of an activity, escalated activity due to SLA breach etc. | |
| 286 | | The Application should provide a GIS based visualization of the various locations of the events within a particular incident | |
| 287 | | There should be provision to create or modify a situation | |
| 288 | | The application should provide a repository of pre-defined SOPs to be executed for a situation event management, incident management, call receipt, health and safety etc. | |
| 289 | | Application should allow operator to define SOP based on the situation | |
| 290 | | The Situation Management System supports decision makers with a powerful machine learning based solutions to build domain specific predictive analytics capabilities. The system further enables the decision maker to get complete visibility of the events, assets and support impact analysis. | |

| | | | |
|---|---|---|---|
| 291 | | The situation management application should also be integrated with ICCC. Based on the nature of the incident and the associated location intelligence and situational awareness the ICCC operator can qualify an incident to be a possible situation and alert the situation management operator. The situation management operator should be provided with advanced visualization capabilities with ability to correlate various incidents as a situation. | |
| 292 | Standard Operating Procedures (SOPs) | ICCC platform shall provide for authoring and invoking un-limited number of configurable and customizable standard operating procedures through graphical, easy to use tooling interface. | |
| 293 | | Standard Operating Procedures shall be established, approved sets of actions considered to be the best practices for responding to a situation or carrying out an Operations. | |
| 294 | | The users shall be able to edit the SOP, including adding, editing, or deleting the activities. | |
| 295 | | The users shall be able to also add comments to or stop the SOP (prior to completion). | |
| 296 | | There shall be provision for automatically logging the actions, changes, and commentary for the SOP and its activities, so that an electronic record is available for after-action review. | |
| 297 | | Platform must be able to create SOP workflows | |
| 298 | | Workflow must support both automated and manual activities (tasks) and each of the activity should be configurable | |
| 299 | | The SOP Tool shall have capability to define the following activity types: | |
| 300 | | Manual Activity - An activity that is done manually by the owner and provide details in the description field. | |
| 301 | | If-Then-Else Activity - A conditional activity that allows branching based on specific criteria. Either enter or select values for Then and Else. | |
| 302 | | Notification Activity - An activity that displays a notification window that contains an email template for the activity owner to complete, and then sends an email notification. | |
| 303 | | SOP Activity - An activity that launches another standard operating procedure. | |
| 304 | | Platform should support simple and complex event processing in real time | |
| 305 | | Platform must be able to raise events based on thresholds | |

| | | | |
|---|---|---|---|
| 306 | | Platform must be able to raise events based on conditions happening in a time window | |
| 307 | | Platform must raise events based on one or more events | |
| 308 | | Platform must map SOP workflows with event | |
| 309 | | Platform should provide an ability to request an approval before SOP workflow is executed | |
| 310 | | Platform should provide an ability to create and manage distribution lists for emails, SMS. | |
| 311 | Responder Mobile App integrate with ICCC | Platform should provide a responder mobile app for the field staff to view real time events, manage their tasks, assign tasks, report incidents and collaborate with back-office and other field officers to address a SOP task | |
| 312 | | Responder mobile application should only display events and tasks based on pre-configurable access rules based on department and region | |
| 313 | | Responder mobile application should support escalation hierarchy of the tasks or events are not redressed with-in a defined SLA | |
| 314 | | Responder mobile application should provide an ability to track field officers | |
| 315 | | Responder mobile application should provide collaboration with the app for field officers and other staff to coordinate | |
| 316 | | Responder mobile application should be available on iOS and Android latest versions | |
| 317 | High Availability | Platform must have redundancy baked into the architecture | |
| 318 | | Platform must support on-prem and cloud deployments | |
| 319 | Scaling | Platform must be able to scale both horizontally and vertically at both on-prem and cloud deployments | |
| 320 | ICCC OEM Criteria | Proposed ICCC Platform should have been deployed and operational in at least 3 smart cities/Safe City/ITMS Projects in India /Global with Integration to minimum 5 different sub systems /applications.<br>Document Proof: OEM Shall submit P.O and Completion Certificate/ Installation Notes/UAT Certificates from SI as documentary proof.<br>ICCC Platform OEM should have valid ISO 9001 & ISO 27001. | |

| S. No | Parameter | Minimum Description |
|---|---|---|
| 1 | ITMS (Intelligent Traffic Management System) | ICCC Will be required to integrate with Intelligent Traffic Management solution using Open API standards. |
| | | ICCC will be required to receive the feeds from ITMS related to the traffic violations in facilitation by PSCDL. |
| | | ICCC will be required to receive the health (Offline/Fault Detection) Alerts of the Traffic Management Devices. |
| | | Geo visualization of the alerts and Operational Status of Traffic Management sensors & Camera. |
| | | All the information received from ITMS will get into Analytics layer of ICCC and provide useful insights and KPI's over dashboard and Generate the Reports for the specific alerts. |
| | | SOP will be executed for specific Traffic Management sensor/Camera alerts based on the alert type. |
| 2 | City Surveillance System | ICCC will be required to integrate with City Surveillance through VMS using Open API standards. |
| | | ICCC will be required to receive the feeds from City Surveillance related events. |
| | | ICCC will be required to receive the health alerts (Offline/Fault Detection) of VMS device |
| | | All the information received from City Surveillance system will be mapped on GIS map. |
| | | ICCC will be able to create SOP and execute for specific VMS alerts |
| | | All the information received from City Surveillance will provide useful insights and KPI's over dashboard and Generate the Reports |
| 3 | Environmental Sensor / Flood sensor | ICCC will be required to integrate with Environmental Management System using Open API standards. |
| | | ICCC should be able to map this information on the GIS layer and help authority monitor the environment condition across the city. |
| | | ICCC should also be able to trigger the commands / alerts (if required) to the respective system. |
| | | All the information received from Environmental management system will get into Analytics layer of ICCC and provide useful insights and KPI's over dashboard and Generate the reports based on the specific alert type. |
| 4 | Citizen Engagement System | ICCC will be required to integrate with Citizen Engagement Application System including social platform (Citizen Mobile and Citizen Web portal) using Open API standards. |
| | | ICCC will be required to show case the citizen complaint Location on the MAP Screen |

| | | |
|---|---|---|
| | | ICCC should also be able to trigger the commands / alerts (if required) to the respective system. |
| | | All the information received from Citizen Engagement system will get into Analytics layer of ICCC and provide useful insights and KPI's over dashboard and Generate the reports based on the specific alert type. |
| 5 | Variable Message Signboard | ICCC will be required to integrate with variable Message signboard sub system using Open API standards. |
| | | ICCC should be able to map variable Message signboard locations over the GIS layer. |
| | | The operator at ICCC should be able to click on the GIS map to view the details of particular Variable message sign board's status (On/off) etc. |
| | | ICCC should also be able to trigger the commands / alerts (if required) to the respective sub system. |
| | | All the information received from variable message signboard sub system will get into Analytics layer of ICCC and provide useful insights and KPI's over dashboard. |
| 6 | Public Address System | ICCC will be required to integrate with Public Address System using Open API standards. |
| | | ICCC should be able to show case the health Alerts (offline/Fault Detection) of speaker device |
| | | ICCC Should be able to show case the Geo visualization of the alerts and Operational Status of Speaker devices |
| | | ICCC should be able to execute the SOP based on the specific speaker alerts. |
| | | All the information received from Public Address System will get into Analytics layer of ICCC and provide useful insights and KPI's over dashboard and Generate the reports to specific alerts. |
| 7 | Ministry of Housing an d Urban Affairs (MoHUA) IUDX platform | ICCC platform will have capabilities to integrate with India Urban Data Exchange of MoHUA and share the data with www.data.gov.in. Please refer to www.iudx.org.in for more details. |
| 8 | | Advisory no 22 of cyber security framework guidelines recommended by MoHUA shall be considered. |

| | | |
|---|---|---|
| 9 | Further it is to be seen the same can be incorporated in BOQ as optional item and used only if budget allows. | ICCC should be integrated with future applications that are used for engaging citizens, ICCC should be ready to fetch the standard reports and KPI's, display the same over the dashboard. |
| | | ICCC should fetch relevant KPI's and reports from all future applications/System and display the same over ICCC dashboard. |
| | | ICCC should have provision for defining SOP's related to future applications. |
| | | ICCC should generate the specific reports based on the alerts for the future applications |

### 6.2 On Premise Data Centre (DC)

Functional requirement:

It is proposed to setup on premise DC for the video-based applications like ITMS and city surveillance. The servers and storage set up are made with redundancy and high availability. The solution shall have the capability to scale up to 50% for 5 years. Detailed elaboration is mentioned in Applications Architecture under sec. 5.3.

#### 6.2.1.42U Rack with All Accessories:

| Sl. No | Technical Specification | Compliance (Yes / No) |
|---|---|---|
| | **Make** <to be provided by the bidder> | |
| | **Model** <to be provided by the bidder> | |
| 1 | ISO Certified. | |
| 2 | Network Rack Dimension :( 800x1000) Rack.<br>Server Rack Dimension :( 600x1000) Rack. | |
| 3 | Height: Full 42U. | |
| 4 | Front & Rear perforated doors. | |
| 5 | FHU WITH FANS, CASTOR (Lockable) and 4 nos horizontal cable managers | |
| 6 | 2 Vertical Power stripe (5/15 Amp Sockets) | |

### 6.2.2 Core Router:

| Sl. No | Specification | Compliance (Yes / No) |
|---|---|---|
| | **Make:** <to be provided by the bidder> | |
| | **Model** : <to be provided by the bidder> | |
| 1 | The Router Should support minimum 160 Gbps full duplex throughput and should be of max 3 RU in height, 19-inch rack mountable. Should have 8x10G SFP+ and 2x40G QSFP based ports on day one. | |
| 2 | Router should support Optical Transceiver Digital Diagnostic Monitoring. | |
| 3 | Router Should support Dual Images. | |
| 4 | Router should support jumbo frames (9000) on all ports | |
| 5 | Router should support BFD for single hop and multihop sessions. | |
| 6 | Router should support MPLS-FRR to ensure high availability (optional) | |
| 7 | Router should support OSPFv2, OSPFv3, ISIS, BGPv4.<br>(and Optional Configuration: MP-BGP, BGP confederations and route reflector and RSVP-TE Fast Reroute (FRR)). | |
| 8 | Router should support VRRP, VRRPv3. | |
| 9 | IPv4 and IPv6 enabled from day one | |
| 10 | The Router scaling should be minimum:<br>a. 1M IPv4 FIB routes and 64K IPv6 FIB routes.<br>b. 32 VRF/L3VPN and 200 L2VPN.<br>c. HQoS and minimum 2K Queues.<br>d. 1K number of MPLS Labels (Provider Router) - optional.<br>e. 6PE /6VPE, MPLS label-Switching router (LSR & LER) functionalityOptional<br>f. 4K VLANs. | |
| 11 | Shall support following class of service features:<br>a) Classification, policing, marking, shaping, filtering<br>b) Manage congestion using a weighted random early detection (WRED) algorithm<br>c) Ingress policing<br>d) egress shaping<br>e) strict queuing , WFQ<br>f) Router should be able to classify based on 802.1 ad, 802.1 p, EXP and DSCP bits | |
| 12 | Shall support the OAM feature<br>a) 802.3ah/802.1ag/TWAMP<br>b) LLDP | |

| | | |
|---|---|---|
| 13 | IPv6 Features<br>a) IPv6 Ping<br>b) IPv6 trace route<br>c) OSPF v3<br>d) IS-IS | |
| 14 | Multicast Feature: It shall support following:<br>a) It shall support IGMP snooping v2/v3<br>b) The router shall support PIM Sparse Mode, RFC 4601<br>d) RFC 3569, Source Specific Multicast (SSM) | |
| 15 | Routers should support Timing and Synchronization such as Synchronous Ethernet or Precision Time Protocol (PTP) | |
| 16 | The router shall support LACP 802.3ad and bundle upto 8 links. | |
| 17 | The router should support IP SLA or RPM (or equivalent) for performance measurements, it should also support monitoring of IP SLA/RPM (or equivalent) probes using SNMP polling (OEM has to provide SNMP MIB information) | |
| 18 | The router should support filtering based on different parameters like: src ip, dst ip, src port, dst port, protocol etc | |
| 19 | The Router Should support DHCP server and client functionality, it Should support DHCPv6 server/relay as well. | |
| 20 | The Router Should support DHCP based option 82. | |
| 21 | It shall support role-based privileges for the system access and radius authentication. | |
| 22 | The router should have a Console or Out-of-band Management. | |
| 23 | Router should support Control-plane and management plane protection | |
| 24 | The Router Should support network management based on SNMP v2c/v3, Syslog, RADIUS/TACACS+, Access via CLI. | |
| 25 | The Router shall be able to operate at Operating Temperature: 0°C to 40°C and Operating Humidity: 20 - 80% RH non-condensing. | |
| 26 | The Router shall support dual redundant AC power supply and AC Power voltage shall be 110 - 240V. Should have dual power supply with hot swappable. | |
| 27 | The Router Should be NEBS Level III or equivalent complied. | |
| 28 | The Router operating system of the Routers category/series/family should be MEF-9/14 or CE (Carrier Ethernet) Certified/compliant. | |

| | | |
|---|---|---|
| 29 | All necessary SFPs, interfaces, connectors, patch cords (if any) & licenses must be delivered along with the Router from day one.<br>Warranty –Hardware/ Software License should be for 5 years. | |

**6.2.3. Firewall + IPS**

| Sl.No | Specification | Compliance (Yes /No) |
|---|---|---|
| | **Make** :<to be provided by the bidder> | |
| | **Model** :<to be provided by the bidder> | |
| 1 | The Firewall should be appliance based and must have redundant power supply. Should have dual power supply with hot swappable. | |
| 2 | Firewall Should have minimum 8 Gigabit RJ45, 8 nos. of 1G SFP and 4 nos. of 10G SFP+ ports populated with the transceivers. | |
| 3 | Firewall Should have console port and dedicated management port. | |
| 4 | Should have Firewall throughput of minimum 60 Gbps. | |
| 5 | IPSec VPN throughput should be 40 Gbps or more. | |
| 6 | NGFW throughput (With IPS) should be minimum 10 Gbps with enterprise mix traffic. | |
| 7 | Threat protection throughput should be minimum 8 Gbps with enterprise mix traffic. | |
| 8 | Must support at least 7,000,000 or more concurrent TCP connections. | |
| 9 | Must support at least 4,50,000 or more new TCP sessions per second processing. | |
| 10 | Should Support Virtualization (Virtual Systems/Virtual Domains/Context). Should have 6 or more Virtual Systems/Virtual Domains/Context license from day one. | |
| 11 | Should support both "bridge mode" or "transparent mode" apart from the standard NAT mode. | |
| 12 | Should provide NAT functionality, including PAT. Should support NAT 66, NAT 64, Static NAT IPv4 to IPv6 and vice versa (VIP64 and VIP46) and IPv6-IPv4 tunnelling or dual stack. | |
| 13 | Should support IPv4 & IPv6 policies. | |
| 14 | Provision to create secure zones. | |

| | | |
|---|---|---|
| 15 | Should support Link aggregation technology (IEEE 802.3ad) to achieve higher bandwidth using redundant links. | |
| 16 | Should support VLAN tagging (IEEE 802.1Q). | |
| 17 | Should support Static routing and Dynamic Routing (OSPF & BGP). | |
| 18 | Should support Active-Active/clustering. | |
| 19 | Should support ISP Load balancing/Link Sharing and Failover and should support link performance check based on packet loss, latency & jitter.. | |
| 20 | Should support protocols such as DES & 3DES, MD5, SHA-1, SHA-256 authentication, Diffie- Hellman Group 1, Group 2, Group 5, Group 14, Internet Key Exchange (IKE) v1 as well as IKE v2 algorithm, The new encryption standard AES 128, 192 & 256 | |
| 21 | Should support minimum 100 IPSec Site-to-Site and 2000 no of IPSsec Site-to-Client VPN tunnels. | |
| 22 | Should have integrated SSL VPN with license for 50 concurrent SSL VPN users | |
| 23 | Support for Client based VPN is mandatory and support for SSL Web VPN is preferable. | |
| 24 | Should support Windows, Linux and MAC OS for SSL-VPN. | |
| 25 | Should support NAT within IPSec/SSL VPN tunnels. | |
| 26 | Should support Stateful failover for both Firewall and VPN sessions. | |
| 27 | Should have protection for 2000+ signatures. | |
| 28 | Firewall able to prevent DOS and DDOS attacks. | |
| 29 | Supports user-defined signatures (i.e., Custom Signatures). | |
| 30 | Should have Application control feature with 1000 or more application signatures. | |
| 31 | Should perform Traffic Shaping/ Rate Limiting based on applications. | |
| 32 | Should control popular IM/P2P, proxy applications regardless of port/protocol. | |
| 33 | The appliance should facilitate embedded anti-virus/anti-malware support | |
| 34 | Gateway AV/ Antimalware should be supported for real-time detection of viruses and malicious code for HTTP, HTTPS, FTP, SMTP, SMTPS, POP3 and IMAP protocols etc. | |
| 35 | Should also include Botnet filtering and detecting and preventing Botnet command and control traffic | |

| | | |
|---|---|---|
| 36 | Should have configurable policy options. Possible to select traffic to scan for viruses | |
| 37 | The appliance should facilitate embedded Web Content and URL Filtering feature | |
| 38 | Web content and URL filtering solution should work independently without the need to integrate with External proxy server. | |
| 39 | URL database should have 100 million or more URLs under more than 40 categories | |
| 40 | Should be able to block different categories/sites based on User Authentication. | |
| 41 | Firewall should support management either through GUI/CLI or through Central Management | |
| 42 | Firewall should support logging to multiple syslog servers. | |
| | Hardware /Software should have 5 year Warranty. | |
| 43 | Log & Reporting should be a dedicated solution out of the Firewall | |
| 44 | The log & reporting tool with OS or any other licenses needs to be bundled or quoted along with the solution. The logging and analysis should either be an Appliance/Server or VM platform with minimum RAID6/RAID10 usable 10TB storage to store logs for 6 months with suitable warranty. | |

### 6.2.4. Server Specification

| # | Parameter | Minimum Specifications | Compliance (Yes / No) |
|---|---|---|---|
| 1. | **Make : The solution will be provided by the SI along with the make** | | |
| 2. | **Model: The solution will be provided by the SI along with the model** | | |
| 3. | Processor | 2 processors Intel® Xeon® Scalable or AMD 3rd Gen processors or latest | |
| | | Minimum 10 cores/processor @ 2.1 GHz base frequency or better | |
| 4. | RAM | Minimum 128 GB RAM | |
| 5. | Internal Storage | Minimum 2x480 GB SSD/Flash | |
| 6. | Network interface | 2X1 Gbe copper ports and 4 x 10G Fibre Ethernet ports along with transceivers SFP+ to connect TOR switch | |
| | | Optional: 1 X Dual-port 16Gbps FC HBA (or FCoE) for providing FC connectivity | |
| 7. | Power supply | Dual Redundant Power Supply | |
| 8. | RAID support | As per requirement/solution | |
| 9. | Operating System | Licensed version OS, DB or any 3rd party Licenses should be supplied as per solution requirement. | |
| 10. | Form Factor | Rack mountable/Blade | |
| 11. | Virtualization | Server should support industry leading virtualization like VMWare VCentre, Citrix XenServer, Hyper V, Oracle VM, KVM etc. In case the MSI proposes the solution to virtualization, then they should propose suitable associated management solution to meet or exceed the SLAs. | |
| 12 | Server can be Rack mountable/ Blade Server. If blade server solution, chassis should be 19" rack-mountable, capable of accommodating minimum 8 or higher hot pluggable blades with Two hot-plugs/hot-swap redundant modules for connectivity to the external TOR Switches and to storage device. | | |
| 13 | Server should have remote management ILO/ILOM/IDRAC/IPMI/RSA or equivalent with support capabilities include KVM over IP, power on, off & reset, virtual media, SNMPv2 or higher with appropriate perpetual licenses. | | |
| 14 | Server should provide with required power cables and rack mounting kit. | | |
| 15 | Server Average CPU load during peak time should be below 75% and RAM should be below 80%. | | |

### 6.2.5. Storage Specification

| # | Parameter | Minimum Specifications | Compliance (Yes /No) |
|---|---|---|---|
| 1. | | **Make : The solution will be provided by the SI along with themake** | |
| 2. | | **Model : The solution will be provided by the SI along with the model** | |
| 3. | Solution/ Type | 1) IP Based/iSCSI/FC/NFS/CIFS<br>2) If bidder is offering FCoE based solution, corresponding ports must be present in server as well as storage controller. | |
| 4. | Storage | 1) Storage Capacity should be as per Overall Solution Requirement (usable, after configuring in offered RAID configuration). Storage Capacity after RAID to be provided with 20% additional capacity for future useto be provided.<br>2) RAID solution offered must protect against double disc failure.<br>3) Disks should be preferably minimum of 1.2 TB capacity for SSD / SAS and 3 TB for SATA/ NL-SAS ( combination as per performance and SLA requirements of overall solution)<br>4) To store all types of data (Data, Voice, Images, Video, etc)<br>5) Proposed Storage System should be scalable (vertically/horizontally) | |
| 5. | Hardware Platform | 1) Rack mounted form-factor<br>2) Modular design to support controllers and disk drives expansion | |
| 6. | Controllers | 1) At least 2 Controllers in active/active mode<br>2) The controllers / Storage nodes should be upgradable seamlessly, without any disruptions / downtime to production workflow for performance, capacity enhancement and software / firmware upgrades. | |
| 7. | RAID support | Should support various RAID Levels RAID 0, 1, 1+0, 5+0 and 6 | |
| 8. | Cache | Minimum 64 GB of useable cache across all controllers. If cache is provided in additional hardware for the storage solution, then cache must be over and above 64 GB. | |
| 9. | Redundancy and High Availability | The Storage System should be able to protect the data against single point of failure with respect to hard disks, connectivity interfaces, fans and power supplies | |
| 10 | Should also include storage performance monitoring and management software. | | |
| 11 | Storage should use the latest stable technology platform, with support available for next 7 years. | | |
| 12 | Storage should be provided with the required optics, cables and rack mounting kit. | | |

### 6.2.6. Hypervisor

| Sl.No | Specification | Compliance (Yes /No) |
|---|---|---|
| 1 | **Make** :<to be provided by the bidder> | |
| 2 | **Model** :<to be provided by the bidder> | |
| 3 | Hypervisor sits directly on the bare metal server hardware with no dependence on a general-purpose OS for greater reliability & security. | |
| 4 | Must be support all leading Operating Systems like Linux/Windows etc.. | |
| 5 | Proactive High availability capability that utilizes server health information and migrates VMs from degraded hosts before problem occurs. | |
| 6 | Migration of VMs in case one physical server fails all the VMs running on that server shall be able to migrate to another physical server running same virtualization software. | |
| 7 | Should support continued operations in the event of 1 node failure or 1 disk failure. | |
| 8 | Should support quick boot. | |
| 9 | The Solution should support taking clones of individual Virtual Machines for faster provisioning. | |
| 10 | The Solution should support VM snapshots. | |
| 11 | It should allow taking snapshots of individual Virtual Machines to be able to revert to an older state, if required. | |

### 6.2.7. Core Switch

| Sl.No | Specification | Compliance (Yes / No) |
|---|---|---|
| | **Make :** | |
| | **Model :** | |
| 1 | Should have minimum 16 nos. QSFP28 based 40/100G ports day one. Should have dual power supply with hot swappable. | |
| 2 | Should have at least 1.6 Tbps switching fabric. | |
| 3 | Should have minimum 1000 Mpps (64 Byte) throughput | |
| 4 | Should support transceiver Digital Diagnostic Monitoring for optical ports. | |
| 5 | Should have support for 802.3x flow control. | |

| | | |
|---|---|---|
| 6 | Should support at least 64K entries in the MAC table. | |
| 7 | Should support at least 4000 active VLANs. | |
| 8 | Should support jumbo frame (9000 Byte or above) | |
| 9 | Should support Port-based VLAN, 802.1Q Tagged VLAN. | |
| 10 | Should support LLDP or similar functionality. | |
| 11 | Should support port mirroring. | |
| 12 | Switch should support IPv6. | |
| 13 | Should support 802.1D spanning tree control/RSTP support and MSTP Support. | |
| 14 | Should support spanning-tree portfast for fast convergence or similar functionality. | |
| 15 | Should support spanning-tree root guard or similar functionality. | |
| 16 | Should support spanning-tree bpdu guard, bpdu filter or similar functionality. | |
| 17 | Should Support VRRP. | |
| 18 | Should support ITU-T G.8032 Ethernet Ring Protection designed for loop protection and fast convergence times (sub 50 ms) in ring topologies | |
| 19 | Should be Ethernet OAM compliant with IEEE 802.3ah/Y.1731. | |
| 20 | Should support IGMP v1/v2/v3 and IGMP Snooping | |
| 21 | Should support security features Broadcast, Multicast and Unicast Storm Control | |
| 22 | Should support security features DoS Attack Prevention | |
| 23 | Should support console port and telnet/ssh based management. | |
| 24 | Should support Static IPv4 and Ipv6 routing. It shall also support OSPFv2 and OSPFv3. | |
| 25 | Should support OSPFv2, OSPFv3 day one. | |
| 26 | Should support BFD for OSPF. | |
| 27 | Should support multicast routing PIM-SM. | |
| 28 | Should support minimum 64K for IPv4 FIB routes and 16K for IPv6 FIB routes. | |
| 29 | Should Support for minimum 256 VLANs SVI or RVI interfaces. | |
| 30 | Should Support VRRP, DHCP local server, DHCP relay and DHCP snooping. | |

| | | |
|---|---|---|
| 31 | Should support management features SNMP, NTP, RFC 2138 RADIUS | |
| 32 | Should support 802.1Q VLAN, 802.1p priority queues. | |
| 33 | Should support 8 hardware queues per port and shall support ingress policing and egress shaping. | |
| 34 | Should support Quality Of Service (QoS):<br>i) Priority Queue,<br>ii) Ingress policer,<br>iii) Rate Limiting (Bandwidth Control), | |
| 35 | Should support automation NETCONF/YANG/OpenConfig | |
| 36 | Should have redundant AC Power Supply 100 to 240 V AC. | |
| 37 | Should have redundant fan modules | |
| 38 | Switch to be mounted on a 19-Inch rack and should consume maximum 2 RU. All accessories required for this mounting and commissioning should be supplied. | |
| 39 | Switch should comply to Operating Temperature range 0°C to 40 °C | |
| 40 | Ports should be populated with transceivers as required. Hardware/Software should have 5-year warranty. | |

**6.2.8. TOR Switch & WAN Aggregation switch:**

| S.No | Specification | Compliance (Yes / No) |
|---|---|---|
| | **Make :** | |
| | **Model :** | |
| 1 | Should have minimum 24 SFP+ based 10G and 2 nos. QSFP28 based 40/100G ports day one. Should have dual power supply with hot swappable. | |
| 2 | Should have at least 400 Gbps switching fabric. | |
| 3 | Should have minimum 300 Mpps (64 Byte) throughput | |
| 4 | Should support transceiver Digital Diagnostic Monitoring for optical ports. | |
| 5 | Should have support for 802.3x flow control. | |
| 6 | Should support at least 64000 entries in the MAC table. | |
| 7 | Should support at least 4000 active VLANs. | |
| 8 | Should support jumbo frame (9000 Byte or above) | |

| | | |
|---|---|---|
| 9 | Should support Port-based VLAN, 802.1Q Tagged VLAN. | |
| 10 | Should support LLDP or similar functionality. | |
| 11 | Should support port mirroring. | |
| 12 | Switch should support IPv6. | |
| 13 | Should support 802.1D spanning tree control/RSTP support and MSTP Support. | |
| 14 | Should support spanning-tree portfast for fast convergence or similar functionality. | |
| 15 | Should support spanning-tree root guard or similar functionality. | |
| 16 | Should support spanning-tree bpdu guard, bpdu filter or similar functionality. | |
| 17 | Should Support VRRP. | |
| 18 | Should support ITU-T G.8032 Ethernet Ring Protection designed for loop protection and fast convergence times (sub 50 ms) in ring topologies | |
| 19 | Should be Ethernet OAM compliant with IEEE 802.3ah/Y.1731. | |
| 20 | Should support IGMP v1/v2/v3 and IGMP Snooping | |
| 21 | Should support security features Broadcast, Multicast and Unicast Storm Control | |
| 22 | Should support security features DoS Attack Prevention | |
| 23 | Should support console port and telnet/ssh based management. | |
| 24 | Should support Static IPv4 and Ipv6 routing. It shall also support OSPFv2 and OSPFv3. | |
| 25 | Should support OSPFv2, OSPFv3 day one. | |
| 26 | Should support BFD for OSPF. | |
| 27 | Should support multicast routing PIM-SM. | |
| 28 | Should support minimum 16K for IPv4 FIB routes and 8K for IPv6 FIB routes. | |
| 29 | Should Support for minimum 256 VLANs SVI or RVI interfaces. | |
| 30 | Should Support VRRP, DHCP local server, DHCP relay and DHCP snooping. | |
| 31 | Should support management features SNMP, NTP, RFC 2138 RADIUS | |
| 32 | Should support 802.1Q VLAN, 802.1p priority queues. | |

| | | |
|---|---|---|
| 33 | Should support 8 hardware queues per port and shall support ingress policing and egress shaping. | |
| 34 | Should support Quality of Service (QoS):<br>i) Priority Queue,<br>ii) Ingress policer,<br>iii) Rate Limiting (Bandwidth Control), | |
| 35 | Should support automation NETCONF/YANG/OpenConfig or equivalent. | |
| 36 | Should have redundant AC Power Supply 100 to 240 V AC. | |
| 37 | Should have redundant fan modules | |
| 38 | Switch to be mounted on a 19-Inch rack and should consume maximum 2 RU. All accessories required for this mounting and commissioning should be supplied. | |
| 39 | Switch should comply to Operating Temperature range 0°C to 40 °C | |
| 40 | Ports should be populated with transceivers as required | |
| 41 | Core Switch and TOR switch should be from same OEM.<br>Hardware /Software should have 5-year warranty | |

### 6.2.9. Access Switch -8 Port – POE-Industrial Grade (Field Switch)

| S.No | Specification | Compliance (Yes / No) |
|---|---|---|
| | **Make :** | |
| | **Model :** | |
| 1 | Should have minimum 8 GE ports. | |
| 2 | Should have minimum 4 nos. SFP based 1 GE ports. | |
| 3 | Should have at least 20 Gbps switching fabric. | |
| 4 | Should support port Trunking of at least 4 nos. 1GE ports. | |
| 5 | Should support 802.3af and 802.3at | |
| 6 | Should support PoE of 8 ports. | |
| 7 | Switch should have minimum POE power budget of 120 watts | |
| 8 | Switch should support IEEE 802.3ad, IEEE 802.3az standards | |
| 9 | Should support transceiver Digital Diagnostic Monitoring for optical ports. | |
| 10 | Should support Auto MDI-II/MDI-X uplink for all the twisted pair ports. | |
| 11 | Should support for 802.3x flow control. | |
| 12 | Should support at least 8000 entries in the MAC table. | |
| 13 | Should support vlan range 1-4000 and at least 32 active VLANs. | |
| 14 | Should support jumbo frame (9000 Byte or above) | |
| 15 | Should support Port-based VLAN, 802.1Q Tagged VLAN. | |
| 16 | Should support LLDP or similar functionality. | |
| 17 | Should support port mirroring. | |
| 18 | Switch should support IPv6. | |
| 19 | Should support 802.1D spanning tree control/RSTP support and MSTP Support | |
| 20 | Should support spanning-tree portfast for fast convergence or similar functionality. | |
| 21 | Should support spanning-tree root guard or similar functionality. | |
| 22 | Should support spanning-tree bpdu guard, bpdu filter or similar functionality. | |

| | | |
|---|---|---|
| 23 | Should support DHCP snooping | |
| 24 | Should support ITU-T G.8032 Ethernet Ring Protection designed for loop protection and fast convergence times (sub 50 ms) in ring topologies | |
| 25 | Should be Ethernet OAM compliant with IEEE 802.3ah/Y.1731. | |
| 26 | Should support IGMP v1/v2/v3 and IGMP Snooping | |
| 27 | Should support security features Broadcast, Multicast and Unicast Storm Control | |
| 28 | Should support security features DDoS Attack Prevention | |
| 29 | Should support console port and telnet/SSH based management. | |
| 30 | Should support management features viz. CLI, Web-based GUI, SNMP, Syslog, NTP, RFC 2138 RADIUS | |
| 31 | Should support Dual Images | |
| 32 | Should support 802.1Q VLAN, 802.1p priority queues. | |
| 33 | Should support Layer 2 QoS | |
| 34 | Should support strict Priority Queue, Weighted Round Robin (WRR), Rate Limiting (Bandwidth Control) or equivalent | |
| 35 | Should have AC Power Supply 100 to 240 V AC with 50 to 60 Hz without any external adaptors | |
| 36 | Switch should comply to Industrial Grade with minimum Operating Temperature range 0°C to 60 °C and Relative Humidity 95% or better. | |
| 37 | All accessories required for this mounting should be supplied from day one. Hardware/Software should have warranty for 5 years. | |
| 38 | Switch should have EMI CERTIFICATE of FCC/IC or CE or equivalent. | |

### 6.2.10. Access Switch-24 Port –POE -Field Switch (Industrial Grade)

| Sl.No | Specification | Compliance (Yes / No) |
|---|---|---|
| | **Make :** | |
| | **Model:** | |
| 1 | Should have minimum 24 GE ports. Should have dual power supply with hot swappable. | |
| 2 | Should have minimum 2 nos. SFP based 1 GE ports. | |

| | | |
|---|---|---|
| 3 | Should have at least 52 Gbps switching fabric. | |
| 4 | Should support port Trunking of at least 2 nos. 1GE ports. | |
| 5 | Should support 802.3af and 802.3at | |
| 6 | Should support PoE of 24 ports | |
| 7 | Switch should have minimum POE power budget of 540 watts | |
| 8 | Switch should support IEEE 802.3ad, IEEE 802.3az standards | |
| 9 | Should support transceiver Digital Diagnostic Monitoring for optical ports. | |
| 10 | Should support Auto MDI-II/MDI-X uplink for all the twisted pair ports. | |
| 11 | Should support for 802.3x flow control. | |
| 12 | Should support at least 8000 entries in the MAC table. | |
| 13 | Should support vlan range 1-4000 and at least 32 active VLANs. | |
| 14 | Should support jumbo frame (9000 Byte or above) | |
| 15 | Should support Port-based VLAN, 802.1Q Tagged VLAN. | |
| 16 | Should support LLDP or similar functionality. | |
| 17 | Should support port mirroring. | |
| 18 | Switch should support IPv6. | |
| 19 | Should support 802.1D spanning tree control/RSTP support and MSTP Support | |
| 20 | Should support spanning-tree portfast for fast convergence or similar functionality. | |
| 21 | Should support spanning-tree root guard or similar functionality. | |
| 22 | Should support spanning-tree bpdu guard, bpdu filter or similar functionality. | |
| 23 | Should support DHCP snooping | |
| 24 | Should support ITU-T G.8032v2 Ethernet Ring Protection designed for loop protection and fast convergence times (sub 50 ms) in ring topologies | |
| 25 | Should be Ethernet OAM compliant with IEEE 802.3ah/Y.1731. | |
| 26 | Should support IGMP v1/v2/v3 and IGMP Snooping | |
| 27 | Should support security features Broadcast, Multicast and Unicast Storm Control | |
| 28 | Should support security features DoS Attack Prevention | |

| | | |
|---|---|---|
| 29 | Should support console port and telnet/SSH based management. | |
| 30 | Should support management features viz. Web-based GUI, SNMP, Syslog, NTP, RFC 2138 RADIUS | |
| 31 | Should support Dual Images | |
| 32 | Should support 802.1Q VLAN, 802.1p priority queues. | |
| 33 | Should support Layer 2 QoS | |
| 34 | Should support Strict Priority Queue, Weighted Round Robin (WRR), Rate Limiting (Bandwidth Control) or equivalent | |
| 35 | Should have AC Power Supply 100 to 240 V AC with 50 to 60 Hz without any external adaptors | |
| 36 | Switch should comply to Industrial Grade with minimum Operating Temperature range 0°C to 60 °C and Relative Humidity 95% or better. | |
| 37 | All accessories required for this mounting should be supplied by day one. Hardware/Software should have 5 year warranty. | |
| 38 | Switch should have EMI CERTIFICATE of FCC/IC or CE or equivalent. | |

### 6.2.11 Wireless LAN Controller:

| Sl. No | Technical Specification | Compliance (Yes / No) |
|---|---|---|
| | Make: | |
| | Model: | |
| 1 | WLC should support 1+1 failover for high availability. | |
| 2 | The proposed WLC must be compliant with IEEE CAPWAP or equivalent for controller-based WLANs. | |
| 3 | The proposed WLC should be virtualized/ hardware appliance, rack mountable with 2 x10G (or better) Ethernet interface. | |
| 4 | The proposed WLC should support both centralized as well as distributed traffic forwarding architecture from day 1. It should be IPv6 ready from day one. | |
| 5 | The proposed controller should support minimum 10K users/devices and WLANs-100 or more. | |
| 6 | The proposed WLAN controller should be supplied with minimum 100 AP license from Day-1 and can scale up to 250 APs without change / additional hardware. Additional AP license will be procured in future. | |

| | | |
|---|---|---|
| 7 | The wireless access points must securely download image from WLC and should be configured from WLC only. | |
| 8 | The proposed WLC should support L2/L3 roaming for mobile clients | |
| 9 | The proposed WLC should provide real-time radio power adjustments based on changing environmental conditions and signal coverage adjustments. It should also adjust radio channel automatically. | |
| 10 | Should support dynamic bandwidth selection among 20Mhz, 40 MHz, and 80Mhz channels. | |
| 11 | Controller should support Wi-Fi 6, 802.11ax technology | |
| 12 | The proposed system must support coverage hole detection and correction that can be adjusted on a per WLAN basis. | |
| 13 | Should support web-based authentication to provide a browser-based environment to authenticate clients that do not support the IEEE 802.1X supplicant. | |
| 14 | Should support port-based and SSID-based IEEE 802.1X authentication. | |
| 15 | Should support MAC authentication to provide simple authentication based on a user's MAC address. | |
| 16 | Should support AP grouping to enable administrator to easily apply AP based or radio-based configurations to all the APs in the same group | |
| 17 | WLC should support Comprehensive Integrated Network Security Services Wired/wireless, built-in Wireless Intrusion Protection System (WIPS), and secure guest access with Captive web portal or equivalent solution. | |
| 18 | WLC should provide BYOD Support. It should provide device fingerprinting and required to help manage and secure user-owned devices. | |
| 19 | WLC should support 802.11w to secure management frames, NAC integration support. | |
| 20 | WLC should support guest access. | |
| 21 | WLC architecture should support tunnel forwarding and local forwarding. | |
| 22 | WLAN Solution should support captive portal with time-based access, Customize Guest page and must have option for self-guest registration options, so that guest can automatic register himself from day 1 or with equivalent solution. | |
| 23 | WLAN Solution should have feature to create captive portal guest users for authenticating using their User ID (Email Address/ Mobile Number/ Member ID) and the received pass code on Email or SMS in order to complete the registration process or any equivalent solution/ third-party components to full-fill the requirement. | |
| 24 | SMS Gateway integration required for OTP should be provided along with the WLC. | |

**6.2.12. Indoor Access Points:**

**General Minimum Requirement:**

| Sl.No | Specification | Compliance (Yes /No) |
|---|---|---|
| | **Make :** | |
| | **Model:** | |
| **1.** | Access Points must comply with IEEE 802.11ax and must include tri radios (2.4 GHz, 5 GHz and dedicated sensor WIPS) or Access Points must include dual radios with MU-MIMO and access point for dedicated dual band sensor (WIPS) | |
| **2.** | Dual band 802.11ac , 2 x2 MIMO radio interfaces | |
| **3.** | Sustained throughput shall be minimum 1 GBPS or more | |
| **4.** | Support minimum 50 concurrent clients for Indoor | |
| **5.** | Should support minimum 16 BSSIDs or more per radio | |
| **Features** | | |
| **6.** | Should be integrated antenna | |
| **7.** | The access point shall be capable of performing security scanning and serving clients on the same radio | |
| **8.** | Should have at least 1 Gigabit Ethernet port | |
| **9.** | Should support power over Ethernet | |
| **10.** | Should support 20, 40, and 80 MHz Channels | |
| **11.** | Must have a dynamic or smart RF management features which allows WLAN to adapt to changes automatically and intelligently in the RF environment | |
| **12.** | Access Point Should have a Transmit power of 18dbm | |
| **13.** | Must support regulatory domain as per country 2.412 to 2.462 GHz and 5.745 to 5.825 GHz | |
| **14.** | Should have LEDs to indicate device status. | |
| **15.** | Must support fast secure roaming | |
| **16.** | Should support RADIUS based 802.1 x authentication including EAP-PEAP, EAP-TTLS, and EAP-TLS | |

| | | |
|---|---|---|
| **17.** | Must support telnet and/ or SSH login to Aps directly for troubleshooting flexibility | |
| **18.** | AP should have mounted kit from the same OEM. Hardware/Software should have 5-year warranty | |
| **19.** | In case of Outdoor Access point the same shall be IP 67, Support minimum 200 concurrent clients. | |

**6.2.13 AAA Server:**

| Sl.No | Minimum Functional requirements | Compliance (Yes / No) |
|---|---|---|
| | Make: | |
| | Model: | |
| 1. | The Solution should provide a highly powerful and flexible attribute-based access control solution that combines authentication, authorization, and accounting (AAA); posture; profiling; BYOD, and guest management services on a single platform.<br>Solution should include all required licenses to perform above mentioned capabilities for 300 endpoints from day one and scalable to 1000 over a period of time. | |
| 2. | It should allow enterprises to authenticate and authorize users and endpoints via wired, wireless, and VPN with consistent policy throughout the enterprise.. | |
| 3. | Provides complete guest lifecycle management by empowering sponsors to on-board guests | |
| 4. | Must be dedicated appliance based with each appliance supporting 1000 endpoints from day one | |
| 5. | Enforces security policies by blocking, isolating, and non compliant machines in a quarantine area /VLAN without requiring administrator attention | |
| 6. | Offers a built-in monitoring, reporting, and troubleshooting console to assist helpdesk operators and administrators streamline operations | |
| 7. | Allows you to get finer granularity while identifying devices on your network with Active Endpoint Scanning | |
| 8. | Offers a rules-based, attribute-driven policy model for creating flexible and business-relevant access control policies. Provides the ability to create fine-grained policies by pulling attributes from predefined dictionaries that include information about user and endpoint identity, posture validation, authentication protocols, profiling identity, or other external attribute sources. Attributes can also be created dynamically and saved for later use | |
| 9. | Utilizes standard RADIUS protocol for authentication, authorization, and accounting (AAA). | |

| | | |
|---|---|---|
| 10. | Verifies endpoint posture assessment for PCs connecting to the network. Should be a persistent client-based agent to validate that an endpointis conforming to a company's posture policies. Provides the ability to create powerful policies that include but are not limited to checks for the latest OS patches, antivirus and antispyware software packages | |
| | with current definition file variables (version, date, etc.), registries (key, value, etc), and applications. | |
| 11. | It should allow Administrators to create their own device templates. These templates can be used to automatically detect, classify, and associate administrative-defined identities when endpoints connect to the network. Administrators can also associate endpoint-specific authorization policies based on device type. | |
| 12. | The Solution should have capability to collect endpoint attribute data via passive network telemetry, querying the actual endpoints, or alternatively from the infrastructure via device sensors on switches. | |
| 13. | Should support full guest lifecycle management, whereby guest users can access the network for a limited time, either through administrator sponsorship or by self-signing via a guest portal. Should include guest portal customize from day one | |
| 14. | Solution should support receiving updated endpoint profiling policies and the updated OUI database as a feed from the OEM database. Solution should have profiling capabilities integrated into the solution in order to detect headless host. | |

### 6.2.14 Centralized-IT security Solution For ICCC

| Sl. No | Technical Specification | Compliance (Yes / No) |
|---|---|---|
| 1 | The solution must utilize Client Server architecture where Central Endpoint Management Console can be used for creating and distributing policies. Central Endpoint Management Console should be able to create, manage and monitor all the endpoints across the organization centrally. Central Endpoint Management Server should utilize On-Premise architecture and no SaaS / Cloud model. | |
| 2 | The solution should support All-in-One Centralized Management — deploy, manage and monitor Clients on-premise or off-premise. Management Server console also should help to provide real-time control and visibility into endpoints when they are either on or off corporate networks. | |
| 3 | Solution should support integration and synchronization with Microsoft Active Directory (AD) to deploy the Agents to all the endpoints. | |
| 4 | Solution should support installing and managing agents on Microsoft Windows 7 / 8 / 8.1 / 10 / 11 & Windows Server 2012+, Mac OS 11+, Linux, UNIX | |
| 5 | Endpoint should be integrated with the on-premise sandbox solution for submitting suspicious files for further analysis & can share the threat intelligence with the other endpoints. | |
| 6 | Endpoint should block the access to the file till it gets the verdict from the sandbox. | |
| 7 | Should be able to manually submit files to sandbox for analysis | |

| | | |
|---|---|---|
| 8 | Solution should support Endpoint Protection features of Anti-Malware, Anti-Exploit, Web Filter, Application Firewall, Vulnerability Assessment and Management, Software Inventory Management and USB Control . | |
| 9 | Solution should be able to Block Access to Malicious Websites, Scan Compressed Files, Scan Network Files, Scan Removable Media on Insertion, Scan Email attachments. | |
| 10 | Solution should support easy creation of security profiles with customizable features such as Antimalware, Exploit Prevention, Application Firewall, Web Filter, USB Control etc. applied to specific set of devices or for all devices. | |
| 11 | The management server should support creation of Custom Installer Packages with included Security Profiles to help simplify deployment and management of endpoints from a single console. | |
| 12 | Custom Installer Package should be available from web-link of Management Console in MSI / EXE / DMG packages. | |
| 13 | The centralized management console should be web-based and should support Role Based Access (RBAC). | |
| 14 | Solution must offer comprehensive client/server security by protecting enterprise networks from Viruses, Trojans, Worms, Network Viruses, Spyware and Rootkits. | |
| 15 | Solution must provide real-time on-access scanning for file systems to prevent or stop malicious code execution. | |
| 16 | The proposed solution should provide tamper protection to prevent end-users or malicious actors from disabling the endpoint protection software. | |
| 17 | Tamper protection should support configurable password in case emergency override is required. | |
| 18 | The proposed system shall be able to querie a real time database of over 50 million+ rated websites categorized into 70+ unique content categories. | |
| 19 | Should support Endpoint Quarantine to quickly disconnect a compromised endpoint from the network and stop it from infecting other assets. | |
| 20 | Solution should be able to detect and prevent communication patterns used by Bots like information about botnet family. | |
| 21 | Solution should be able to block traffic between infected host and remote C&C operator but at the same time allow traffic to legitimate destinations. | |
| 22 | The solution should detect and prevent various exploit techniques providing protection against memory-based attacks. | |
| 23 | Solution should monitor behaviour of applications like Web Browsers (IE, Chrome, Firefox, Opera), Java/Flash plug-ins, Microsoft Office applications, and PDF reader as part of anti-exploit feature. | |
| 24 | Endpoint solution should have vulnerability scanning feature to check for known vulnerabilities in the endpoints. | |
| 25 | The solution must support creation of exclusions / exceptions from Central Console and pushing them to the endpoints. It should not require creation of exclusions on individual endpoints. | |
| 26 | The solution must be provided for at least 100 endpoint licenses including software updates, upgrades and technical support for 5 years. | |

### 6.2.15 Video wall and Video wall Controller

Following are the minimum expected technical specifications for Video wall and Video Wall controller.

| Sl. No | Parameters | Minimum Technical Requirements | Compliance (Yes /No) |
|---|---|---|---|
| | **Make:** | | |

| | | | |
|---|---|---|---|
| | **Model:** | | |
| 1 | Configuration | Video Wall cubes of 70"(± 5 %) diagonal in a 6(C) x 2(R)configuration complete with base stand with Unique cooling system ensures longer LED lifetime | |
| 2 | Cube & Controller | Cube & controller, Software should be from the Same OEM | |
| 3 | Native Resolution | Full HD (1920x 1080) DLP Single chip/DLP LED Technology or higher or better | |
| 4 | Technology | LED Lit DLP Rear Projection Technology without any colour wheel or Laser or better | |
| **Sl. No** | **Parameters** | **Minimum Technical Requirements** | **Compliance (Yes /No)** |
| | **Make:** | | |
| | **Model:** | | |
| 5 | Light Source | LED light source with a minimum life time of 1,00,000 hrs. in Normal Mode & Eco Mode; Individual cube should be equipped with multiple LED banks and each LED bank should have an array of diodes. Single or multiple diode failure should not impact image display on the screen or Laser or better | |
| 6 | Display Technology | DLP Rear Projection with single DMD Chip Along with Color Gamut of REC 709 or Better. | |
| 7 | Brightness on Screen | Minimum 500 (nits or cd/m2) and should be adjustable for lower or even higher brightness requirements. This should be supported by datasheet | |
| 8 | Brightness Uniformity | >95% or better | |
| 9 | Color | Should provide auto color adjustment function and should be sensor based, automatic calibration system which works with an advanced color sensor. The sensor continuously measures the primary levels of the entire wall and adjusts white point and color when needed. | |

| | | | |
|---|---|---|---|
| 10 | | Color and brightness sensor should be in-built inside the projector only<br>Placing sensors outside the projector and projector body is not acceptable | |
| 11 | Screen | 180° viewing angle | |
| 12 | General | System must be modular in installation; Dark box type stacking model is not acceptable. 1000000:1 or more | |
| 13 | Brightness of Projection engine | Typ. 1100 lumens or Better | |
| 15 | Control | IP Based control or better | |
| 16 | Remote | IP based control should also be provided for quick access and IR remote control should also be provided for quick access. | |
| **Sl. No** | **Parameters** | **Minimum Technical Requirements** | **Compliance (Yes /No)** |
| | **Make:** | | |
| | **Model:** | | |
| 17 | Screen to Screen Gap | <0.2 to 0.5 mm Gap between 2 screens | |
| 19 | Terminal in each Cube | 2x Input (DP1.2)<br>2x Input (HDMI2.0)<br>2x LAN<br>2x USB<br>1x Output (DP1.2) | |
| 21 | Power Supply | 100 – 240 VAC, 50-60Hz; Power supply: Rack Mountable Redundant Hot swappable power supply to be provided in N+1 Redundancy for 24x7 Fail safe operations. | |
| 24 | Cooling Inside Cube | Any advanced cooling mechanism, Low noise and high dissipation system. Less than 510 BTU / h. This should be supported by datasheet. | |
| 26 | Maintenance Access | Cube should be accessible from the rear/front side for maintenance only | |

| | | | |
|---|---|---|---|
| 27 | Cube control & Monitoring | Video wall should be equipped with a cube control & monitoring system. It should provide options to view control layouts on remote devices such as tab, laptop, etc through web browsers | |
| 28 | | Should be able to control & monitor individual cube, multiple cubes and multiple video walls | |
| 29 | | Should provide a virtual remote GUI over the IP to control the video wall | |
| 30 | | Status log file should be downloadable as per user convenience | |
| 31 | | System should be AI (Artificial Intelligence) with Advance Pro-active real-time Monitoring and Diagnosis of hardware over cloud for predictive failure to have maximum uptime | |
| 32 | Sharing & Collaboration | It should be possible to share the layouts over LAN/WAN Network with Display in | |
| **Sl. No** | **Parameters** | **Minimum Technical Requirements** | **Compliance (Yes /No)** |
| | **Make:** | | |
| | **Model:** | | |
| | | Meeting room or on Remote Workstations connected on LAN/WAN Network | |
| 33 | Dust Protection | Engine should be protected from dust ingress | |
| 34 | Monitoring of critical parameters to ensure stable operation of the system 24 x 7 | Internal Temperature | |
| 35 | | Brightness | |
| 38 | | Should be possible to demonstrate these parameters through an active monitoring | |

*6.2.15.1* Video Wall Controller

| **No** | **Parameters** | **Minimum Technical Requirements** | **Compliance (Yes /No)** |
|---|---|---|---|
| | **Make:** | | |

| | | | |
|---|---|---|---|
| | **Model:** | | |
| 1 | Display controller | Controller to be able to control mentioned video wall and should be based on the latest architecture. Hardware / software should have 5-year warranty | |
| 2 | Chassis Type | 19" Rack mount industrial chassis | |
| 3 | Network | 2 x 1Gb/s LAN | |
| 4 | DVI/HDMI Inputs | 8 or more | |
| 5 | Resolution Support for Outputs | Each o/p should have 4K support | |
| 6 | Hard disk, RAM, OS, RAID | 480 GB or Higher, 8GB or Higher, Windows 10 or higher, R.A.I.D-1 redundant setup with 2x 480 GB or higher | |
| 7 | Tampering Alarm | Controller cover opening alarm | |
| 8 | Control | The system should have the capabilities of interacting (Monitoring & Control) with various applications on different network through the single Operator Workstation. It shall be possible to launch layouts, change layouts in real time using Tablet. | |

| **No** | **Parameters** | **Minimum Technical Requirements** | **Compliance (Yes /No)** |
|---|---|---|---|
| | **Make:** | | |
| | **Model:** | | |
| 9 | Keyboard & Mouse Extension | Keyboard and Mouse along with mechanism to extend them to 20mtrs. Operator desk from display controller to beprovided | |
| 10 | 24 x 7 operation | The controller shall be designed for 24 x 7 operation | |
| 11 | Redundancy | Redundant controller should be provided | |
| 12 | Others | The Video Wall and the Controller should beof the same make to ensure better performance and compatibility | |
| 13 | Output | DP/DVI/HDMI | |

| | | | |
|---|---|---|---|
| 14 | Input | H.264, MPEG2/4, MxPEG, MJPEG, V2D, H.263 or better | |
| 15 | Dimensions | 19" Rack mount | |
| 16 | Operating Conditions | 100-240V ,10-5A, 50/60Hz, Redundant Powersupply | |
| 17 | Wireless | The operator should be also possible to show Laptop Or Android/IoS phone over the video wall without disturbing the existing network over wireless | |
| 18 | Software | The software should be able to preconfigure various display layouts and access them atany time with a simple mouse click or schedule/timer based. | |
| 19 | Software | The software should be able display multiple sources anywhere on video wall in any size Key features of Video Wall management Software<br>•Central configuration database<br>•Browser based user interface<br>•Auto-detection of network sources<br>•Online configuration of sources, displaysand system variables | |
| 20 | Software | Video Wall Control Software shall allow commands on wall level or cube level or aselection of cubes:<br>• Switching the entire display wall on or | |

| No | Parameters | Minimum Technical Requirements | Compliance (Yes /No) |
|---|---|---|---|
| | **Make:** | | |
| | **Model:** | | |
| | | off.<br>• Setting all projection modules to a common brightness target, which can be either static (fixed) or dynamic to always achieve maximum (or minimum) common brightness between projection modules.<br>• Fine-tune colour of each cube | |
| 33 | Software | Should support Multiple clients / Consoles to control the Wall layouts | |

| | | | |
|---|---|---|---|
| 34 | Software | The Software should be able to share layouts b/w available different videowalls on same network as well as preview of sources on the workstation | |
| 35 | Software | Software should enable the user to display multiple sources (both local & remote) up to any size and anywhere on the display walls (both local & remote). | |
| 36 | Software | The software should be able to create layouts and launch them as and when desired | |
| 37 | Software | The display Wall and sources (both local & remote) should be controlled from Remote PC through LAN without the use of KVM Hardware. | |
| 38 | Software | Software should support display of Alarms | |
| 39 | Software | The software should provide at least 2 layers of authentication | |
| 40 | Software | Software should able to Save and Load desktop layouts from Local or remote machines | |
| 41 | Software | All the Layouts can be scheduled as per user convince.<br>Software should support auto launch of Layouts according to specified time event by user | |
| 42 | Software | It should be possible to create layouts comprising of screen scrapped content of Workstations, DVI inputs, Web sources, URLs | |

| No | Parameters | Minimum Technical Requirements | Compliance (Yes /No) |
|---|---|---|---|
| | **Make:** | | |
| | **Model:** | | |
| | | configured as sources. Layouts can be pre-configured or changed in real timeCan be pre-configured or changed in real time | |
| 43 | Software | It should be possible to schedule specific Layout based on time range It should be possible to share the layouts over LAN/WAN Network with Display in meeting room or on Remote Workstations connected on LAN/WAN Network | |
| 44 | Software | System should have a quick monitor area to access critical functions of the video wall User should be able to add or delete critical functions from quick monitor area Full featured Web services-based API supports Legacy RS-232 and TCP/IP. All software communication should be encrypted, Secure user Management with AD and LDAP Support Zero Maintenance, automatically saves the user's work | |
| 45 | Software | Integrated Embedded & External Audio formats with Audio decoding of video streams also possible. Software also supports UMD, IDC, Source name, Time (time zone aware), Date, text, Logo, Message Ticker, Source Status | |
| 46 | Software | The system shall include complete Bi-directional Soft KVM to permit operators to take mouse & keyboard control of Displays, Screen Scrapped applications and DVI source | |
| 47 | Software | It should be possible to create two separate Tickers which run concurrently. These can be positioned at top or bottom and can run independently. The Ticker can be picked from data source through screen scrapping or through typing specific incidence, manually | |

| | | | |
|---|---|---|---|
| 48 | Software | The system should have the capabilities of interacting (Monitoring & Control) with | |
| **No** | **Parameters** | **Minimum Technical Requirements** | **Compliance (Yes /No)** |
| | **Make:** | | |
| | **Model:** | | |
| | | various applications on different network through the single Operator Workstation. It shall be possible to launch layouts, change layouts in real time using Tablet | |
| 49 | Software | The control of the wall shall be possible via a network. All cubes shall have their own IP address, and the control software can access all of them at the same time. The available features shall be: On/Off, Brightness and Colour, Input control. Separate hardware server for monitoring features Wall or Panel On/Off, Brightness and Colour, Input control, health monitoring.<br><br>Also, software have feature to show maximum, minimum and current brightness / colour values of all the projectors. | |
| 50 | Software | Central setup & Connection management, Central configuration database, Fully distributed & modular component technology, Browser based UI, Auto-detection of network sources | |
| 51 | Software | Online configuration of sources, backup & restore, Scheduled backup, Fully features web services based API covering all legacy and encrypted communications | |
| 52 | Software | Save and load layouts (complete display presents including perspectives and applications), start stop and position applications & sources freely over the complete desktop, remote keyboard and mouse control from and towards other networked desktops (bi-directional) | |

| | | | |
|---|---|---|---|
| 53 | Software | Supported sources:<br>Analog & digital / streaming video, Analog (RGB) and Digital (DVI-I) Sources, Network desktops, Network multi-channel workstations and applications, Internet & | |
| **No** | **Parameters** | **Minimum Technical Requirements** | **Compliance (Yes /No)** |
| | **Make:** | | |
| | **Model:** | | |
| | | internet sources, Embedded & external audio formats, Localization | |
| 54 | Modules | The Display Modules, Display Controller & Software should be from a single OEM | |

### 6.2.16 Lan Networking For ICCC

- The System Integrator shall prepare the sites for commencement of work. Site preparation in terms of laying LAN cables in the buildings will be the responsibility of theSI. The SI would need to undertake the provisioning of LAN cabling between end usertill the access switch in each of the respective buildings as per the scope of work.
- SI shall provide and install all cables and connectors necessary, including both copper(Cat 6) and fiber optic patch cables, to complete the installation. The Authority expects all cables to be installed in a neat and workmanlike manner and adhere tobest practices for cable management.
- The SI is required to have structured cabling in place for both LAN and Internet Connectivity.
- All fiber jumper/patch cables installed must be labeled according to TIA/EIA standards and must indicate connections at both ends.
- When installing patch cables, the SI shall provide and install "hook and loop" stylewraps to provide proper support and management of cables. No plastic tie wraps maybe used.
- SI is responsible to provide and install horizontal wire management devices above,below, and between stacks of devices (only those devices part of this project) at allthe floors and wiring closets.
- The distance between any I/O point and the corresponding switch should not be morethan 90 meters. The place for installing the racks & network equipment will be theresponsibility of SI.
- Cat 6 shall be laid for connecting the user systems with the network.
- Fiber cables should be laid between any two uplinks between the NetworkEquipment's.

- Dedicated raceways / cable-trays should be used for laying LAN.
- Additional cabling requirements on an on-going basis shall also need to be cateredto.
- All the cable raceways shall be adequately grounded / Overheated and fully concealed with covers.
- The cables should be appropriately marked, numbered and labeled.
- There should be enough space between data and power cabling and there should not be any cross wiring of the two, to avoid any interference, or corruption of data.
- There shall not be any network outages in the existing network due to laying of new cables.

### 6.2.17 Centralized Help Desk

- Proposed helpdesk solution must provide flexibility of logging, viewing updating andclosing incident manually via web interface for issues.
- Helpdesk system should provide incident management, problem management templates along with helpdesk SLA system for tracking SLA's pertaining to incidentresolution time for priority / non- priority incidents.
- Helpdesk should be an ITIL certified tool from certified Authority like Pink Verify forIncident, Problem, Change, Knowledge, Configuration and SLA Management processes.
- The proposed helpdesk solution must have a built-in workflow engine to define escalations or tasks to be carried out after issues or change order are logged pertaining to surveillance project.
- Solution should provide a clustered view of recurring themes hidden in the huge quantities of data for spotting service desk trends easily
- Helpdesk should have capability to automatically categorize, understand the impact, and assign the service desk ticket to relevant helpdesk team members
- Centralized Help Desk System should have integration with Network / Server MonitoringSystems so that the Help Desk Operators can to associate alarms with Service Desktickets

### 6.2.18 IP Phones

| # | Parameter | Minimum Specifications | Compliance (Yes / No) |
|---|---|---|---|
| | **Make:** | | |
| | **Model:** | | |
| 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 10/100BASE-T Ethernet network through an RJ-45 interface | |
| 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 | 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 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 | |
| 16 | QoS | QoS mechanism through 802.1p/q | |

*6.2.18.1 IP PABX*

| # | **Minimum Specifications** | **Compliance (Yes / No)** |
|---|---|---|
| | **Make:** | |
| | **Model:** | |
| 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 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 in future | |
| 7. | The entire solution (IP PBX, its hardware, IP Phones, Voice Gateway) should be from a single OEM | |
| 8. | Support for call-processing and call-control | |
| 9. | Should support signaling standards/Protocols – SIP, MGCP, H.323, Q.Sig | |
| 10. | Voice Codec support - G.711, G 719, G.729, G.729ab, g.722, ILBC, GSM | |
| 11. | The System should have GUI support web-based management console | |
| 12. | Security | |
| 13. | The protection of signaling connections over IP by means of authentication, Integrity and encryption should be carried out using TLS | |
| 14. | System should support MLPP feature | |
| 15. | Proposed system should support SRTP for media encryption and signaling encryption by TLS | |
| 16. | 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 | |
| 17. | The administrator logging on to the call control server needs to authenticate by suitable mechanism such as User Login Information and Passwords/ Radius Server | |
| 18. | Voice gateway to be provided with 1 PRI card scalable to 3 PRI in future<br>for PSTN (PRI) line termination. | |

### 6.2.19 Three Monitoring Workstations:

| Sl. No | Parameter | Minimum Specifications | Compliance (Yes / No) |
|---|---|---|---|
| | **Make:** | | |
| | **Model:** | | |
| **1** | Processor | Intel i7 11th generation/AMD Rayzen Thread ripper or Higher latest Processor with 3GHz or higher frequency | |
| **2** | Chipset | Latest series 64bit Chipset | |
| **3** | Cores | 6 Cores or Higher | |
| **4** | RAM | Minimum 16 GB DDR4 or latest | |
| **5** | Graphics card | Minimum Graphics card with 1 GB or higher video | |
| | | memory (non- shared) | |
| **6** | HDD | 256 GB, PCIe NVMe, SSD and 1TB SATA SSD | |
| **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), HDMI Port and Mini DP Port | |
| **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 ICCC) | 1) PTZ speed dome control for IP cameras | |
| | | 2) Minimum 10 programmable buttons | |
| | | 3) Multi-camera operations | |
| | | 4) Compatible with all the camera models offered in the solution | |
| | | 5) Compatible with VMS /Monitoring software offered | |
| **14** | Monitor | Three Monitors of 22" TFT LED monitor, Minimum 1920 x 1080 resolution, 5 ms or better response time, TCO 05 (or higher) certified. The TFT Monitor, CPU, Mouse and keyboard workstation shall be of same make. | |
| **15** | Certification | Energy star 5.0/BEE star certified. | |
| **16** | Operating System | 64 bit pre-loaded OS Latest windows 11 pro or latest and MSOffice | |

| | | | |
|---|---|---|---|
| **17** | Security | BIOS controlled electro-mechanical internal | |
| | | chassis lock for the system. | |
| **18** | Warranty | Hardware /Software should have Minimum 5-year warranty. | |

### 6.2.20 Data Center & ICCC: Non-IT Components

ICCC and Data Center in terms of redundancy and concurrent maintainability requirements. Solution Provider is expected to establish and operationalize ICCC as per the location provided by PSCDL.

**General Standards for interiors and Console**

| Sl. No | Minimum Requirements |
|---|---|
| 1 | The ICCC interiors shall be state of the art adhering to the various best practices norms for integrated control centres, including:<br>• The scope of the project includes designing; engineering, supply & installation of 24X7 ICCC Interiors. As ICCC is a significant place, it is imperative that it is designed properly in terms of Aesthetics, Ergonomics and Functionality. Various aspects should be considered while designing ICCC area to create ideal workplace, considering physiological aspects such as line of sight and field of vision and cognitive factors such as concentration and perceptivity.<br>• Should have ISO 11064, ISO 14001 (environment), OHSAS 18001, HFE and ISO 9241 or similar certifications<br>• ICCC is considered to be heart of any Operation. Hence the project get world class ICCC in line to standard norms. The proposed interior material for ICCC should be designed properly in terms of Safety, Aesthetics, Ergonomics and Functionality<br>• The proposed wall panelling tiles and Ceiling tiles shall be industrial grade for surface spread of flame and smoke generation. This is mandatory to ensure that the materials used in the interiors do not provoke fire.<br>• Safety of User & ICCC: Safety is a high concern area therefore panelling and Plank ceiling must be standard one to withstand vibrations.<br>• Standard design feature of integrated channel in ceiling for quick installation& replace ability of continuous linear light: The ceiling system having integrated inbuilt channel for installation of cove lights and shall permit quick and easy replacement of cove light without using any tools.<br>• The Metal Panelling and Ceiling shall ensure restriction of hazardous substance so that the final product does not contaminate the environment and we give a healthy life to our coming generations.<br>• Sound transmission class (STC) value should be as per site conditions.<br>• Standard design feature of Load bearing capacity of panelling - panelling structure shall have sufficient load carrying capacity . |

### 6.2.21 Intranet router at DC:

| Sl. No | Technical Specification | Compliance (Yes / No) |
|---|---|---|
| | **Make:** <to be provided by the bidder> | |
| | **Model:** <to be provided by the bidder> | |

| | | |
|---|---|---|
| 1 | The Router Should support minimum 160 Gbps full duplex throughput and should be of max 3 RU in height, 19-inch rack mountable. Should have 8x10G SFP+ and 2x40G QSFP based ports on day one. | |
| 2 | Router should support Optical Transceiver Digital Diagnostic Monitoring. | |
| 3 | Router Should support Dual Images. | |
| 4 | Router should support jumbo frames (9000) on all ports | |
| 5 | Router should support BFD for single hop and multihop sessions. | |
| 6 | Router should support MPLS-FRR to ensure high availability. | |
| 7 | Router should support OSPFv2, OSPFv3, ISIS, BGPv4, MP-BGP, BGP confederations and route reflector and RSVP-TE Fast Reroute (FRR). | |
| 8 | Router should support VRRP, VRRPv3. | |
| 9 | IPv4 and IPv6 enabled from day one | |
| 10 | The Router scaling should be minimum:<br>a. 64K IPv4 FIB routes and 16K IPv6 FIB routes.<br>b. 32 VRF/L3VPN and 200 L2VPN.<br>c. HQoS and minimum 2K Queues.<br>d. 1K number of MPLS Labels (Provider Router).<br>e. 6PE /6VPE, MPLS label-Switching router (LSR & LER) functionality.<br>f. 4K VLANs. | |
| 11 | Shall support following class of service features:<br>a) Classification, policing, marking, shaping, filtering<br>b) Manage congestion using a weighted random early detection (WRED) algorithm<br>c) Ingress policing<br>d) egress shaping<br>e) strict queuing , WFQ<br>f) Router should be able to classify based on 802.1 ad, 802.1 p, EXP and DSCP bits | |
| 12 | Shall support the OAM feature<br>a) 802.3ah/802.1ag/TWAMP<br>b) LLDP | |
| 13 | IPv6 Features<br>a) IPv6 Ping<br>b) IPv6 trace route<br>c) OSPF v3<br>d) IS-IS | |
| 14 | Multicast Feature: It shall support following:<br>a) It shall support IGMP snooping v2/v3<br>b) The router shall support PIM Sparse Mode, RFC 4601<br>d) RFC 3569, Source Specific Multicast (SSM) | |
| 15 | Routers should support Timing and Synchronization such as Synchronous Ethernet or Precision Time Protocol (PTP) | |

| | | |
|---|---|---|
| 16 | The router shall support LACP 802.3ad and bundle upto 8 links. | |
| 17 | The router should support IP SLA or RPM (or equivalent) for performance measurements, it should also support monitoring of IP SLA/RPM (or equivalent) probes using SNMP polling (OEM has to provide SNMP MIB information) | |
| 18 | The router should support filtering based on different parameters like: src ip, dst ip, src port, dst port, protocol etc | |
| 19 | The Router Should support DHCP server and client functionality, it Should support DHCPv6 server/relay as well. | |
| 20 | The Router Should support DHCP based option 82. | |
| 21 | It shall support role based privileges for the system access and radius authentication. | |
| 22 | The router should have a Console or Out-of-band Management. | |
| 23 | Router should support Control-plane and management plane protection | |
| 24 | The Router Should support network management based on SNMP v2c/v3, Syslog, RADIUS/TACACS+, Access via CLI. | |
| 25 | The Router shall be able to operate at Operating Temperature: 0°C to 40°C and Operating Humidity: 20 - 80% RH non-condensing. | |
| 26 | The Router shall support dual redundant AC power supply and AC Power voltage shall be 110 - 240V. Should have dual power supply with hot swappable. | |
| 27 | The Router Should be NEBS Level III or equivalent complied. | |
| 28 | The Router operating system of the Routers category/series/family should be MEF-9/14 or CE (Carrier Ethernet) Certified/compliant. | |
| 29 | All necessary SFPs, interfaces, connectors, patch cords (if any) & licenses must be delivered along with the Router from day one.<br>Warranty –Hardware/ Software License should be for 5 years. | |

### 6.2.22 Backbone Router

| Sl. No | Technical Specification | Compliance (Yes / No) |
|---|---|---|
| | **Make:** <to be provided by the bidder> | |
| | **Model:** <to be provided by the bidder> | |
| 1 | The Router Should support minimum 80 Gbps full duplex throughput and should be of max 3 RU in height, 19-inch rack mountable. Should have 8x10G SFP+ based ports on day one. | |
| 2 | Router should support Optical Transceiver Digital Diagnostic Monitoring. | |

| | | |
|---|---|---|
| 3 | Router Should support Dual Images. | |
| 4 | Router should support jumbo frames (9000) on all ports | |
| 5 | Router should support BFD for single hop and multihop sessions. | |
| 6 | Router should support MPLS-FRR to ensure high availability. | |
| 7 | Router should support OSPFv2, OSPFv3, ISIS, BGPv4, MP-BGP, BGP confederations and route reflector and RSVP-TE Fast Reroute (FRR). | |
| 8 | Router should support VRRP, VRRPv3. | |
| 9 | IPv4 and IPv6 enabled from day one | |
| 10 | The Router scaling should be minimum:<br>a. 32K IPv4 FIB routes and 8K IPv6 FIB routes.<br>b. 32 VRF/L3VPN and 200 L2VPN.<br>c. HQoS and minimum 2K Queues.<br>d. 1K number of MPLS Labels (Provider Router).<br>e. 6PE /6VPE, MPLS label-Switching router (LSR & LER) functionality.<br>f. 4K VLANs. | |
| 11 | Shall support following class of service features:<br>a) Classification, policing, marking, shaping, filtering<br>b) Manage congestion using a weighted random early detection (WRED) algorithm<br>c) Ingress policing<br>d) egress shaping<br>e) strict queuing , WFQ<br>f) Router should be able to classify based on 802.1 ad, 802.1 p, EXP and DSCP bits | |
| 12 | Shall support the OAM feature<br>a) 802.3ah/802.1ag/TWAMP<br>b) LLDP | |
| 13 | IPv6 Features<br>a) IPv6 Ping<br>b) IPv6 trace route<br>c) OSPF v3<br>d) IS-IS | |
| 14 | Multicast Feature: It shall support following:<br>a) It shall support IGMP snooping v2/v3<br>b) The router shall support PIM Sparse Mode, RFC 4601<br>d) RFC 3569, Source Specific Multicast (SSM) | |
| 15 | Routers should support Timing and Synchronization such as Synchronous Ethernet or Precision Time Protocol (PTP) | |
| 16 | The router shall support LACP 802.3ad and bundle upto 8 links. | |
| 17 | The router should support IP SLA or RPM (or equivalent) for performance measurements, it should also support monitoring of IP SLA/RPM (or equivalent) probes using SNMP polling (OEM has to provide SNMP MIB information) | |

| | | |
|---|---|---|
| 18 | The router should support filtering based on different parameters like: src ip, dst ip, src port, dst port, protocol etc | |
| 19 | The Router Should support DHCP server and client functionality, it Should support DHCPv6 server/relay as well. | |
| 20 | The Router Should support DHCP based option 82. | |
| 21 | It shall support role based privileges for the system access and radius authentication. | |
| 22 | The router should have a Console or Out-of-band Management. | |
| 23 | Router should support Control-plane and management plane protection | |
| 24 | The Router Should support network management based on SNMP v2c/v3, Syslog, RADIUS/TACACS+, Access via CLI. | |
| 25 | The Router shall be able to operate at Operating Temperature: 0°C to 60°C and Operating Humidity: 20 - 90% RH non-condensing. | |
| 26 | The Router shall support dual redundant AC power supply and AC Power voltage shall be 110 - 240V. Should have dual power supply with hot swappable. | |
| 27 | The Router Should be NEBS Level III or equivalent complied. | |
| 28 | The Router operating system of the Routers category/series/family should be MEF-9/14 or CE (Carrier Ethernet) Certified/compliant. | |
| 29 | All necessary SFPs, interfaces, connectors, patch cords (if any) & licenses must be delivered along with the Router from day one.<br>Warranty –Hardware/ Software License should be for 5 years. | |

| Sl. No | Minimum Specifications | Compliance (Yes / No) |
|---|---|---|
| | a. Designer Acoustic Metal False ceiling with Plank<br>b. ICCC ceiling must be 100% modular to accommodate future technological expansions/retrofitting without taking any shut-downs and must be easily replaceable in case of damage.<br>c. The proposed ceiling tiles shall be as per industrial grade standards .<br>d. Standard design feature of integrated channel in ceiling for quick installation & replace ability of continuous linear light: The ceiling system having integrated inbuilt channel for installation of cove lights and shall permit quick and easy replacement of cove light without using any tools.<br>e. The Ceiling system must ensure restriction of hazardous substance in any of the materials.<br>f. The Non uniform gaps between the designer Metal ceiling / Grid type Snap Fit Ceiling shall be covered with Calcium Silicate Ceiling.<br>g. **Control Desk:** The control desk solution shall conform to high standard of engineering. It shall be capable of performing 24X7 operations under the all environmental conditions.<br>h. **Structure:** - Made of heavy duty Extruded Vertical and Horizontal Aluminium profiles. The Extrusions shall be duly powder coated with 40+ micron over all surfaces. All sheet metal parts must be finished with a durable, black, electrostatic powder coating.<br>i. To allow future extension and expansion, a weld free system shall be proposed. Interconnecting joints shall not be visible. The structure shall be rigid enough. The | |

| | | |
|---|---|---|
| | structure shall allow easy assembly of Hinged Shutters, Slat wall, Gland Plate, Monitor arms in extremely rigid manner.<br>j. **Table-top:** - The material of the working surface should be of industrial grade.<br>k. **Front Edge:** - Industrial Standard design feature of modular Edge. The edge shall be mechanically replaceable in case of damage or wear without opening or removing the worktop.<br>l. Slat Wall shall be made of industrial grade material .<br>m. **Monitor Arm:** - Feature of monitor arm assembly shall have auto lock, push & remove feature for quick release of VESA mounts and modular arm extensions for ease in maintenance and fixing of monitor .<br>n. **Shutters & Side Legs:** - Front, back shutters shall be industrial grade material . Side leg shall be of the same finish.<br>o. **Cable Trays Cable Trays and Wiring:** - The desks must be designed with vertical and horizontal cable trays to allow for continuous cable management between the cabinets. Wire shall be routed into the cabinet through gland plate.<br>p. Acoustic Metal Panelling: Factory made removable type self inter lockable metal panels with front sheet of Preformed Textured Hot dip galvanized sheet with rigid polyvinylchloride (PVC) film on one side and on the other side a coating to avoid rust . The panelling design shall comprise of specially designed combination of perforated and non-perforated panels through CNC laser Cutting, bending & punching.<br>q. **Acoustic Metal Partition** - The material of construction shall remain the same however in partition the cladding shall be done on either side of the section/grid work.<br>r. Sound transmission class (STC) value as per site conditions.<br>s. Standard design feature of Load bearing capacity of panelling - panelling structure shall have sufficient load carrying capacity .<br>t. The Metal Panelling and Ceiling shall ensure restriction of hazardous substance so that the final product does not contaminate the environment and we give a healthy life to our coming generations.<br>u. Industrial grade feature of Modular wall panelling tile having secure locking arrangement for equidistant mounting.<br>v. **Acoustic Laminate Flooring:** - Acoustic flooring shall be decorative type of approved shade, pattern, texture and design and of industrial grade. Dimensions shall be as per the final approved design and site requirement. Flooring shall be laid over concrete floor with laying compound. | |

| Sl. No | Minimum Specifications | Compliance (Yes / No) |
|---|---|---|
| | w. False Flooring: Mandatory: Top Surface shall be Acoustic Laminate flooring.<br>x. The Panel should be as per industrial grade.<br>y. Painting: To maintain the aesthetic appeal of the ICCC, painting shall be done only on those walls which are not visible within & from the ICCC. | |

**Fireproof Enclosure**

| Sl. No. | Minimum Specification |
|---|---|
| 1 | Capacity: as per site requirement. |

**Fire Suppression System**

| Sl. No | Minimum Specification | Compliance (Yes / No) |
|---|---|---|
| 1 | Comply with NFPA 2001 or ISO 14520 standard or better . Hardware should have 5 year warranty | |
| 2 | Be efficient, effective and shall not require excessive space and high pressure for storage. | |
| 3 | Key components are valves and its accessories, actuators, flexible discharge and connection hoses, check valves, pressure switch, and nozzles | |

**Water Leak Detection System**

| Sl. No | Minimum Specification |
|---|---|
| 1 | • Should be mechanically strong, resistant to corrosion and abrasion.<br>• Shall have end circuit to detect open circuit fault. |

**Raised Floor**

| Sl. No | Minimum Specification | Compliance (Yes / No) |
|---|---|---|

| | | |
|---|---|---|
| 1 | System:<br>• Access floor system to be installed at finished floor height as per site conditions.<br>• The system will provide for suitable pedestal and under-structure designed to withstand various static loads and rolling loads subjected to it in an office / server / DCS / panel / rack area.<br>The entire Access floor system will provide for adequate fire resistance, acoustic barrier and air leakage resistance. | |

**PVC Conduit**

| Sl. No. | Minimum Specification | Compliance(Yes/No) |
|---|---|---|
| 1 | • The conduits for all systems shall be high impact rigid PVC heavy-duty type and shall comply with I.E.E regulations for standardized conduit.<br>• All sections of conduit and relevant boxes shall be properly cleaned and glued using appropriate epoxy resin glue and the proper connecting pieces, like conduit fittings such as Mild Steel and should be so installed that they can remain accessible for existing cable or the installing of the additional cables.<br>• Conduit runs shall be so arranged that the cables connected to separate main circuits shall be enclosed in separate conduits, and that all lead and return wire of each circuit shall be run to the same circuit.<br>• All conduits shall be smooth in bore, true in size and all ends where conduits are cut shall be carefully made true and all sharp edges trimmed. All joints between lengths of conduit or between conduit and fittings boxes shall be pushed firmly together and glued properly.<br>• Cables shall not be drawn into conduits until the conduit system is erected, firmly fixed and cleaned out. Not more than two right angle bends or the equivalent shall be permitted between draw and junction boxes<br>• Conduit concealed in the ceiling slab shall run parallel to walls and beams and conduit concealed in the walls shall run vertical or horizontal.<br>• The chase in the wall required in the recessed conduit system shall be neatly made and shall be of angle dimensions to permit the conduit to be fixed in the manner desired. | |

**Wiring**

| Sl. No | Minimum Specification | Compliance (Yes / No) |
|---|---|---|

| | | |
|---|---|---|
| **1** | • PVC insulated copper conductor cable shall be used for sub circuit runs from the distribution boards to the points and shall be pulled into conduits. They shall be stranded copper conductors as per industrial grade. Colour code for wiring shall be followed.<br>• Looping system of wring shall be used, wires shall not be jointed. No reduction of strands permitted at terminations. | |

| Sl. No | Minimum Specification | Compliance (Yes / No) |
|---|---|---|
| | • Wherever wiring is run through trucking or raceways, the wires emerging from individual distributions shall be bunched together with cable straps at required regular intervals. Identification ferrules indication the circuit and D.B. number shall be used for sub main, sub circuit wiring the ferrules shall be provided at both end of each sub main and sub-circuit.<br>• Where, single phase circuits are supplied from a three phase and a neutral distribution board, no conduit shall contain wiring fed from more than one phase in any one room in the premises, where all or part of the electrical load consists of lights, fans and/or other single phase current consuming devices, all shall be connected to the same phase of the supply.<br>• Circuits fed from distinct sources of supply or from different distribution boards or M.C.B.s shall not be bunched in one conduit. In large areas and other situations where the load is divided between two or three phases, no two single-phase switches connected to difference phase shall be mounted within two meters of each other.<br>• All splicing shall be done by means of terminal blocks or connectors and no twisting connection between conductors shall be allowed.<br>• Metal clad sockets shall be of die cast non-corroding zinc alloy and deeply recessed contact tubes. Visible scraping type earth terminal shall be provided. Socket shall have push on protective cap.<br>• All power sockets shall be piano type with associate's switch of same capacity. Switch and socket shall be enclosed in a mild steel sheet enclosure with the operating knob projecting. Entire assembly shall be suitable for wall mounting with Bakelite be connected on the live wire and neutrals of each circuit shall be continuous everywhere having no fuse or switch installed in the line excepting at the main panels and boards. Each power plug shall be connected to each separate and individual circuit unless specified otherwise. The power wiring shall be kept separate and distinct from lighting and fan wiring. Switch and socket for light and power shall be separate units and not combined one.<br>• Balancing of circuits in three phases installed shall be arranged before installation is taken up. | |

**Earthing**

| Sl. No | Minimum Specification | Compliance(Yes/No) |
|---|---|---|

| | | |
|---|---|---|
| **1** | All electrical components are to be earthen by connecting two earth tapes from the frame of the component ring and will be connected via several | |
| **Sl. No** | **Minimum Specification** | **Compliance(Yes/No)** |
| | earth electrodes. The cable arm will be earthen through the cable glands. Earthling shall be in conformity with provision of latest Indian Electricity rules and as per IS standard. The entire applicable IT infrastructure in the ICCCs shall be earthed.<br>• Earthing should be done for the entire power system and provisioning should be there to earth UPS systems, Power distribution units, and A.C units etc. so as to avoid a ground differential. State shall provide the necessary space required to prepare the earthing pits.<br>• All metallic objects on the premises that are likely to be energized by electric currents should be effectively grounded.<br>• The connection to the earth or the electrode system should have sufficient low resistance in the range of 0 to 10 ohm to ensure prompt operation of respective protective devices in event of a ground fault, to provide the required safety from an electric shock to personnel & protect the equipment from voltage gradients which are likely to damage the equipment.<br>• Recommended levels for equipment grounding conductors with very low impedance level.<br>• There should be enough space between data and power cabling and there should not be any cross wiring of the two, in order to avoid any interference, or corruption of data.<br>• The earth connections shall be properly made. A small copper loop to bridge the top cover of the transformer and the tank shall be provided to avoid earth fault current passing through fastened bolts, when there is a lighting surge, high voltage surge or failure of bushings.<br>• A complete copper mesh earthing grid needs to be installed for the server farm area, every rack need to be connected to this earthing grid. A separate earthing pit need to be in place for this copper mesh.<br>• Provide separate Earthing pits for Servers, UPS & Generators as per the standards. | |

**Cable Work**

| Sl. No | Minimum Specification |
|---|---|
| 1 | • Cable ducts should be of such dimension that the cables laid in it do not touch one another. If found necessary the cable shall be fixed with clamps on the walls of the duct. Cables shall be laid on the walls/on the trays as required using suitable clamping/ fixing arrangement as required. Cables |
| **Sl. No** | **Minimum Specification** |
| | shall be neatly arranged on the trays in such manner that a criss-crossing is avoided and final take off to switch gear is easily facilitated.<br>• All cables will be identified close to their termination point by cable number as per circuit schedule. Cable numbers will be punched on 2mm thick standard strips and securely fastened to the. In case of control cables all covers shall be identified by their wire numbers by means of PVC ferrules. For trip circuit identification additional red ferrules are to be used only in the switch gear / control panels, cables shall be supported so as to prevent appreciable sagging. In general distance between supports shall not be greater than 600mm for horizontal run and 750mm for vertical run or as per site conditions.<br>• Each section of the rising mains shall be provided with suitable wall straps so that same can be mounted on the wall.<br>• Whenever the rising mains pass through the floor they shall be provided with a built-in fire proof barrier so that this barrier restricts the spread of fire through the rising mains from one section to the other adjacent section.<br>• Neoprene rubber gaskets shall be provided between the covers and channel to satisfy the operating conditions imposed by temperature weathering, durability etc.<br>• Necessary earthling arrangement shall be made alongside the rising mains enclosure by Mean of a GI strip of adequate size bolted to each section and shall be earthed at both ends. The rising mains enclosure shall be bolted type.<br>• The space between data and power cabling should be as per standards and there should not be any criss-cross wiring of the two, in order to avoid any interference, or corruption of data. |

**Air-conditioning**

| Sl. No | Minimum Specification | Compliance (Yes / No) |
|---|---|---|
| | Make: | |
| | Model: | |

| | | |
|---|---|---|
| 1 | • Cooling Capacity as per the requirements at each of the ICCCs<br>• Compressor – As per site condition<br>• Refrigerant – As per site condition<br>• Power Supply – Three Phase, 380-415 V, 50 Hz<br>• Air Flow Rate – minimum 19 cu m / min<br>• Noise Level - < 50 dB<br>• Operation – Remote Control | |

**Fire Alarm System**

| Sl. No | Minimum Specification | Compliance (Yes / No) |
|---|---|---|
| 1 | • **System Description**<br>➢ The Fire alarm system should be installed as per latest NFPA 72 guidelines.<br>➢ Detection shall be by means of automatic heat and smoke detectors (multi sensor) located throughout the ICCC (ceiling, false floor and other appropriate areas where fire can take place) with break glass units on escape routes and exits.<br>•<br>• **Smoke detectors** – Smoke detectors shall be of the optical or ionization type.<br>➢ Heat detectors<br>➢ Heat detectors shall be of the fixed temperature (58° C) or rate of temperature rise type with a fixed temperature operating point.<br>➢ Detector bases shall fit onto an industry standard conduit box.<br>• **Audible Alarms** – Electronic sounders shall be provided. | |

**Access Control System**

| Sl. No | Minimum Specification | Compliance (Yes / No) |
|---|---|---|
| 1 | The Access Control System shall be deployed with the objective of allowing entry and exit to and from the premises to authorized personnel only. The system deployed shall be based on Biometric Technology. Access control shall be provided for entry / exit doors. These doors shall be provided with electric locks, and shall operate on fail-safe principle. The lock shall remain unlocked in the event of a fire alarm or in the event of a power failure. The fire alarm supplier shall make potential free contacts available for releasing the locks in a fire condition especially for staircase and main doors. Entry to the restricted area shall be by showing a proximity card near the reader and exit shall be using a push button installed in the secure area. The system shall monitor the status of the doors through magnetic reed contacts. The system should be designed and implemented to provide following functionality:<br>• Controlled Entries to defined access points.<br>• Controlled exits from defined access points.<br>• Controlled entries and exits for visitors. | |

| | | |
|---|---|---|
| | • Configurable system for user defined access policy for each access point.<br>• Record, report and archive each and every activity (permission granted and / or rejected) for each access point.<br>• User defined reporting and log formats.<br>• Fail safe operation in case of no-power condition and abnormal condition such as fire, theft, intrusion, loss of access control, etc.<br>• Day, Date, Time and duration based access rights should be user configurable for each access point and for each user.<br>• One user can have different policy / access rights for different access points Hardware / Software should have 5 year warranty. | |

**Ceiling Speakers**

| Sl. No | Minimum Specification | Compliance (Yes / No) |
|---|---|---|
| 1 | • The ceiling speakers shall have high power and high sensitivity with extended frequency responses.<br>• The ceiling speakers shall have wide, controlled constant directivity dispersions for optimum coverage.<br>• The ceiling speakers shall have in-built amplifiers or shall be supported by an external amplifier.<br>• The ceiling speakers shall have a conical coverage pattern.<br>• The ceiling speakers shall be in a colour to match the ceiling and surrounding interior design.<br>• Full audio coverage within the command centre room and video room should be made.<br>• The Ceiling Speakers shall automatically adjust the output audio level based on ambient noise.<br>• Hardware /Software should have 5-year warranty | |

**Diesel Generator Set 200 KVA Specification: Kirloskar/Cummins/Eicher/Mahindra/Cooper**

| Sl. No | Minimum Specification | Compliance (Yes /No) |
|---|---|---|
| | **Make:** | |
| | **Model:** | |

| | | |
|---|---|---|
| 1 | DIESEL ENGINE SPECIFICATION:<br>Diesel Engine 6 cylinders, water cooled, turbocharged, developing suitable BHP @ 1500 RPM, confirming to ISO 3046/ BS:5514, with an overload capacity of 10% for One hour in any 12 continuous hours operation. DG set shall be BMS compatible. The bidder shall ensure compliance to relevant Central Pollution Control Board (CPCB) guidelines as applicable. | |
| | The Engine shall be complete with following accessories<br>• In-line fuel pump with mechanical governor<br>• Optimised turbocharger<br>• Stainless steel exhaust flexible coupling<br>• Silencer<br>• Radiator<br>• Coolant inhibitor<br>• Plate-type lube oil cooler<br>• Dry-type, heavy duty, replaceable paper element air cleaner with restriction indicator<br>• Flywheel housing and flywheel to suit single bearing alternator<br>• Electrical starter motor<br>• Battery charging alternator<br>• First fill lube oil | |
| 2 | ALTERNATOR SPECIFICATIONS:<br>Stamford make standard design alternator, suitably rated at 200KVA, 0.8P.F., 415 Volts, 3 phases, 4 wires, 50 cycles/sec., 1500RPM, self-excited & self-regulated, with brushless excitation, band of voltage regulation 61% of rated voltage, from no load to full load. Insulation class 'H'. The alternator generally conforms to BS:5000/IS:4722.<br>• Self-excited, self-regulated<br>• Class 'H' insulation<br>• Salient pole revolving field<br>• Single bearing<br>• Digital automatic voltage regulator (part of PCC 1301) | |
| 3 | BASE FRAME:<br>Sturdy, fabricated, welded construction, channel iron base frame for mounting above Engine & Alternator. | |
| 4 | FUEL TANK:<br>400 Litres capacity fuel tank with mounting brackets, complete with level indicator, fuel inlet & outlet, air vent, drain plug, inlet arrangement for direct filling & set of 5 ft. Long fuel hoses. | |
| 5 | BATTERY:<br>Set of 2 nos., 12V, Dry Lead acid automotive batteries. | |

| | | |
|---|---|---|
| 6 | MANUAL CONTROL PANEL:<br>Cubicle Type, floor mounting control panel with hinged doors, undrilled bottom gland plate, AL. Bus Bar & accommodating following, Panel shall be BMS compatible. | |
| 7 | SWITCH GEARS:<br>• 1250A, 4 Pole Contactor for ALTERNATOR with Thermal O/L relay<br>• BACK-UP PROTECTION:<br>• HRC fuse for short circuit protection. | |
| 8 | MICROPROCESSOR BASED AMF MODULE INCORPORATING:<br>Functions: | |
| | • Supply Failure Timer<br>• Restoration Timer<br>• Impulse automatic engine start / stop logic<br>• Mains / Generator Voltage & Frequency sensing<br>Controller with the following features:<br>Water Temperature/ Lube Oil Pressure / engine speed<br>Voltage / Ampere / Frequency / kVA o Running-hour counter<br>No. of starts<br>• Fault Indication (LED Type)<br>Over /Under Speed<br>Fails to Start<br>Low Oil pressure<br>High Engine Temperature<br>Under / over voltage<br>Over current<br>• Combined Meter for kW / Power Factor / KVA<br>• Electronic kWH Meter (Counter Display)<br>• Current Transformers | |
| 9 | Relay:<br>• Earth Fault Relay (Electronic type)<br>• Reverse Power Relay | |
| 10 | Indications (LED):<br>• DG ON, Load on DG<br>• Mains ON, Load on Mains, Battery Charger ON | |
| 11 | Push Buttons (AMF MODULE BY PASS MODE):<br>• Generator Contactor CLOSE / TRIP<br>• Mains Contactor CLOSE / TRIP (If Provided)<br>• Fault ACCEPT / RESET | |
| 12 | BATTERY CHARGER:<br>• SMPS Based Unit with inbuilt Auto / Manual & Float /Boost Facility<br>• DC Voltmeter & Ammeter (Separate)<br>• PLHO / 0712/RKS/ASN | |

**Online UPS for indoor (Data Center / ICCC) Location: 60 kVA**

| Sl. No | Minimum Specification | Compliance (Yes / No) |
|---|---|---|
| | **Make:** | |
| | **Model:** | |
| 1 | Capacity / Credentials: Adequate capacity to cover all above IT Components at respective location. Modular (only for ICCC/DC), Redundant(N+N), Scalable upto 300kva & with Hot Swappable type full rated rectifier, inverter & battery charger Power Modules of capacity more than 60 kVA for Command Centre/Data Centre UPS with 10" inch Touch LCD. Hot swap type Dual and Redundant |
| **Sl. No** | **Minimum Specification** | **Compliance (Yes / No)** |
| | **Make:** | |
| | **Model:** | |
| | main Controller & Hot swap type with Static Switch. Unitary type UPS for all other purpose in Indoor requirements. | |
| 2 | Output Waveform: Pure Sine wave | |
| 3 | Output Power Factor at Full Load: >0.90 for input & Unity for Output | |
| 4 | Input: Three Phase 3 Wire | |
| 5 | Input Voltage Range: 305-445 VA Cat Full Load, or 3Ph and 175-280VAC at Full Load for 1Ph, 50Hz+/-3 Hz | |
| 6 | Output Voltage: 400V AC, Three Phase for over 60 KVA UPS Else Single Phase 220/230/240 Vac | |
| 7 | Output Frequency: 50 Hz+/-0.5 % (Free running); +/-3 % (Sync. Mode) | |
| 8 | Inverter efficiency: >90% | |
| 9 | Overall AC-AC Efficiency: >88% for 1Ph & 95% for all 3Ph UPS | |
| 10 | UPS Shutdown: UPS should shut down with an alarm and indication on following conditions 1) Output over voltage 2) Output under voltage 3) Low Battery 4) Inverter over load 5) Over temperature 6) Output short | |
| 11 | Battery Back-up: Min 2 Hours and as per design consideration (On 0.8 O/P PF load) | |

| | | |
|---|---|---|
| 12 | Battery: For ICCC/DC, only Li-Ion batteries to be supplied with NMC technology. Compliance/Certification to IEC 62619 or equivalent or Higher, UN38.3. Compact form factor with individual rack of 600mm(W) x 1090mm(D) x 2000mm(H). 2 Level BMS Design (Module CMU & Rack BMU). Communication - CAN2.0/RS485 | |
| 13 | 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. Event log in display – min 200 no's for 3Ph Unitary UPS & min. 10000 nos for Modular UPS (for ICCC/DC) | |
| 14 | Not used. | |
| 15 | Cabinet: Tower (other than DC UPS if required) / Modular type (For ICCC/DC UPS), SNMP support through TCP/IP | |
| **Sl. No** | **Minimum Specification** | **Compliance (Yes / No)** |
| | **Make:** | |
| | **Model:** | |
| 16 | Operating Temperature - As per City condition and requirement (0 to 50 deg without de-rating on offered O/p Power Factor) | |
| 17 | Management Protocol: SNMP Support through TCP/IP. Warranty – 5 years | |

**UPS for Outdoor application (2 KVA)**

| Sl. No | Minimum Specification | Compliance (Yes / No) |
|---|---|---|
| | **Make:** | |
| | **Model:** | |
| 1 | Capacity: Adequate capacity to cover filed sensors and installations respective location | |
| 2 | Output Waveform: Pure Sine wave | |
| 3 | Input & Output Power Factor at Full Load: min. 0.90 | |
| 4 | Input: Single Phase | |
| 5 | Input Voltage Range:<br>Single Phase 175 to 280Vac for any rating below 10kva | |

| | | |
|---|---|---|
| 6 | Output Voltage: 400V AC, Three Phase for over 2 KVA UPS. Single Phase 220/230/240Vac for any rating below 10kva. UPS below 3kva shall have min. one programmable inbuilt Indian type Outlet at back of UPS | |
| 7 | Output Frequency: 50 Hz+/-0.5 %( Free running); +/-3 %( Sync. Mode) | |
| 8 | Inverter efficiency: >90% | |
| 9 | Overall AC-AC Efficiency: >89% for 1 Ph upto 3kva. For 5kva or higher – 95% | |
| 10 | UPS Shutdown: UPS should shut down with an alarm and indication on following conditions 1) Output over voltage 2) Output under voltage 3) Low Battery 4) Inverter over load 5) Over temperature 6) Output short | |
| 11 | Battery Back-up: Min 2 Hours and as per design consideration (on 0.8 O/p PF load). All UPS below 5kva shall have min. internal charger capacity of 15A | |
| 12 | Battery: VRLA (Valve Regulated Lead Acid), SMF (Sealed Maintenance Free) | |
| **Sl. No** | **Minimum Specification** | **Compliance (Yes / No)** |
| | **Make:** | |
| | **Model:** | |
| 13 | Indicators & Metering(LCD) : Indicators for AC Mains, Load on Battery, Fault, Load Level, Low Battery Warning, Inverter On, UPS on By- pass,Overload, etc. | |
| 14 | Metering for Input Voltage, Output Voltage and frequency, battery voltage, output current(for any 3PH UPS) etc. | |
| 15 | Audio Alarm: Battery low, Mains Failure, Over temperature, Inverter overload, Fault etc. | |
| 16 | Cabinet: Rack/Tower type. Should have 5 year warranty | |

**6.3 Cloud Services to deploy all smart solutions**

It proposed to have all the smart solutions deployed on industry standard Cloud. It isproposed to host all ICCC applications and smart solution applications on industry standard Cloud. The proposed Cloud Service Provider (CSP) should be MeiTY empaneled and offer all services from India only as per guidelines of MeiTY. The solution provider should estimate the required cloud computing requirements based the proposed solution.

Detailed architecture is mentioned in Sec. 5.3: Finalization of Detailed Technical Architecture

And following are the minimum technical requirements,

i) Cloud DR Should be at least 500 KM from On-premise Data Centre and

ii) Both On-premise DC and Cloud DR should be in the different seismic zone and

iii) Both On-premise DC and Cloud DR should not be in same River Flood plain and

iv) The proposed Cloud Data center must be TIA 942/Tier III or above for better availability of cloud services and certified under:

a) Valid and active TIA 942/ Uptime Institute Certification

b) CSP to have ISO-22301 or similar certification for business continuity.

c) The CSP should provide financially backed SLAs for all the services offered.

d) The offered cloud solution of proposed CSP should be as per MeiTY guidelines.

Following are the minimum expected Cloud Services specifications

| Sl. No | Specifications | Compliance (Yes / No) |
|---|---|---|
| | **Make:** | |
| | **Model:** | |
| 1 | The CSP must provide the following services from both DC and DR<br>VM and dedicated physical server based compute services | |
| 2 | Multiple options of storage including managed disks, unmanaged disks, block storage, file share and data lake storage in multiple performance tiers. | |
| 3 | PaaS/SAAS, IAAS Services to be offered. | |
| 4 | Options for container registry and resource template libraries to support faster deployment and best practice implementation. | |
| 5 | Managed instances and Database as a service for databases such as Microsoft SQL, MYSQL and PostGre SQL etc | |
| 6 | | |
| 7 | Options for shipping of data from CSP to department if required for backup purposes | |
| 8 | Native Firewall, EDR and WAF services both as a native PaaS from the CSP as well as certified third party solutions. | |
| 9 | Native Bastion host as a service to ensure secure and resilient access to VMs without opening up public IP addresses. | |

| | | |
|---|---|---|
| 10 | Native CSP VPN based access to cloud services to ensure no open direct public IP based access to any cloud service under this RFP. | |
| 11 | | |
| 12 | Offering for perimeter, host and in-memory security solutions for the compute and storage offerings provided by CSP. | |
| 13 | The CSP should provide the below or equivalent services seamlessly:<br>• Layer 3 and Layer 4 Firewall<br>• Layer 7 Firewall (WAF)<br>• SIEM & SOAR ( CSP / CSP marketplace)<br>• Vulnerability Scanner<br>• Endpoint Security ( Attack Surface Management)<br>• Backup Tools<br>• Disaster Recovery Tools | |
| 14 | The CSP should have minimum following features .<br>• Providing the Public Cloud Services (PaaS OR SaaS) in India | |
| 15 | CSP should support both BYOL (Bring your own license) and with a Pay as you go option. The OS offered should come with continuous updates and upgradesanytime. | |
| 16 | Monitoring services for cloud resources hosted in the data centre and support for customized report generation. | |
| 17 | Blank | |
| 18 | Blank | |
| 19 | Blank | |
| 20 | Data Centers should be compliant to MeitY recommended security guidelines. | |
| 21 | Blank | |
| 22 | The CSP must support dedicated connectivity from at least 3 ISP providers for department/organization to choose between at the time of deployment. | |
| 23 | Cloud Native Monitoring & Management & Security Services | |

| | | |
|---|---|---|
| 24 | Cloud Resource Monitoring: Capability to monitor cloud environment centrally, custom monitoring metrics, monitor and store logs, view graphs & statistics, set alarms, monitor and react to resource changes. Support monitoring of custom metrics generated by your applications and services and any log files your applications generate. Gain system-wide visibility into resource utilization, application performance, and operational health, using these insights to react intelligently and keep applications running smoothly. | |
| 25 | Audit Trail: Logs of all user activity within a CSP account including actions taken through the CSP's Management Console, CSP's SDKs, command line tools, and other CSP services. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the Cloud service. | |
| 26 | Cloud Advisor: Analyses the Cloud environment and provides best practice recommendations (or checks) in five categories: cost optimization, security, fault tolerance, performance, and service limits. | |
| 27 | Cloud Service Providers must offer Cloud native/ 3rd party SIEM Marketplace solutions turnkey SIEM offering by which customers can configure real-time analysis and alerting of security events. At a minimum, the integration or service must support alerting, log retention and some form of forensic analysis that is able to search across logs and periods of time for patterns. | |
| 28 | Cloud Service Providers should provide Integration with existing Local identity management system (that is, local accounts) with granular role-based authorization for network services in both the service interfaces and management console. At a minimum, the role-based authorization must support assigning authorization based on individual users and groups of users and delineation must be assignable per firewall, load balancer, IP address and network segment and support, as applicable, the following granular actions: create, delete and configure. | |
| 29 | Cloud Service Providers must allow customers to access the cloud service via an IPsec VPN tunnel or Secure Sockets Layer (SSL) VPN tunnel over the public Internet. This shall be a self service capability from the provider side, with the capability to make configurations for customer | |
| 30 | Blank | |

| | | |
|---|---|---|
| 31 | A CSP must provide an option to the customer to encrypt the data on the instance block storage volume so that data remains encrypted at rest. This shall be a simple, self-service option when the instance is provisioned. | |
| 32 | The block and object storage services must offer customers the self-service ability from both management console and Command Line Interface to opt into provider-enabled server side encryption (SSE) for objects or object hierarchies within the storage service. | |
| 33 | Large instance support: Providers must offer customers instances with a large number of processor cores and memory for processor- or memory intensive use cases. The provider must be able to provide instances that support at larger vCPUs and RAM. | |
| 34 | Cloud provider should offer a dashboard that displays up-to-the minute information on service availability across multiple regions. | |
| 35 | Cloud provider should offer Service Health Dashboard history as required | |
| 36 | Cloud provider should offer a service that acts like a customized cloud expert and helps provision resources by following best practices. | |
| 37 | Monitoring tools that will enable collection and tracking metrics, collection and monitoring log files, set alarms, and automatically react to changes in the provisioned resources. The monitoring tools should be able to monitor resources such as compute and other resources to gain system-wide visibility into resource utilization, application performance, and operational health. | |
| 38 | Able to define guidelines for provisioning and configuring cloud resources and then continuously monitor compliance with those guidelines. Ability to choose from a set of pre-built rules based on common best practices or custom rules (e.g., ensure Storage volumes are encrypted, Compute instances are properly tagged, and static IP addresses are attached to instances and continuously monitor configuration changes to the cloud resources and provides a dashboard to track compliance status. | |
| 39 | Provide Audit Trail of the account activity to enable security analysis, resource change tracking, and compliance auditing | |
| 40 | CSP should offer a fully managed service in India that makes it easy to identify potentially fraudulent online activities such as online payment fraud and the creation of fake accounts. | |

| | | |
|---|---|---|
| 41 | CSP should provide in India, a single location to track migration tasks across multiple cloud native tools and partner solutions certified on the cloud to provide visibility into migration. | |
| 42 | CSP should offer a fully managed service in India, that lets customer to easily create and publish interactive dashboards that include Insights. The dashboards should be accessible from any device and embedded into city applications, portals, and websites. | |
| 43 | Web Application Firewall (Layer 7): Protection from attacks by filtering traffic based on rules that you create. Filter web requests based on IP addresses, HTTP headers, HTTP body, or URI strings, which allows you to block common attack patterns, such as SQL injection or cross-site scripting that could affect application availability, compromise security, or consume excessive resources. Features like protection against Web Traffic visibility, east of deployment and maintenance, integrated security. | |
| 44 | DDoS Protection: Managed DDoS protection service that defends against most common, frequently occurring network and transport layer DDoS attacks that target web site or applications. When used with Content Delivery Network and global DNS service, should provide comprehensive availability protection against all known infrastructure (Layer 3, 4 and 7) attacks. Should provide always-on detection and automatic inline mitigations, minimize application downtime and latency. | |
| 45 | Identity and Access Management: Service that properly separates users by their identified roles and responsibilities, thereby establishing least privilege and ensuring that users have only the permissions necessary to perform their assigned tasks. | |
| 46 | Managed Threat Detection Service: Continuously monitor for malicious or unauthorized behavior to help you protect your accounts and workloads. It should monitor for activity such as unusual API calls or potentially unauthorized deployments that indicate a possible account compromise. | |
| 47 | The service should also detect potentially compromised instances or reconnaissance by attackers. | |
| 48 | Appropriately configure the security groups in accordance with the Clients's networking policies. | |
| 49 | Regularly review the security group configuration and instance assignment in order to maintain a secure baseline. | |
| 50 | Secure and appropriately segregate / isolate data traffic/application by functionality using DMZs, subnets etc | |

| | | |
|---|---|---|
| 51 | Ensure that the cloud infrastructure and all systems hosted on it, respectively, are properly monitored for unauthorized activity and follow the security advisories (Advisory No. 22 and any other) guidelines provided by MoHUA | |
| 52 | Properly implementing anti-malware and host-based intrusion detection systems on their instances, as well as any required network-based intrusion detection systems in accordance with the Client's Security policies. | |
| 53 | Review the audit logs to identify any unauthorized access to the Client's systems. | |
| 54 | Virtual Machines offered should be compatible with applications and meet the SLAs. | |
| 55 | Physical core to vCPU ratio should meet the SLA requirement. | |
| 56 | Ability to automatically increase/scale the number of Instances/VMs during demand spikes to maintain performance if required (i.e. 'scale-out'). | |
| 57 | Cloud service architecture should be in such a way that avoids VM outages or downtime when the provider is performing any kind of hardware or service maintenance at the host level | |
| 58 | MSP should have capability to provide dedicated hosts in its native Cloud Infrastructure in India, which allows usage of existing third-party software license | |
| 59 | CSP Should meet monthly uptime as per SLA. | |
| 60 | Cloud provider should offer the following instance types –<br>• Optimized for generic applications and provides a balance of compute, memory, and network resources.<br>• Optimized for memory intensive applications.<br>• Optimized for compute intensive applications.<br>• Graphics intensive GPU compute applications | |
| 61 | Cloud provider should offer instances that provide a baseline level of CPU performance with the ability to burst above the baseline. | |
| 62 | Cloud provider should offer instances that run on hardware dedicated to a single customer. | |
| 63 | Cloud provider should offer instances that can run nested virtual machines, that is virtual machine inside a virtual machine. | |
| 64 | Cloud provider should be able to support OS as per solution requirement. | |

| | | |
|---|---|---|
| 66 | Customer must be able to specify and modify server configuration (CPU, memory, storage) parameters seamlessly. | |
| 67 | Cloud service should support local storage for compute instances to be used for temporary storage of information that changes frequently. | |
| 68 | Cloud service must offer self-service provisioning of multiple instances concurrently either through a programmatic interface (API/CLI) or through a management console. | |
| 69 | Cloud capability: should be able to logically group instances together for applications that require low network latency and/or high network throughput. | |
| 70 | Cloud capability: should be able to split and host instances across different physical data centers to ensure that a single physical failure event does not take all instances offline. | |
| 72 | Cloud capability: should be able to import their existing image and save it as a new, privately available image that can then be used to provision instances in the future. | |
| 73 | Cloud service must support the ability to take an existing running instance or a copy of an instance and export the instance into a VMDK or VHD image format as per user requirement | |
| 75 | Cloud service must be architected in such a way to automatically restart instances on a healthy host if the original physical host fails. | |
| 76 | Cloud provider must be able to schedule events for customer's instances, such as a reboot, stop/start, or retirement. Depending on the event, customer might be able to take action to control the timing of the event. | |
| 77 | Cloud service should support containers, including Docker and/or other containerization platforms. | |
| 78 | Cloud provider should offer a highly scalable, high performance container management service. | |
| 79 | Cloud service should be able to run customer code in response to events and automatically manage the compute resources. | |
| 81 | Cloud provider should offer VMs with up to large storage (TB) size or as required. | |
| 86 | Support complete eradication of data such that it is no longer readable or accessible by unauthorized users and/or third parties. | |

| | | |
|---|---|---|
| 88 | Offer object storage tiering capability, i.e. the ability to recommend transitioning an object between object storage classes based on its frequency of access. | |
| 89 | Block Storage<br>• Cloud provider should offer persistent block level storage volumes for use with compute instances.<br>• Cloud provider should offer higher block storage volumes as required<br>• Cloud service should support solid state drive (SSD) backed storage media that offer millisecond latencies.<br>• Cloud service should support the needs of I/O-intensive workloads, particularly database workloads that are sensitive to storage performance and consistency in random access I/O throughput.<br>• Cloud service should support encryption of data on volumes, disk I/O, and snapshots using industry standard AES-256 cryptographic algorithm.<br>• Cloud service should support encryption using customer managed keys.<br>• Cloud service should support point-in-time snapshots. These snapshots should be incremental in nature.<br>• Cloud Service should support sharing of snapshots across regions making it easier to leverage multiple regions for geographical expansion, data center migration, and disaster recovery.<br>• Cloud service should support adding more than one compute instance to a single storage volume in R/W mode so that many users can access and share a common data source.<br>• Cloud service should support a baseline IOPS/GB and maintain it consistently at scale<br>• Cloud service should be durable and support annual failure rates of less than 0.01% or as required by SLA, and the information must be disclosed. | |

| | | |
|---|---|---|
| 90 | Object Storage<br>• Cloud provider should offer secure, durable, highly scalable object storage for storing and retrieving any amount of data from the web.<br>• Cloud provider should support an extremely low-cost storage for archival. The CSP should automatically tier the data.<br>• Cloud service should support encryption for data at rest using 256-bit Advanced Encryption Standard (AES-256) encryption to encrypt your data.<br>• Cloud service should support encryption using customer provided keys. These keys should be used to manage both the encryption, as data is written to disks, and decryption, when data is accessed.<br>• Cloud service should support encryption using a Key<br>• Management Service that creates encryption keys, defines the policies that control how keys can be used, and audits key usage to prove they are being used correctly.<br>• Cloud Service should support managing an object's lifecycle by using a lifecycle configuration, which defines how objects are managed during their lifetime, from creation/initial storage to deletion.<br>• Cloud service should be able to send notifications when certain events happen at the object level (addition/deletion).<br>• Cloud service should be able to host a website that uses client side technologies (such as HTML, CSS, and JavaScript) and does not require server-side technologies (such as PHP and ASP.NET).<br>• Cloud Service should support versioning, where multiple versions of an object can be kept in one location. Versioning protects against unintended overwrites and deletions.<br>• Cloud service should support flexible access-control policies to manage permissions for objects.<br>• Cloud service should be able to provide audit logs on storage location including details about a single access request, such as the requester, location name, request time, request action, response status, and error code.<br>• CSP should offer a mechanism to avoid accidental deletion of data. In such case data when deleted should be preserved for a minimum of 3 months or as required.<br>• Cloud service should support a lower cost option for noncritical, reproducible data at lower levels of redundancy.<br>• Cloud service should allow uploading a single object as a set of parts where each part is a contiguous portion of the object's data and these object parts can be uploaded | |

| | | |
|---|---|---|
| | independently and in any order. | |
| | • Cloud provider should offer service to speed up distribution of static and dynamic web content.<br>• Cloud service should support read-after-write consistency for PUT operations for new objects.<br>• Cloud provider should offer a solution for seamlessly storing on premises data to the cloud, primarily for Video Management Systems data storage in cloud for longer durations.<br>• Cloud provider should support moving large amounts of data into the cloud by bypassing the internet.<br>• Cloud provider should support replicating data to DR site and should provide read-only access to the replicated data. | |
| 91 | File Storage<br>• Cloud provider should offer a simple scalable file storage service to use with compute instances in the cloud.<br>• Cloud service should offer SSD backed storage media to provide the throughput, IOPS, and low latency needed for a broad range of workloads.<br>• Cloud service should support petabyte-scale file systems and allow thousands of concurrent NFS connections.<br>• Cloud service should support consistent low latency performance and should support scalable IOPS and throughput performance.<br>• Cloud service should support thousands of instances so that many users can access and share a common data source.<br>• Cloud service should automatically scale up or down as files are added or removed without disrupting applications.<br>• Cloud service should be highly durable - file system object (i.e. directory, file, and link) should be redundantly stored across multiple data centers.<br>• Cloud service should support read after write consistency (each read and write operation is guaranteed to return the most recent version of the data). | |

### 6.4 Intelligent Traffic Management System

Towns and cities are facing traffic-related challenges, from improving safety, to addressing mobility-related emissions and reversing levels of congestion. Congestion is one of the most prevalent transport challenges in large urban agglomerations. Pollution, including noise generated by circulation, has become an impediment to the quality of life and even the health of urban populations. Further, energy consumption by urban transportation has dramatically increased, and so the dependency on petroleum.

#### 6.4.1 Key Issues

The main challenges of Traffic Management in urban ecosystem are as follows:

- Traffic congestion and parking difficulties.
- Longer commuting
- Public transport inadequacy
- Difficulties for non-motorized transport
- Loss of public space
- High infrastructure maintenance costs
- Environmental impacts and energy consumption.
- Accidents and safety

#### 6.4.2 Indicative Key Outcomes and KPIs

**The KPI and outcomes can be achieved bringing in multiple domain data integration with ICCC along with ITMS data.**

i. Reduction in stoppage time
ii. Optimized cycle times of intersection to regulate and maintain free flow of traffic to enhance the efficiency of the road and transport infrastructure.
iii. Extent of signal synchronization
iv. Increased Travel Speed
v. Improve Traffic Services: The traffic services to the public can be improved through the user-friendly presentation of the various traffic information in real time.
vi. 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.
vii. Real Time Information and Response: The real time information at the control room shall enable the operator to take necessary actions based on the real time information, arranging alternate route to VIP convoys, diverting the traffic to different routes etc.
viii. Improved and accurate Traffic violation detection for the following traffic rules violations:
ix. Red Light Violation Detection
x. Speed Violation Detection
xi. Free Left Blocking Violation Detection
xii. No Helmet Detection
xiii. Triple Ride Detection
xiv. No Seatbelt Detection
xv. Driver Talking on Phone while Driving
xvi. Improved Traffic Related Emergency Notification and Personal Security
xvii. % emergency vehicle dispatches facilitated by ICCC or Dial 100 or Dial 108
xviii. % urban intersections providing safety enhancements for pedestrians and disabled or other vulnerable road users
xix. Traffic-related fatality per lakh population (livability index)
xx. Change in number of all reported accidents per vehicle km
xxi. Change in severity of accidents (i.e., numbers killed or serious injured) per number of accidents reported

xxii. Change in crime reports relating to illegal parking
xxiii. Improve Environmental Impacts
xxiv. Change in CO2 emissions per vehicle km
xxv. Percentage of interchanges with bicycle parking facilities
xxvi. Change in number of hours where NOx levels are above threshold
xxvii. Change in PM10 emissions per vehicle km
xxviii. Change in number of hours where transport noise is above dB threshold
xxix. Add any other innovative use cases as proposed/ modify of the above features asper requirements.

### 6.4.3 Key components

Automatic Number Plate Recognition (ANPR)

a) Red Light Violation Detection (RLVD)

b) Speed Violation Detection (SVD)

c) Vehicle Detector

d) Adaptive Traffic Control System (ATCS)

e) Traffic Analytics

f) e-Challan

g) Video Management & Operator Functions

### 6.4.4 Automatic Number Plate Recognition (ANPR)

a) The System should automatically detect a vehicle in the camera view using video detection and activate license plate recognition.

b) The System should automatically detect the license plate in the captured video feed inreal-time and the system should perform Optical Character Recognition (OCR) of the license plate characters.

c) System should be able to detect and recognize the English alpha numeric license plate in standard fonts and formats for classes of vehicles such as cars, Heavy Commercial Vehicles, Three Wheelers and Two Wheelers. The system should be innovative to detect English Alphanumeric license plate in non-standard fonts and formats too.

d) The system should capture standard vehicle's number plates with an accuracy of at least 90% at day time and at least with an accuracy of 70% at night time.

e) The System should store JPEG image of vehicle and license plate and enter the license plate number into the database along with the date, time stamp and site location details.

f) The system should detect the color of all the vehicles on best effort basis, in the cameraview during daytime and label them as per the predefined list of configured system colours. The system should store the color information of each vehicle along with thelicense plate information for each transaction in the database.

g) The system should identify the category of the vehicle such as cars, Heavy Commercial Vehicles, Three Wheelers and Two Wheelers and should store this information along with the license plate information for each transaction in the database.

h) The system should have an option to store certain license plates of vehicles which arestolen or suspicious. The system should have the functionality to enter such license plate numbers to lists such as "Wanted", "Suspicious", "Stolen" termed as hot lists of vehicles. Thesystem should allow the user to import the vehicle license plate data in the hot lists storedin Excel sheets for batch operation.

i) The system should generate an automatic alert in the ICCC, when it detects the vehicle from the hot list/s through the ANPR camera. The system should give an instant alert in suchcase. The system should also have the functionality to send the alert via email and SMS todesignated email addresses and mobile phone numbers.

j) The system should allow the operator to change the hot list category of the vehicle and accordingly the new hot list category should be reflected in the records stored in the database. E.g., on retrieval of stolen vehicle, system entry should be changed from "Stolen"to "Retrieved".

k) The system should be able to store license plates numbers of at least suspected vehicles at a time and should generate an Alert if any one of the vehicles is found crossing the stopline (irrespective whether the signal is GREEN or RED) in form of Video popup at the Monitorand/or SMS on Cell phones.

l) The system should have the functionality to trace the movement of a vehicle of interest onGIS Map. The Function should show the trajectory of the vehicle drawn on the map. The vehicle of interest should be tracked for all the junctions where it is detected through ANPR.

m) The system should give an option to the operator to edit the license plate number of the vehicle. The system should show the license plate of the vehicle in a zoomed window foreasy inspection of the license plate number. The system should keep audit trail of anylicense plate number edited by the operator.

n) The system should have function of quickly searching the number plate based on the following criteria:

   i. full or partial number of the license plate,
   ii. color of the vehicle,
   iii. classification of vehicle,

iv. junction Name,

v. Event Type (e.g., ANPR, Red light Violation, Speed Violation, etc.)

o) The ANPR system should improve the number plate detection for up to 90 percent for four-wheeler vehicles with standard and non-standard number plates during the night time (with proper illumination / provision of IR light).

p) The system should detect the vehicles with no license plate and should raise an alert along with the video and snapshots of the vehicle.

q) The system should allow the operator to set traffic rule such as "no heavy vehicles during certain time of the day" for selected traffic junctions and display in VMD. The system should identify the heavy vehicles and generate an alert in case the vehicle is violating the rule within the configured time.

### 6.4.5 Red Light Violation Detection (RLVD)

I. The system should capture the License Plate of the vehicles violating the red light or stop line when the signal is Red.

II. The system should have provisions to either detect red light status by taking the signal feedfrom the traffic signal controller or by video analytics by recording the evidence snapshowing the violating vehicle and the traffic signal status.

III. The system should have an in-built tool to facilitate the operator to compose detailed evidence by stitching video clips from any IP camera in the junction (including but not limited to the red-light violation detection camera, evidence camera), and any other surveillance cameras in the vicinity of the spot of incidence.

IV. The system should have the functionality export the violation evidence with water markand encryption as per the techno-legal requirements.

V. The system should synchronize the evidence camera, license plate recognition cameraand store the record in database with License plate image, image of the vehicle, and atleast five snaps showing clearly that the vehicle is crossing the red light / stop line while thesignal is RED. This event should be corroborated with the video clip archived in the VMSsystem at the ICCC. It should be possible to intimate the incidence in real time through SMS to the designated mobile phone.

VI. The system should allow mapping of multiple ANPR cameras to a single evidence camera associated with the traffic junction.

VII. The system should allow capturing multiple evidence snaps based on the time duration before, during and after the event.

VIII. The system should allow restricting an operator to a single or multiple traffic junction/s and associated cameras.

IX. The system should have function to forward the generated alerts to designated email and mobile phone number.

X. The System should also record the video of all the cameras/selected cameras using a predefined and user configurable schedule. The recorded video can be searched usingthe following filters:

a) Appearance of a particular license plate.

b) When the signal is RED

c) When the signal is GREEN

d) During any given date-time span

XI. The system should generate alert when the signal light doesn't change for the pre-configured duration. The system should allow the user to set minimum and maximum timefor the signal light status change.

### 6.4.6 Speed Violation Detection (SVD)

i. The system should be video based speed violation detection system to be used for speed detection.

The offered system should be able to detect vehicle license plates along with speed violation detection for vehicles having speed in excess of 5KMPH or as defined by the local authorities (with suitable camera with required frame rate) with an accuracy of at least ±2KMPH as compared to conventional speed laser gun system. The system should generate an automatic alert in case of a speed violation.

ii. The system should have the capability to classify the vehicle under categories such as car, three wheelers, two wheelers, heavy vehicle, etc.
iii. The system should allow the operator to set different speed limits for different categories of vehicles.
iv. The event window should show the video associated with the event. The window should also show at least five snapshots associated with the event.
v. The system should allow the operator to flag the event for storing the event perennially.

### 6.4.7 Traffic Analytics

i. The system should have the proven technology-based video analytics for intelligent traffic management applications such as:

a) No Helmet Detection System
b) Triple Ride and No Helmet Detection System
c) Free Left Blocking Detection
d) Object classification for detection of stray animals on the road

ii. The system should work on centralized or decentralized architecture.
iii. In case of any failure in any LPUs, the SI must ensure design and implementation for no data loss and functionalities of video analytics processing of failed LPU at ICCC.

#### 6.4.7.1 No Helmet Detection

i. System should have the capability to capture image of two-wheeler rider not wearing a helmet and should have automatic number plate recognition (ANPR) of the violating vehicle with auto-localization and OCR conversion. The system should have the capability to detect the 'no helmet' instance for the rider and pillion.
ii. The system should collectively identify and detect the motor bike, the rider and the pillion (if applicable), helmet for the rider and the pillion and the number plate. The system shouldbe able

to differentiate between a helmet and various other conditions such as the baldhead, person covering the head with a cap or dupatta or pagree, or any other headgear.

iii. The system should be able to differentiate a person sitting on a motor bike and a pedestrian in the close proximity of the motor bike.
iv. The system should be able to detect the speed of the motor bike.
v. On detection of No-Helmet, the system should generate events, store them and should allow retrieval of such events on need basis for later analysis.
vi. The system should be able to search and show the report of the No Helmet violations based on the day, time of the day, license plate number (partial or full), location nameetc.
vii. System should have capability to identify and eliminate non-standard crash helmets like industrial safety helmets, sports helmets (cricket, cycling, etc) and mark them as invalid.
viii. System should integrate with challan generation software and RTO database to generate challans for No-Helmet violation event with details like violation image, time stamp, date, vehicle number.
ix. No- Helmet detection system should seamlessly integrate with traffic management systems like ANPR, RLVD, Speed Detection and should have unified user interface.

#### 6.4.7.2 Triple Ride Detection

i. The system should have the capability to detect the persons riding triple seat on the motor bike. The system should capture the number plate of the motor bike with ANPR and generate an alert with the evidence video.
ii. The system should be able to detect the No Helmet violation for persons riding in triple ride.

#### 6.4.7.3 Free Left Blocking Violation Detection

i. The system should detect the vehicle blocking the free left traffic wherever it is allowed.
ii. The system should capture the number plate of the vehicle blocking the free left traffic from the front side.
iii. The system should generate an automatic alert with the details of the vehicle blocking the traffic.

**Object classification for detection of stray animals on the road**

i. The system should detect the animal blocking the traffic.
ii. The system should generate an automatic alert with the details (image, location etc..) of the animal blocking the traffic.

#### 6.4.8 Adaptive Traffic Control System (ATCS)

- The ATCS should address typical Indian driving and traffic conditions such as poor lane discipline and high heterogeneity. The traffic signal controller should be ready for integrating with Vehicle priority system (Red light enforcement system, and other similar applications). The software and hardware supplied should comply with applicable standards for interoperability and data sharing between different applications.
- Objective of the ATCS would be 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 shall operate in real time with the capacity to calculate the optimal cycle times, effective green time ratios, and change intervals for all system traffic signal controllers connected to it.
- Identify the critical junction of a corridor or a region based on maximum traffic demand and saturation.
- The critical junction cycle time 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. Offset deviation measured using distance and speed between successive intersections shall be corrected within 5 cycles at a tolerance of +/- 5 seconds 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 suggest the priority route to the higher demand direction.

- Develop appropriate stage timing plans for each approach of every intersection under the ATCS, based on real time demand
- Propose timing plans to every intersection under the ATCS in every Cycle
- Verify the effectiveness of the proposed timing plans in every cycle
- Identify Priority routes
- 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
- Graphically present signal plan execution and traffic flow at the intersection on desktop
- Graphically present time-space diagram for selected corridors on desktop
- Graphically present network status on Desktop
- Make available the network status and report viewing on Web
- The ATCS shall generate standard and custom reports for planning and analysis. Report formats to be finalized during design stage.
- Shall provide a decision support tool for assessing strategies to minimize congestion, delays and emergency response time to events with real time traffic data fusion and control of traffic signaling infrastructure on ground.
- Shall calculate customizable Key Performance Indicators (KPI) to quickly assess the results
- Shall generate alerts to the operator that trigger on customizable conditions in the network
- Shall 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 create a traffic data warehouse for all historic traffic information gathered from the hardware installed on the road network.
- Shall operate in real time that is continuously updating the estimates on the state of the network 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
- Enable a smart public transport priority respecting the delays for all road users at once with the adaptive signal controller
- Junctions with similar traffic patterns can be grouped flexibly into sections or sub- areas. The system shall allow group of compatible junctions to be linked and operated in a coordinated manner to optimize traffic operations in a real time basis. It shall be possible for the operator to lock junctions, sub-areas together causing them to operate on a common cycle length if desired
- Pedestrian zone scheme: The system shall allow individual signal groups to be switched on or off according to time of the day as required to facilitate for special pedestrian zone operation. Should be capable of pre-programmed in site configuration data being activated or de-activated by time scheduling. Should be capable of being activated by central system or at controller connected to the system
- Traffic adaptive control: The system shall be capable of utilizing inputs from the detectors to dynamically implement the most suitable cycle time, splits and offset to optimize traffic operations on the junction network on a real-time basis. The system shall be equipped with flexibility to handle partial or total failure of detectors in an appropriate and logical

manner.

- A controller drop procedure shall be provided to safely transfer a controller from the central computer-controlled state to local control. The drop procedure shall allow for the drop of controller either in the total network, a section or an individual controller, as desired by the operator, both manually and through the activity scheduler. The drop could be planned or emergency situation.
- Traffic adaptive system should have green wave route pre-emption capability.. Route pre-emption can be applied to a single junction or a series of junctions to allow emergency (fire/ambulance/VVIP) vehicles. The software shall be capable to simultaneous operation of two or more route pre-emption plans
- Communications Monitoring – The System shall monitor the status of the communication continuously and shall provide for the "recording" of all pertinent data for any specified controller into a disk file. The recorded data shall include the current time, second by second current operating information (e.g., timing plan data, etc.), and the current communications messages being transmitted and received between the control computer and the field control equipment. Once there is any lack of communication from any one of the local controllers, an alarm shall be raised to indicate that the controller is off-line or there is a communication alarm. An appropriate message shall be recorded in the System alarm and event log and fault databases
- System shall deliverable measurable performance for the important use-case for Adaptive traffic control system for the benefit of the end user.
- The system should be able to handle emergency priority routing on a consistent basis.
- Adaptive Traffic Control System shall offer traffic signal optimizing functionalities, use data from vehicle detectors and optimize traffic signal settings resulting improved vehicle delays and stops. The system shall also allow interconnecting individual area controllers and thus enabling traffic monitoring and regulating functionality from the central location. This shall allow each intersection controller to be monitored from central control for proper functionality. Any corrective action can be initiated either automatically based on status information or by an operator. The real time detection data shall be communicated to the ICCC by each controller.
- ATCS shall be driven central control system, on real time basis, with the capacity to calculate the optimal cycle times, effective green time ratios, and change intervals for all system traffic signal controllers connected to it which in turn can also work in configurable manner
- The system after update, creating or expanding database, including the addition of new junctions or deleting of existing junction should not require system reboot

### **6.4.9** Reports

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.

- 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.
- 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 switchinghas taken place. The report shall show the cycle sequence and cycle timings for the cyclein a day.
- Mode switching report – The report shall give details of the mode switching taken placeon a day.
- Event Report - The report shall show events generated by the controller with date and time of event.
- 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 remotely through a PC or Server.
- Time Update – The report shall show the time when the Master controller updated its time either manually or through remote server.
- Mode Change – The report shall show the time when Master controller's operating modeis changed either manually 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.
- Corridor Performance Report – The report shall show the saturation of all the intersectionsin 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 corridorfor every cycle for a day

#### 6.4.10 Graphical User Interface

The application software shall have the following Graphical User Interface (GUI) for user friendliness

- Network Status Display – This online display shall indicate with appropriate color codingon site map whether an intersection under the ATCS is online or off. On double clickingthe 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 elapsedfor the stage in seconds on X-axis.
- Junction names shall be identified with each plot.
- 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.
- The system shall have other graphical interfaces for configuring the ATCS, as appropriate.

#### 6.4.11 Video Management & Operator Functions

- The system should have built-in Video Management features for continuous recording of the traffic cameras. The system should have the following functionality:
- Continuous recording of every lane video irrespective of presence of vehicle.
- Such recording schedules can be continuous, event based, schedule based, trigger based etc.
- Archive Search using dates, time, event etc.

a) High Availability/Redundancy of Recording & Database

- The system should have operator clients for all ITMS related functions including video management functions and configuration of the system.
- The system should allow the operator to create continuous recording schedule for the camera based on the time of day and day of week. It should be possible to set the camera recording schedule for a single camera or a group of cameras or all cameras.
- The system should have the functionality to restrict the user to login from a specific workstation.
- The system should be able to show Live video in multiple matrix layout for all the cameras in the system in real time. At least 1x1, 2x2, 3x3, 1+5, 1+7 views must be supported. The system should have the function to enable multiple matrix layouts to appear on the screen with configurable on-screen duration for each matrix layout.
- The system should allow configuring cameras in multiple groups independently. It should be possible to assign all, single or multiple groups to operators. At least 100 such groups should be possible with unlimited number of cameras in each group. It should be possible to assign camera/s to single or multiple groups simultaneously.
- It should be possible to drag and drop cameras from the camera directory to the display screen.
- The system should allow creation of customised, layered maps using standard picture files and it should be possible to drag and drop the cameras on the map for easy navigation based on the location on the map. It should be possible to select any camera or group of cameras on the map for live viewing or archive viewing.
- The system should allow creation of events for any camerafrom the drop-down menu or any other easy to use interface. Such an event, when stored, should be searchable based on the camera, time, and event type. It should be possible to write description about the event.

- The system should show event notification from the cameras on the map itself. The operator should be able to click on the event notification of a particular camera on the map and the system should open the event window on the operator screen.
- The system should integrate with existing city GIS, online maps such as Google Maps, OpenStreetMap etc.. as required by the local authorities
- The system should generate an alert when the total available storage drops below the configured threshold limit.
- The operator console should show icons for the quick understanding of the system health status related to camera status, junction server status, database server connection status and storage status. The respective icons should change the color when any of the system component has problems. The health status should have the following information in drill down report format:
- System map showing all junction servers in the system. Clicking a junction server entry should lead to details of the junction server such as camera status, real time utilization of server resources such as cores, RAM and storage. Drilling further down, camera details should be available such as camera name, IP address, major and minor stream, real time bitrate and frames configured for analytics.

- Storage Status showing central storage and all the network drives and utilization of the storage
- All the users logged into the system with the time since login. It should be possible to force log-out the user, send a message to the user and mirroring the desktop of the user from the same screen.

  a) Recording server status showing status of the live recording of the cameras in the central server, list of junctions which are sending live feed, total events generated at each junction and events pending to synchronized.

- The system should have a dashboard which should show the following information:

  a) Status of analytics, events and clips generated at junction servers

- Camera-wise status showing processed and dropped frames

  a) Event clip generation time, status of transfer of clips from junction server to central aggregation server

- The operator console should show vital system parameters for components such as Database Server, Media Servers, Local Workstation and Storage System (all available storages). The client should show the parameters such as CPU Core Usage, RAM Utilization and Storage Utilization.
- The system should have reports such as camera uptime availability, camera recording percentage, recording status, critical events, incident video, etc.
- The system should provide facility to search for the cases of violations occurred during any specific span of time, and provide a statistical analysis of the number of such incidences occurring during various days of the month, various months of the year in graphical format.A report of all such incidences should be automatically generated by the system in a spreadsheet (.xls format),and can be automatically emailed to the designated email addresses.

- The system should allow the users to download multiple segments of the video, which are encrypted with password from single or multiple cameras from the archive with an option to tag each downloaded segment with text messages. The Video segments should be downloaded in a single folder along with excel spreadsheet where details of each of the video segments are listed as hyperlinks to the exported video.
- The system should allow the operator to configure email account and SMS gateway for sharing various alerts through email and SMS.
- The system should maintain log of various system generated alerts. The system should also maintain full audit trail in the logs.
- The system should be integrated with ICCC platform to show alerts and any other details required.

**Data Security**

- The system should have the capability to transfer the data to ICCC through proper encryption in real time. The application for traffic violation detection system should adhere to National Cyber Security Policy to ensure that the critical information processed and stored by the application is secure from cyber-attacks / hacking / hijacking.
- Integration with CCTNS & Transport Dept Systems: Bidders need to ensure that there is seamless integration between various Government databases and security of citizens & their assets is carried in a holistic manner. Please note that some of the integration would need to be through web services while in some cases it may be required to maintain local databases.

**ICT Solution:**

With a view to address the above issues it is now proposed to implement the following modules under Intelligent Traffic Management System

1. Entry Exit Point Management
2. Corridor Management
3. Red Light Violation Detection
4. Speed Violation Detection
5. Adaptive Traffic Controller System
6. Automatic E Challan System

Following are ICT solutions.

1. Entry Exit Point Management with video based automatic traffic count & classification along with ANPR for all major Entry Exit points to have precise information about vehicle entering, exiting, monitoring and control of traffic in primary city corridor for Traffic Information, management & Control.
2. ATCS system with edge based processing using Local processing units(LPU)
3. Variable Messaging Display integrated with video based speed detection to display the speed information for awareness of drivers
4. Traffic Enforcement System:
   The ITMS shall provide various traffic violation detection use cases using Artificial Intelligence and Deep Learning based technology. It shall provide insights for the traffic planners using innovative dashboards for various parameters such as violations, traffic count, vehicle classification, present and historical trends, comparison of roads or junctions. The ITMS shall serve as a decision support system and provide actionable intelligence to help make the city roads safer and less congested for both motorists and pedestrians.
   The ITMS shall have the components such as Junction Servers (available at a traffic junction or available centrally), Event Aggregation Servers, Management Server and a Database. Each component shall provide failover redundancy. There shall be no dependency on thespecific operating system, database software, virtualization platform, storage technology and compute infrastructure.
   The ITMS platform architecture shall allow flexible and modular deployment of software components in a distributed computing architecture. At the same time, it shall allow fully centralized deployment of the software application. The distributed architecture shall support a Junction Server installation in any COTS hardware server suitable for operation as per the respective temperature and environmental conditions at the traffic junction for local processing of the connected video surveillance cameras. The Junction Server should send the traffic events and the metadata to the Events Aggregation servers. The Events Aggregation Server shall manage and aggregate the alerts generated from the Junction Servers spread across various locations. Under the centralized deployment the video feeds shall be processed on the servers at the data center. The platform shall be robust to support on-premise or on-cloud infrastructure.
   It shall be possible to connect the Junction Servers using wireless connectivity such as 3G / 4G or 5G if required, without any dependency on the static public IP addresses. The Junction Servers shall store the violation records and the junction camera video streams locally for the configurable duration.

   The ITMS shall offer business continuity in case of disasters. DC-DR architecture shall

support granular control on the data safe-keeping and business continuity with automated two-way synchronization of events, violation records, images, and video clips. It shall be possible to configure business continuity, data safe -keeping , store archived informationon DR .

The ITMS shall have support for Block and Object Storage on cloud platforms. The system shall support pushing the recorded video file on a definable schedule to the Object Storage.

The ITMS shall be built considering the information security risks. It shall have multiple levels of authentication and access control mechanisms such as

A. Role based Authentication
B. Session control using encrypted tokens
C. Restricted user to a particular hardware workstation
D. Multi Factor Authentication with provision to receive the OTP via text message on the registered mobile of the user and through the registered email address and

F. Single sign-on based on LDAP and Active Directory. It shall allow restricting an operator to a single or multiple traffic junction/s and associated cameras.

ITMS must provide necessary software required to meet the security requirements stated above.

All the communication among the servers and clients shall be secured and the ITMS shall support the SSL and TLS communication. It shall have option of encryption with AES 128/ 256 and RSA 1024/2048 encryption standards. It shall support secure communication between the camera and the server using SRTP and RTSP protocols. The ITMS shall have been tested for vulnerabilities and shall have been penetration tested as per the OWASP guidelines. Certificates from the CERT-In empaneled auditor from the respective country of origin clearly indicating the encryption and Vulnerability Assessment and Penetration Testing (VAPT) test shall be available.

To facilitate communication and information collaboration among the operators from various traffic zones, the ITMS shall provide the built-in chat function to exchange the text, image, video clips or any other file from the workstation to other fellow operators or supervisors, thus creating an ad-hoc collaborative environment for incident investigation.

The ITMS shall provide all the use cases and functionalities mentioned in the specifications in a unified platform. The ITMS shall provide the multicasting functionality for monitoring live and archived videos from the unified client. It shall provide an integrated management functionality for camera, recording, traffic violation and incident use cases management and user management for ease of operation.

The ITMS shall be a futuristic solution and shall offer flexibility in distributing the compute at various stages within the architecture to optimize the compute requirements.

**System Management Functions**

ITMS should have robust system management functions. The ITMS shall provide centralized management of the Junction Servers, aggregation, and processing servers through a unified client interface. The ITMS shall be based on the latest Artificial Intelligence and Deep Learning technologies for continuous improvement of accuracy in generating data by means of analyzing video frames.

At minimum, ITMS shall have:

- User friendly, centralized software update mechanism on Junction Servers based on the schedule.
- Framework to deploy trained model files to all the Junction Servers at a single go.

- Provision to check the performance of various stages in Analytics application deployment pipeline
- Camera-wise status showing processed and dropped frames.
- Total number of events generated in the Junction Servers, total events, event clips and images transferred to the control room servers and events in the queue that are yet to be transferred.
- Dashboard to display storage availability and in the Junction Servers including camera and Junction Servers uptime or SLA reports
- Provision to prioritize the transfer of data from the Junction Server to the central servers. Event Metadata and event images shall be prioritized over the video clips and also prioritize the latest events over the old events.
- Health-dashboard to display CPU and memory utilization status of Junction Server and servers

The ITMS unified client shall show system health alerts for camera, junction server, database server and storage. The drill-down system health shall cover area, junction, to further details of system utilization, major and minor stream, real time bitrate and frames configured for analytics, camera details such as Camera Name, IP Address, Recording Server status showing status of the live recording of the cameras in the central server, list of junctions which are sending live feed etc.
The storage status shall show central storage and all the network drives and utilization of the storage and alert when the total available ITMS storage drops below the configured threshold limit.
The ITMS shall maintain log of various system generated alerts. The system shall also maintain full audit trail in the logs.

**Video Handling and General Functions**

The Junction Servers shall record the camera streams locally (continuous, event based, schedule based, trigger based) for the duration as per the requirement. The ITMS shall synchronize the recorded video streams from the Junction Servers to the Control Room storage devices. The system shall synchronize such videos in the background depending on the event transfer priority. For example, during the night when there are fewer events generated in the system, the Junction Server shall transfer the recorded video to the Control Room ITMS servers. It shall be possible for the operators to replay the recorded videos stored in Junction Servers on-demand.

The below functionalities should be achieved by ITMS or VMS or integration of both as required.

1. ITMS shall allow recording a matrix of cameras from the operator workstation in a single file to create investigative report as a single video file in case of an event or an accident.

It shall be possible to share such a file to the fellow operators or supervisors using a built-in chat function. It shall be possible to search the archive video using date, time, type of event, etc. It shall be possible to view live/archive videos in multiple matrix layout for all the cameras in the system in real time. At least 1x1, 2x2, 3x3, 1+5, 1+7. It shall be possible to cycle multiple layouts with configurable time. A drag and drop functionality shall be supported for viewing cameras on the screen.

2. ITMS shall allow creation of customized, layered maps using standard picture files or GIS maps and it shall be possible to drag and drop the cameras on the map for easy navigation based on the location on the map. It shall be possible to select any camera or group of cameras on the map for live viewing or archive viewing.

3. ITMS shall allow creation of manual events by the operators. from any live camera view using a drop-down menu of various anomalies. Such an event, when stored, shall be searchable based on the camera, time, and event type. It shall be possible to write description about the events.

4. The system shall allow the users to download multiple segments of the video, which are encrypted with password from single or multiple cameras from the archive with an option to tag each downloaded segment with text messages. The Video segments shall be downloaded in a single folder along with excel spreadsheet where details of each of the video segments are listed as hyperlinks to the exported video files.

The system shall provide facility to search for the cases of violations occurred during any specific span of time and provide a statistical analysis of the number of such incidences occurring during various days of the month, various months of the year in graphical format. A report of all such incidences shall be automatically generated by the system in a spreadsheet (.xls, .csv format) and can be automatically emailed to the designated email addresses.

The system shall allow the operator to configure email account and SMS gateway for sharing various alerts through email and SMS.

**Data Analytics and Decision Support Functions**

The ITMS shall support to implement a data driven ITMS and not a mere transaction based system. ITMS shall be useful to all the stakeholders such as Crime investigation department, Traffic Police and City Planners. The ITMS shall provide various ways to collect and synthesize the data. At minimum it shall be possible to:

- Analyze the frequency of the events and generate notifications on the configurable deviation from the median.
- It shall assist in finding the anomaly than mere violation alerts.
- It shall help extract various attributes for the actors operational on the road forassisting in traffic planning and investigation.
- Show graphical representation of the data generated from the system such astraffic violations by A. type, B. vehicle classes, C. Junction D. Time frame E. TrafficDistrict, F. Traffic Flow, G. Average Speed, H. Headway, I. Private, Commercial,Auto, Electric Vehicles, J. License Plate Quality and classification such as HSRP,Non-HSRP, Dilapidated, No License

Plates, etc. It shall allow comparison for a group of junctions (up to three) on these parameters.

- Provide impact analysis of the traffic planning decisions taken such as making a road one-way, blocking turns in a junction, restricting certain classes of vehicles during certain times of the day, restricting lanes for certain classes of vehicles, etc. It shall be possible via a video analysis, synopsis and simulation tool to analyze the before and after effect of the traffic planning decisions. It shall allow entering information for such decisions and monitor the same on the graph. It shall have ready to use filters – last 1 day, 7 days, 15, days, month, year, etc.
- Plot average count of vehicles or violations on the GIS map. The system shall show traffic violations hotspot on the GIS.
- Provide customized dashboards for various stakeholders with configurable information such as a developing congestion, dropping headway, dropping average speed, increasing violations, etc.
- The system shall make use of the data being generated through the ITMS system for the benefit of the authority as a decision support system. ITMS shall generate an alert on the following conditions:
- When the average speed of any junction drops by the configured threshold (e.g., 20%) as compared to the regular average of last one or two weeks.
- When an average volume of vehicles of any category increases suddenly by the configured threshold (e.g., 20%) as compared to the regular average of last one or two weeks.
- When an overall volume of vehicles increases suddenly by the configured threshold (e.g., 20%) as compared to the regular average of last one or two weeks.
- Detect commercial vehicles having age more than the configured age in years (e.g., 15 years).

**Integration Functions**

ITMS should have published APIs to interface with external systems such as Integrated Command and Control Application,

The ITMS should have a proven track record in automatically validating the traffic violations based on the ANPR conversion confidence level.

The system should have the capability to integrate with the VAHAN / SARATHI system to fetch vehicle related details as required and as made available by the VAHAN / SARATHI system. It should allow automated and on-demand modes for verification.

The system should provide a query service to the other districts / states to query a particular vehicle if it was seen in the city OR a provision to issue a lookout notice to police which can be fed in the database and any detection of the lookout vehicle should generate an alert.
The system should have integration with the WhatsApp messaging service to share information on the selected groups. The operator should be able to share alert/violation/footage related to an event or a vehicle.

The system should be able to integrate with external systems such as integrated command and control system, C4i systems, IP Speakers, etc.

### 6.4.12 Entry Exit Point Management:

The City of Puducherry has 4 entry exits and it is proposed to install the Entry & Exit point Management system in the following indicative locations to monitor the Public transportation schedules and Bus timing thru ANPR along with City Entry/Exit.

| | |
|---|---|
| 1 # | ECR Entry |
| 2 | Near Accord Pondy |
| 3 | Indira Gandhi Junction |
| 4 | Cuddalur Exit |

The functional/ Technical requirement of the proposed system for entry exit point shall be as follows:

#### 6.4.12.1 ANPR for Entry Exit:

The system shall capture the license plates of the vehicles while capturing the vehicle categories such as cars, Heavy Commercial Vehicles, Three Wheelers, Two Wheelers andBuses and shall store this information along with the license plate information for eachtransaction in the database. The system shall provide 95% and better detection accuracyand 90% and better license plate conversion accuracy into a text string for Four wheelersand above vehicles for standard reflective license plates.

The system shall categorize the license plates into Good (readable), Bad/dilapidated (partial or fully non-readable), Broken, License Plates without numbers. System shall also provide the license plate conversion confidence percentage. Dashboard with various filters shall also be available with the application. The system shall have the dashboard to viewcaptured vehicles with categories such as private, commercial, electric, and other specialvehicles such as military (subject to the availability of training datasets for the special categories) at day time without connecting other systems, e.g vehicles registry database.

The ITMS shall provide the ability to capture vehicles with no number plate, hand-written / fancy number plates, number plates with regional languages.

The system shall have Vehicle Counting and Classification functions using the ANPR and overview cameras.

The system shall detect the colour of all the vehicles on best effort basis, in the camera view during daytime and label them as per the predefined list of configured system colours. The system shall store the colour information of each vehicle along with the license plate information for each transaction in the database.

The system shall store certain license plates of vehicles which are stolen or suspicious with a facility to edit the lists as required including bulk importing functionality. The system shall generate an automatic alert in the control room when it detects the vehicle from the hot list/s through the ANPR camera. It shall be possible to get a trajectory of such/any selected vehicle

on a GIS map on demand.

The operator shall be able to edit the license plate number of the vehicle in case it is wrongly captured. The system shall show the captured vehicles with selectable, ANPR conversion confidence. The system shall keep full audit trail of the user actions.

The system shall have function of quickly searching the number plate based on criteria such as full or partial number of the license plate, colour of the vehicle, Speed of the vehicle, Classification of vehicle, Junction Name, etc.

The system shall allow the operator to set traffic rule such as "no heavy vehicles during certain time of the day" for selected traffic junctions/cameras and display in VMD. The system shall identify the heavy vehicles and generate an alert in case the vehicle is violating the rule within the configured time.

The system shall self-analyse the confidence level of the ANPR conversion. In case the confidence level is above user-configured threshold, the violation shall be pushed automatically for traffic ticket generation.

The system shall be flexible to capture the license plates and the traffic violations (subject to the required field of view) from front-side or back-side using a single camera for each lanes at least.

#### 6.4.12.2 Specification for ANPR Camera /Overview Camera/ Evidence Camera

| Sl. No | Minimum Specification | | Compliance (Yes / No) |
|---|---|---|---|
| | **Make:** | | |
| | **Model:** | | |
| 1 | Image Sensor | 1/2.8" 2MP Progressive Scan CMOS or better | |
| 2 | Day/Night Operation | Yes with IR Cut Filter | |
| 3 | Minimum Illumination | Color: 0.03 lux or better ; B/W 0 Lux with IR | |
| 4 | Lens | 5.5-62 mm (+/- 1mm) Motorized Varifocal Lens or better | |
| 5 | Electronic Shutter | 1/5 to 1/50,000s or better | |
| 6 | Image Resolution | 1920x1080 or better | |
| 7 | Compression | H.265 or better | |
| 8 | Frame Rate and Bit Rate | Up to 60 fps with Controllable bit rate, frame rate and Maximum Bit rate | |

| Sl. No | Minimum Specification | | Compliance (Yes / No) |
|---|---|---|---|
| 9 | Video Streams | Minimum 3 Nos, individually configurable simultaneous streams in H.265 @ 1920x1080 & 60 Fps | |
| 10 | Angular Field of View | H: 54.58°(Wide)~5.30°(Tele) / V: 32.19°(Wide)~3.00°(Tele) / D: 61.4(Wide)~6.06(Tele) | |
| 11 | Motion Detection | Built in 8 point polygonal zones areas in the video stream. | |
| 12 | Lens/Barrel Distortion Correction & Corridor View | Built in feature required | |
| 13 | Wide Dynamic Range | 150 dB or better | |
| 14 | IR | 100 Meter (Built in or External) IR. | |
| 15 | Alarm | 1 Input & 1 Output | |
| 16 | Audio In | Selectable (Mic in/Line in), Supply voltage: 2.5VDC(4mA), Input impedance: 2K Ohm | |
| 17 | Audio Out | Line out, Max. output level: 1Vrms | |
| 18 | Audio Compression | G.711 u-law /G.726 Selectable G.726(ADPCM) 8KHz, G.711 8KHz G.726 : 16Kbps, 24Kbps, 32Kbps, 40Kbps AAC-LC : 48Kbps at 16KH | |
| 19 | Analytics | Defocus detection, Directional detection, Fog detection, Face detection, Motion detection, Digital auto tracking, Appear/Disappear, Enter/Exit, Loitering, Tampering, Virtual line, Audio detection, Sound classification. Can be achieved via VMS and VA | |
| 20 | Event Triggers | Alarm input, Motion detection, Analytics, Network disconnect and others | |
| 21 | Event Actions | FTP, HTTP, Email notification, Edge Storage, Alarm Output | |
| 22 | Edge Storage | Micro SD/SDHC/SDXC 1 no. slot of 512GB capacity or better with min.512GB Memory card | |

| Sl. No | Minimum Specification | | Compliance (Yes / No) |
|---|---|---|---|
| 23 | Protocols | IPv4, IPv6, TCP/IP, UDP/IP, RTP(UDP), RTP(TCP), RTCP,RTSP, NTP, HTTP, HTTPS, SSL/TLS, DHCP, FTP, SMTP, ICMP, IGMP, SNMPv1/v2c/v3(MIB), ARP, DNS, DDNS, QoS, PIM-SM, UPnP, Bonjour , LLDP(optional), SRTP | |
| 24 | Security | HTTPS(SSL) Login Authentication, Digest Login Authentication, IP Address Filtering, User access Log<br>802.1X Authentication (EAP-TLS, EAP-LEAP) | |
| 25 | Firmware Upgrade | The firmware upgrade shall be done though web interface, The firmware shall be available free of cost | |
| 26 | Interface | RJ 45, 100 Base TX or better | |
| 27 | Memory | 1024 MB RAM, 256 MB Flash or better | |
| 28 | Enclosure | IK10 &IP67 or Nema4x or better | |
| 29 | Power requirements | Vendor to specify, POE Preferred | |
| 30 | Operating Temperature | 0 °C to 55°C or better | |
| 31 | Operating Humidity | 90% RH or better | |
| 32 | Certification | UL, CE, FCC, BIS, | |
| 33 | Application Programmers Interface | 1. The interface shall be available for integration with 3rd party analytics and applications in public domain<br>2. ONVIF | |
| 34 | **Deleted** | | |
| 35 | Mount | Wall Mount/ Pole Mount | |
| 36 | Warranty | Min. 5 Years | |
| 37 | Privacy Masks | Minimum 4 | |

**6.4.13** Corridor Management**:**

- With a view to ensure that the traffic in the major trunk roads are monitored and proper details are being disseminated to the commuters. It is proposed to install corridor

management systems in three corridors. These Corridors will also have Traffic enforcement systems like Instant Speed, Average Speed, Wrong direction, sudden lane changing. Prime corridor as mentioned above will have evidence cameras video-based analytics to provide traffic data and will also provide possibility to view video from these monitoringstations to verify any unusual incident from ICCC. The precise information from solution will provide volume, classification, average speed of traffic, any unusual incident on the corridor which can impact traffic flow conditions. The system should have Vehicle Counting and Classification functions using the ANPR and evidence cameras.

The details of the said corridor are as follows:


| Sl. No | Name | From | To |
|---|---|---|---|
| 1 | Main Corridor | ECR Entry | Cuddalur Exit |
| 2 | Corridor 1 | Indira Gandhi Junction | Beach Start |
| 3 | Corridor 2 | Adigal Salai Junction | PWD Office Junction |

The functional/Technical requirement of the said system shall be as follows:

### 6.4.14 Variable Message Display

- The Variable Message Display(VMD) will be able to play Text Image and Full Color Video and approximately 3.8 meterX1.9 meter. Hardware should have minimum 5 year warranty
- The (VMD) should have : pixel density 2500Pixels/sq.m , RGB Resolution 16pixelsX 8 pixels , brightness >12300 cd/sq.m., color amount 16million., Contrast 3000:1,
- The (VMD) should have best view distance of 20 to 100 meter with optimum viewing Horizontal>30, Vertical>
- The (VMD) shall be of IP 67
- The cabinet material should be steel and should double side back door
- The (VMD) system should be supplied with all required controllers and should have integrated base with traffic and other information portal from smart city control roomICCC and Central Control Software shall allow controlling multiple (VMD) from one console. Capable of programming to display all types of Message/ advertisement having alphanumeric character in English, - and combination of text with pictograms signs. The system should have feature to manage video / still content for VMS display.
- The system should have capability to divide VMS screen into multi-parts to display diverse form of information like video, text, still images, advertisements, weather info, city info etc. The system should also provide airtime management and billing system for paid content management. 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 (VMD). 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 ICCC via communication network.
- Real time log facility – log file documenting the actual sequence of display to be available at central control system.
- Multilevel event log with time & date stamp.
- Access to system only after the authentication and acceptance of authentication based on hardware dongle or similar with its log.
- Location of each (VMD) will be plotted on GIS Map with their functioning status which can be automatically updated.
- Report generation facility for individual/group/all (VMD) 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.
- Configurable scheduler on date/day of week basis for transmitting pre-programmed message to any (VMD) unit.

- Various users should access the system using single sign or similar 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
- Mounting : Should be mounted with standard poles , erecting structures and road clearance.

### 6.4.15 Specification for Speed Violation Camera:

| # | Parameter | Minimum Specifications or better | Compliance ( Yes or No) |
|---|---|---|---|
| | **Make:** | | |
| | **Model:** | | |
| 1 | Image Sensor | 1/2.8" 2MP Progressive Scan CMOS or better | |
| 2 | Day/ Night Operation | Yes with IR Cut Filter | |
| 3 | Minimum Illumination | Color: 0.03 lux or better ; B/W 0 Lux with IR | |
| 4 | Lens | 5.5-62 mm (+/- 1mm) Motorized Varifocal Lens or better | |
| 5 | Electronic Shutter | 1/10 to 1/12,000s or better | |
| 6 | Image Resolution | 1920x1080 or better | |
| 7 | Compression | H.265 or better | |
| 8 | Frame Rate and Bit Rate | Upto 60 fps with Controllable bit rate, frame rate and Maximum Bit rate | |
| 9 | Video Streams | Minimum 3 Nos, individually configurable simultaneous streams in H.265 @ 1920x1080 & 60 Fps | |
| 10 | Angular Field of View | H:54.58°(Wide)~5.30°(Tele)/V: 32.19°(Wide)~3.00°(Tele)/D: 61.4(Wide)~6.06(Tele) | |
| 11 | Motion Detection | Built in 8 point polygonal zones areas in the video stream. | |
| 12 | Lens/ Barrel Distortion Correction & Corridor View | Built in feature required | |
| 13 | Wide Dynamic Range | 150 dB or better | |
| 14 | IR | 100 Meter (Built in or External) IR | |
| 15 | Alarm | 1 Input & 1 Ouput | |
| 16 | Audio In | Selectable(Mic in/Line in), Supply voltage: 2.5VDC(4mA), Input impedance: 2K Ohm | |
| 17 | Audio Out | Line out, Max. output level: 1Vrms | |

| | | | |
|---|---|---|---|
| 18 | Audio Compression | G.711 u-law /G.726 Selectable G.726(ADPCM) 8KHz, G.711 8KHz G.726 : 16Kbps, 24Kbps, 32Kbps, 40Kbps AAC-LC : 48Kbps at 16KH | |
| 19 | Analytics | Defocus detection, Directional detection, Fog detection, Face detection, Motion | |
| | | detection, Digital auto tracking, Appear/Disappear, Enter/Exit, Loitering, Tampering, Virtual line, Audio detection, Sound classification and others. Can be achieved via VMS and VA | |
| 20 | Event Triggers | Alarm input, Motion detection, Analytics, Network disconnect and others | |
| 21 | Event Actions | FTP, HTTP, Email notification, Edge Storage, Alarm Output | |
| 22 | Edge Storage | Micro SD/SDHC/SDXC 1 no. slot of 512GB capacity each or better with min.512GB Memory card | |
| 23 | Protocols | IPv4, IPv6, TCP/IP, UDP/IP, RTP(UDP), RTP(TCP), RTCP,RTSP, NTP, HTTP, HTTPS, SSL/TLS, DHCP, FTP, SMTP, ICMP, IGMP, SNMPv1/v2c/v3(MIB-2), ARP, DNS, DDNS, QoS, PIM-SM, UPnP, Bonjour , LLDP, SRTP | |
| 24 | Security | HTTPS(SSL) Login Authentication, Digest Login Authentication, IP Address Filtering, User access Log 802.1X Authentication (EAP-TLS, EAP-LEAP) | |
| 25 | Firmware Upgrade | The firmware upgrade shall be done though web interface, The firmware shall be available free of cost | |
| 26 | Interface | RJ 45, 100 Base TX or better | |
| 27 | Memory | 1024 MB RAM, 256 MB Flash or better | |
| 28 | Enclosure | IK10 & IP67 or Nema4x or better | |
| 29 | Power requirements | Vendor to specify, POE Preferred | |
| 30 | Operating Temperature | 0 °C to 55 °C or better | |
| 31 | Operating Humidity | 90% RH or better | |
| 32 | Certification | UL, CE, FCC, BIS, | |

| | | | |
|---|---|---|---|
| 33 | Application Programmers Interface | 1. The interface shall be available for integration with 3rd party analytics and applications in public domain<br>2. Onvif | |
| 34 | **Deleted** | | |
| 35 | Mount | Wall Mount/ Pole Mount | |
| 36 | Warranty | Min. 5 Years | |
| 37 | Speed detection system to capture speed | Upto 200 Kmph +/- 2% | |
| 38 | Speed Enforcement Technology | Radar/Laser/Other better technologies | |

#### 6.4.16 Instant Speed Violation Detection:

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

- Install the Speed Violation Detection Systems across the city. This system shall capture the infractions of speed violations at these locations. The proposed Instant Speed system should have proper test certification in compliance with standards for speed enforcement systems.
- Design, supply, and install the speed violation detection system as per requirement. This includes supply all the necessary equipment for the camera and detection system, including but not limited to sensors, computers, ancillary camera equipment, camera housings, camera poles, warning signs and shall make the final connections to the camera.
- The solution proposed shall seamlessly integrate with the E-Challan system proposed under the scope of this project.
- Providing all the necessary IT infrastructure for analysis, storage & retrieval of the infraction information at ICCC or any other location as per the requirement.

The functional requirement of the said system shall be as follows:

**Functional Specification for Instant Speed System:**

| S/N | Functional Requirement | Compliance ( Yes / No) |
|---|---|---|

| | | |
|---|---|---|
| | **Make:** | |
| | **Model:** | |
| 1 | The proposed solution should have video based speed violation detection feature with a facility to set different speed limits for different categories of | |
| | vehicles and schedule. The feature should have the functionality to prove the vehicle speed using a simple on-screen tool. | |
| 2 | The speed detection use case (along with license plate recognition) should be capable to read speeds in excess of 100- 200 km/hr. A certificate from an institute of repute, which can issue such a certificate in India should be provided to substantiate the claim. | |
| 3 | The speed detection software system shall be certified by any accredited laboratory for speeds from 40 KMPH to 200 KMPH with variation of less than 2% at various speed thresholds such as 40 KMPH, 70 KMPH, 100 KMPH, 130KMPH, 170 KMPH and 200 KMPH speeds. | |
| 4 | Software should also provide Average Speed detection functionality for a control section / corridor within the city. All vehicles passing through the control section at a Speed greater than a determined speed limit shall be detected as violation. It should be possible to create multiple points within a long corridor for determining the average speed. | |

### 6.4.17 Average Speed Violation Detection:

Software should also provide Average Speed detection functionality for a control section / corridor within the city. All vehicles passing through the control section at a Speed greater than a determined speed limit shall be detected as violation. It should be possible to create multiple points within a long corridor for determining the average speed.

### 6.4.18 Wrong Side Driving Violation

| # | Minimum Requirements | Compliance ( Yes / No) |
|---|---|---|
| **A.** | **General** | |
| 1. | Wrong Side Detection of Vehicle Movement –The system should be installed at critical junctions or streets as identified by the department to capture the wrong direction vehicle movement. | |
| 2. | The system should identify and capture multiple violating vehicles and the E-Challan standard procedure should be triggered. | |

### 6.4.19 Adaptive Traffic Control System

It is proposed to implement Adaptive Traffic Controller at identified junctions. The proposed system shall have a fully adaptive traffic controller with the following functionalities:

**Traffic Signal Controller**

| # | Description | Compliance ( Yes / No) |
|---|---|---|
| | **Make:** | |
| | **Model:** | |
| 1 | The Traffic Signal Controller equipment is a 32 bit or 64-bit microcontroller with a 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 monitoring facility to ensure that conflicting, dangerous are pre-flagged at the programming stage and these are disallowed even during the manual override phase. Should have 5 year warranty | |
| 2 | The Traffic Signal Controller can be controlled through the central traffic control center as an individual junction or as part of the 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 a central command controller easily | |
| 3 | Site-specific configuration data shall be stored in a non-volatile memory device (FLASH memory) easily programmable at the site through a 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. | |
| 4 | 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. | |
| 5 | The controller shall provide a real-time clock (RTC) with battery backup that sets and update the time, date, and day of the week from the GPS. The RTC shall have a minimum of 10 years battery backup with maximum time tolerance of +/- 2 sec per day. | |
| 6 | The controller shall have the facility to update the RTC time from the ATCS server, GPS, and through manual entry. | |
| 7 | The traffic signal system including the controller shall have provision for audio output tones and should be disabled-friendly. | |
| 8 | 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. | |

**Police Panel**

| # | Description | Compliance (Yes / No) |
|---|---|---|
| | **Make:** | |
| | **Model:** | |
| 1 | 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 theright of way to emergency vehicles. It should be possible to configure the Hurry Call switches to any stage as per site requirements. | |
| 2 | One Forced Flash Switch: Activation of this switch should force the signal to Flashing Amber / Flashing Red. | |
| 3 | One Auto / Manual Switch: Activation of this switch should enable the manual operation of the controller. Deactivation of the manual switch shall continue from the current stage without interruption. | |
| 4 | 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. | |
| 5 | 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. | |

**Modes of Operation**

| # | Description | Compliance (Yes / No) |
|---|---|---|
| 1 | 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 at any stage. Cycle time remains constant in every cycle execution for a given time period. | |
| 2 | 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 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. | |

| | | |
|---|---|---|
| 3 | 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. | |
| 4 | 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 the clearance amber time of the previous stage. | |
| 5 | Transit Signal Priority (TSP) for buses: The traffic signal controller shall provide transit signal priority for buses in the dedicated lane to ensure minimum stop delay at the intersection, without violating safety clearances. | |
| 6 | 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 for all demand actuated stages except for the Priority Stage shall be possible. | |

| | | |
|---|---|---|
| | 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 period. In such an event the signal plan timings shall be executed from the local timetable stored in the traffic signal controller FLASH memory. The fallback mode of the traffic signal controller shall be vehicle actuated. On the restoration of the communication with the central computer, the traffic signal controller shall automatically resort to FATCS mode.<br>The traffic signal controller shall accept commands for remote selection / de-selection of the following from the Central Computer at ICCC.<br>· Hurry Call<br>· Flashing Amber / Flashing Red<br>· Junction Off<br>If not reverted to the normal operation within the period listed below, the traffic signal controllers shall timeout the commands and operate normally<br>· Hurry Call – 5 Minutes<br>· Flashing Amber / Flashing Red – 30 Minutes<br>· Junction Off – 30 Minutes<br>The traffic signal controller shall report the following to the Central Computer through the communication network every cycle or on an event as appropriate.<br>· Green time exercised for each approach (stage pre-emption timing) against the Green running period set for the approach by the Central Computer<br>· Mode of Operation<br>· Lamp failure, if any<br>· Output short circuit, if any<br>· Detector failure, if any | |

**Traffic Signal Controller Operating Parameters**

| # | Description | Compliance (Yes / No) |
|---|---|---|
| 1 | It shall be possible to operate the filtered green (turning right signal) along with a vehicular phase. The filter green signal shall flash for some time | |

| | | |
|---|---|---|
| | equal to the clearance amber period at timeout when operated with a vehicular phase. | |
| 2 | The pedestrian phase signal shall be configured for flashing red or flashing green aspects during pedestrian clearance. | |
| 3 | It shall be possible to configure any phase to the given lamp numbers at the site. | |
| 4 | Stages – The controller shall have the facility to configure at least 32 Stages | |
| 5 | Cycle Plans – The controller shall have the 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 the fixed mode of operation. | |
| 6 | Day Plans – The controller shall have the facility to configure each day of the week with different day plans. It shall also be possible to set any of the day's plans to any day of the week. The controller shall have the capability to configure 20-day plans or as per requirement. | |
| 7 | Special Day Plans – The controller shall have the facility to configure a minimum of 20 days as special days in a calendar year or as per requirement. | |
| 8 | Starting Amber – During power up the controller shall initially execute the Flashing Amber / Flashing Red plan for some time of 3 Seconds to 10 Seconds. The default value of this Starting Amber is 5 Seconds. The facility shall be available to configure the period of Starting Amber within the given limits at the site. | |
| 9 | 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 periods from 3 Seconds to 10 Seconds. | |
| 10 | 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 starts commencing execution. | |
| 11 | All Red – Immediately after the Starting Amber all the approaches should be given the 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. | |
| 12 | Signal lamps monitoring – The controller shall have inbuilt circuitry to monitor the lamp status | |

| | | |
|---|---|---|
| 13 | 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 a short circuit in the output) shall force the signal into Flashing Amber / Flashing Red. | |
| 14 | Cableless 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 a communication network. GPS enabled RTC shall be the reference for the cable less synchronization. | |
| 15 | Fixed Time mode with fixed offsets | |
| 16 | Vehicle Actuated mode with fixed offsets | |

**Input and Output facilities**

| # | Description | Compliance (Yes / No) |
|---|---|---|
| 1 | Lamp Switching: The controller shall have a minimum of 48 (Scalable to 64) individual output for signal lamp switching. The signal lamps shall be operating on appropriate DC/AC voltage of applicable rating | |
| 2 | 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 the vehicle For future scalability to ATCS | |
| 3 | Communication Interface: The traffic signal controller shall support an Ethernet interface to communicate with the ATCS server | |
| 4 | Power Saving: The traffic signal controller shall have a facility to regulate the intensity of signal lamps during different ambient light conditions thereby saving energy. | |
| 5 | Real-time Clock (RTC): The GPS receiver for updating time, date, and day of the week information of the traffic signal controller should be an integral part of the traffic signal controller. | |
| 6 | The traffic signal controller shall update the date, time, any day of the week automatically from GPS during power ON and at scheduled intervals. | |
| 7 | Manual entry for the date, time, any day of the week shall be provisioned for setting the traffic signal controller RTC (Real Time Clock). | |
| 8 | It shall be possible to set the RTC from the Central Server when networked | |

| | | |
|---|---|---|
| 9 | 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 | |
| 10 | Operator Display (optional): The traffic signal controller shall have a LED-backlit Liquid Crystal Display (LCD) as the operator interface. | |

**Countdown Timer**

Countdown Timer shall be installed at each traffic junction under this Project

| # | Description | Compliance (Yes / No) |
|---|---|---|
| | **Make:** | |
| | **Model:** | |
| 1 | Count Down Timer to be configured in Vehicular Mode. Hardware should have 5 year warranty | |
| 2 | The Vehicular countdown timer should be dual-color,<br>· Red for Stop or STP<br>· Green color for Go | |
| 3 | There should be alternate Red and Balance phase time for STOP or STP<br>in Flashing | |
| 4 | Alternate Green and Balance Phase Time for Go in Flashing | |

**Communication Network**

| # | Description | Compliance (Yes / No) |
|---|---|---|
| 1 | Function of the Communication network is for remote monitoring of 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 ICCC and also individual junctions can be controlled and actuated from central ICCC(Hurry Calls, Forced Flash , Junction Switch off, Plan download and upload etc.). | |

**ATCS Software Application :**

The Adaptive Traffic Control Software application software shall do the following:

| # | Description | Compliance (Yes / No) |
|---|---|---|
| 1 | Identify the critical junction(s) of a corridor or a region based on maximum traffic demand and saturation. | |
| 2 | The critical junction cycle time shall be used as the group cycle time i.e. cycle time common to all intersections in that corridor or region. | |
| 3 | Stage optimization to the best level of service shall be carried out based on the traffic demand. | |
| 4 | 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. | |
| 5 | Offset correction shall be carried out to minimize the number of stops and delays along the corridor for the priority route. Offset deviation measured using distance and speed between successiveintersections shall be corrected within 5 cycles at a tolerance of +/- 5seconds maximum. | |
| 6 | The system shall have provision to configure the 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. | |
| 7 | Develop appropriate stage timing plans for each approach of every intersection under the ATCS, based on real-time demand | |
| 8 | Propose timing plans to every intersection under the ATCS in every Cycle | |
| 9 | Verify the effectiveness of the proposed timing plans in every cycle | |
| 10 | Identify Priority routes | |
| 11 | Synchronize traffic in the Priority routes | |
| 12 | Manage and maintain communication with traffic signal controllers under ATCS | |
| 13 | Maintain database for time plan execution and system performance | |
| 14 | Maintain error logs and system logs | |
| 15 | Generate Reports on request | |
| 16 | Graphically present signal plan execution and traffic flow at the intersection on desktop | |
| 17 | Graphically present time-space diagram for selected corridors on desktop | |
| 18 | Graphically present network status on desktop | |
| 19 | Make available the network status and report viewing on Web | |

| | | |
|---|---|---|
| 20 | The ATCS shall generate standard and custom reports for planning and analysis | |
| 21 | It 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 | |
| 22 | Shall have the ability to predict, forecast, and smartly manage the traffic pattern across the signals over the next few minutes, hours, or 3-5 days and just in the current real-time. | |
| 23 | Shall provide a decision support tool for assessing strategies to minimize congestion, delays, and emergency response time to events via simulation and planning tools like real-time traffic data fusion and control of traffic signaling infrastructure on the ground. | |
| 24 | Shall collect continuous information about current observed traffic conditions from a variety of data sources and of different kinds (traffic states, signal states, vehicle trajectories, incidents, road works etc) | |
| 25 | Shall infer a coherent and comprehensive observed traffic state (speeds, vehicular densities, and presence of queues) on all network elements, from the above-mentioned observations, including vehicle trajectories, through several map matching, data validation, harmonization, and fusion processes | |
| 26 | Shall extend the measurements made on only several elements both on the rest of the unmonitored network, and over time, thus obtaining an estimation of the traffic state of the complete network and the evolution of this traffic state in the future | |
| 27 | Shall forecast the traffic state concerning 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 | |
| 28 | Shall calculate customizable Key Performance Indicators (KPI) to quickly assess the results | |
| 29 | Shall provide calculated traffic flows estimation and forecast, queues and<br>delays to Urban Control and Adaptive Signal Control Systems, allowing for proactive Traffic Management and Control | |
| 30 | Shall generate alerts to the operator that trigger on customizable conditions in the network (starting with simple drops inflow, up to total queue lengths along emission sensitive roads surpassing a definable threshold) | |
| 31 | Shall 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" | |

| | | |
|---|---|---|
| 32 | Shall create a traffic data warehouse for all historic traffic information gathered from the hardware installed on the road network. | |
| 33 | Shall operate in real-time that is continuously updating the estimates on the state of the network and the travel times based on data collected continuously over time. | |
| 34 | 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 | |
| 35 | Enable a smart public transport priority respecting the delays for all road users at once with the adaptive signal controller | |

**Reports**

Reports System shall generate corridor based and junction/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.

| # | **Description** | **Compliance (Yes / No)** |
|---|---|---|
| 1 | Junction/Intersection based reports | |
| 2 | Stage Timing report – The report shall give details of the 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). | |
| 3 | Cycle Timing report – The report shall give details of the 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. | |
| 4 | Stage switching report – The report shall give details of the time at which a stage switching has taken place. The report shall show the stage sequence, stage timings, and stage saturation for a day. | |
| 5 | Cycle Time switching report – The report shall give details of the 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. | |
| 6 | Mode switching report – The report shall give details of the mode switching that takes place on a day. | |
| 7 | Event Report - The report shall show events generated by the controller with the date and time of the event. | |
| 8 | Power on & down: The report shall show the time when the master is switched on, and the last working time of the master controller. | |

| | | |
|---|---|---|
| 9 | Intensity Change – The report shall show the brightness of the signal lamp is changed according to the light intensity either manually through the keypad or automatically by LDR with a time stamp. | |
| 10 | Plan Change – The report shall show the time of change of plan either through the keypad or remotely through a PC or Server. | |
| 11 | RTC Failure – The report shall show the time when the RTC battery level goes below the threshold value. | |
| 12 | Time Update – The report shall show the time when the Master controller updated its time either manually through the keypad, automatically by GPS, or through the remote server. | |
| 13 | Mode Change – The report shall show the time when the Master controller's operating mode is changed either manually through the keypad or a remote server. The typical modes are FIXED, FULL VA SPLIT, FULL VA CYCLE, FLASH, LAMP OFF and HURRY CALL. | |
| 14 | Lamp Status Report – The report shall show lamp failure report with date and time of failure, the color of the lamp, and associated phase | |
| 15 | Loop Failure Report – The report shall show the date and time of detector failure with detector number and associated phase. | |
| 16 | Conflict – The report shall show the conflict between lamps (RED, AMBER, GREEN) in the same phase or conflict between lamps with another phase. | |
| 17 | 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 | |
| 18 | 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 | |

**Graphical User Interface**

The application software shall have following Graphic User Interface (GUI) for user friendliness

| # | Description | Compliance (Yes / No) |
|---|---|---|
| 1 | User login – Operator authentication shall be verified at this screen with login name and password | |
| 2 | Network Status Display – This online display shall indicate with appropriate color coding on the 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. | |

| | | |
|---|---|---|
| 3 | 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. | |
| 4 | Saturation Snapshot – This display shall show the current saturation levels of all intersections in a corridor. | |
| 5 | Reports Printing / Viewing – This link shall allow selection, viewing, and printing of different reports available under ATCS | |
| 6 | Time-Space Diagram – The time-space diagram shall display the current stages being executed at every intersection in a corridor with immediate previous history. | |
| 7 | Junctions shall be plotted proportionally to their distance on Y-axis and time elapsed for the stage in seconds on X-axis. | |
| 8 | Junction names shall be identified with each plot. | |
| 9 | The facility shall be available to plot the time-space diagram from history. | |
| 10 | Currently running stage and completed stages shall be identified with different colors. | |
| 11 | Stages identified for synchronization shall be shown in a different color. | |
| 12 | Speed lines shall be plotter for stages identified for synchronization to the nearest intersection in both directions. | |
| 13 | It should be possible to freeze and resume online plotting of the Time-Space diagram. | |
| 14 | The system shall have other graphical interfaces for configuring the ATCS, as appropriate. | |

Other features of the components in ATCS:

The proposed traffic controller shall be disabled friendly and shall also provide audio tones output. The supplied ATCS controller would have all the functional capability as mentioned above and also the future scalability to work an any of adaptive traffic algorithms available

- The system shall be able to detect the presence of vehicles near stop-line and do advance detection for vehicles such as Traffic volume, count
- The system shall be capable of
- Counting the vehicle with at least 80% accuracy
- Classification of the vehicle with at least 3 classes

**Red Light Violation Detection:**

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

1. The RLVD Systems at traffic junctions across the city. This system shall capture the

infractions of Red light and stop line violations at these junctions.

2. The RLVD system as defined of, all wiring connections to the traffic signal controllers and to the camera platforms. Supply all of the necessary equipment for the camera and detection system, including but not limited to: computers, ancillary camera equipment, camera housings, camera poles, warning signs and shall make the final connections to the camera. In some of the accident-prone junctions client might decide to put over speed detection system and thus Shall consider these accident prone junctions.
3. The solution proposed shall seamlessly integrate with the E-Challan system proposed under the scope of this project. The Authority shall facilitate to get access to the Vaahan and Sarathi database, to access the same through use of appropriate APIs.
4. Providing all the necessary IT infrastructure for analysis, storage & retrieval of the infraction information at ICCC or any other location as per requirement

**Functional Specification for RLVD Application:**

| S/N | Functional Requirement | Compliance (Yes / No) |
|---|---|---|
| 1 | Proposed software should capture the License Plate of the vehicles violating the red light or stop line when the signal is Red. It should be possible to detect the signal color through image analysis or through controller integration. The system should generate 3-5 violation images of the vehicle as required. | |
| 2 | Proposed software should have an in-built tool to compose detailed evidence by stitching video clips from any IP camera in the junction including surveillance cameras in the vicinity. The system should have the functionality to export the violation evidence with water mark and encryption as per the techno-legal requirements. | |
| 3 | Proposed software should flag the RLVD event in the recorded video within the system. It should allow mapping of multiple ANPR cameras to a single evidence camera associated with the traffic junction. | |
| 4 | It should be possible to view the video from an ANPR camera and the evidence camera side-by-side for any selected violation. | |
| 5 | To assess the traffic pattern, proposed software should have the report of number of vehicles crossed during any signal state such as Green Light / Orange Light, etc. The report should be available for each arm and each signal. It should be possible to analyse the report for traffic planning. | |
| 6 | The system should generate alert when the signal light doesn't change for the pre-configured duration. The system should allow the user to set minimum and maximum time for the signal light status change. | |

**Red Light Violation Detection System**

| # | Description | Compliance (Yes / No) |
|---|---|---|
| **1** | **General** | |
| a. | The following Traffic violations to be automatically detected by the system by using appropriate non-Intrusive sensors technology: The system should have both provisions to detect red light status by taking the signal feed from the traffic signal controller as well as by video analytics method using another camera (Evidence Camera) focused at the red light. The Evidence camera should also be used for evidence snap generation. | |
| | a) Red Light Violation<br>b) Stop Line Violation | |
| b. | 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:<br>a) Type of Violation<br>b) Date, time, Site Name, and Location of the Infraction | |
| | c) Registration Number of the vehicle through ANPR Camera system for each vehicle identified for the infraction. | |
| c. | 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 the nature of violation and proof there of: -<br><br>When it violates the stop line.<br>When it violates the red signal.<br>Besides, a closer view indicating readable registration number plate patch of the violating vehicle for court evidence for each violation.<br>The system must have the in-built tool to facilitate the user to compose detailed evidence by stitching video clips from any IP camera in the junction (including but not limited to the red-light violation detection camera, evidence camera), and any other surveillance cameras in the vicinity of the spot of incidence. The entire evidence should be watermarked and encrypted to stand in the court of law. | |

| | | |
|---|---|---|
| d. | The system shall be able to detect all vehicles infracting simultaneously in each lane/ arm at the junction as per locations provided. It should also be able to detect the vehicles infracting serially one after another in the same lane. The vehicles should be identifiable and demarcated in the image produced by the camera system. | |
| e. | The Evidence image produced by the system should be wide enough to give the exact position of the infracting vehicles concerning the stop line and indicate the color of the Traffic light at the instant of Infraction even if any other means are being used to report the color of the light. | |
| f. | The system should interface with the traffic controller to validate the color of the traffic signal reported at the time of Infraction to give correct inputs of the signal cycle. | |
| g. | 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 ICCC. The network should have the capability to provide the real- time feed of the evidence camera to the ICCC at the best resolution possible on the available network. | |
| h. | 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. | |
| **2** | **Recording & display information archive medium** | |
| a. | The recording and display of information should be detailed on the snapshot of the infracting vehicle as follows: | |
| b. | Computer-generated unique ID of each violation | |
| c. | Date (DD/MM/YYYY) | |
| d. | Time (HH:MM: SS) | |
| e. | Equipment ID | |
| f. | Location ID | |
| g. | Carriageway or direction of violating vehicle | |
| h. | Type of Violation (Signal/Stop Line) | |
| i. | Lane Number of violating vehicle | |
| j. | Time into Red/Green/Amber | |
| k. | Registration Number of violating vehicle | |

| | | |
|---|---|---|
| **3** | **On site-out station processing unit communication & Electrical Interface** | |
| a. | The system should automatically reset in the event of a program hanging up and restarting on a button press. However, the system should start automatically after power failure. | |
| b. | The system should have a secure access mechanism for the validation of authorized personnel. | |
| c. | Deletion or addition and transfer of data should only be permitted to authorized users. | |
| d. | A log of all user activities should be maintained in the system. | |
| e. | Roles and Rights of users should be defined in the system as per the requirements of the client | |
| f. | All formats of the stored data concerning the infractions should be Non-Proprietary. | |
| g. | 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. | |
| h. | The system should have the capability to transfer the data to ICCC 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. | |
| i. | If the connectivity to the ICCC is not established dueto network/connectivity failures, then all data about the infraction shall be stored on-site and will be transferred once the connectivity is re- established automatically. There shall also be a facility for the physical transfer of data on the portable device whenever required. There should be a provision to store a minimum of **one week** of data at each site on a 24x7 basis. | |
| **4** | **Mounting structure** | |
| a. | Should be cantilever mounted and shall have a minimum of 6 mtrs height with appropriate vertical clearance under the system from the Road surface to ensure no obstruction to vehicular traffic. | |
| b. | It should be capable to withstand high wind speeds and for structural safety, the successful bidder has to provide a structural safety certificate from qualified structural engineers approved/ certified by Govt. Agency. | |

| | | |
|---|---|---|
| c. | It shall be painted with one coat of primer and two coats of PU paint.<br>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. | |
| d. | Rugged locking mechanism should be provided for the onsite enclosures and cabinets. | |
| **5** | **RLVD Application** | |
| a. | It should be capable of importing violation data for storage in the database server which should also be available to the Operator for viewing and retrieving the violation images and data for further processing. The program should allow for viewing, sorting, transfer & printing of violation data. | |
| b. | It should generate the photograph of violations captured by the outstation system which 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 or its weblink on notices for court evidence. | |
| c. | All outstation units should be configurable using the software at the Central Location. | |
| d. | Violation retrieval could be sorted by date, time, location, and vehicle registration number and the data structure should be compatible with the Police database structure. It should also be possible to carry out recursive search and wild card search. | |
| e. | 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 a traffic signal, connectivity failure, Camera tampering, sensor tampering). | |
| f. | The automatic number plate recognition Software will be part of the supplied system, Success rate of ANPR will be taken as 95% or better during the daytime and 90% or better during the nighttime with a standard number plate. | |
| g. | 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. | |

| | | |
|---|---|---|
| h. | Image zoom function for number plates and images should be provided.<br>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. | |
| i. | Various users should be able to access the system using a 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. | |
| j. | Apart from role-based access, the system should also be able to define access based on location. | |
| k. | Rights to different modules / Sub-Modules / Functionalities should be role-based and proper log reports should be maintained by the system for such access. | |
| l. | 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, the 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 the minimum outage. | |
| m. | The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, etc. Provisions for the security of field equipment as well as protection of the software system from hackers and other threats shall be a part of the proposed system. Using Firewalls and Intrusion detection systems such as attacks and theft shall be controlled and well supported (and implemented) with the security policy. The virus and worms' attacks shall be well defended with Gateway level Anti-virus system, along with workstation level Anti-virus mechanism. There shall also be an endeavor to make use of the SSL/VPN technologies to have secured communication between Applications and their end-users. Furthermore, all the system logs shall be properly stored & archived for future analysis and forensics whenever desired. | |
| n. | The evidence of Infraction should be encrypted and protected so that any tampering can be detected. | |
| o. | 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. | System shall use open standards and protocols to the extent possible and declare the proprietary software wherever used. | |

| | | |
|---|---|---|
| q. | The user interface should be user-friendly and provide facilities to the user for viewing, sorting, and printing violations. The software should also be capable of generating query-based statistical reports on the violation data. | |
| r. | The data provided for authentication of violations should be in an easy-to-use format as per the requirements of the user. | |
| s. | Users should be provided with means of listing the invalid violations along with the reason(s) of invalidation without deleting the record(s). | |
| t. | Basic image manipulation tools (zoom etc.) should be provided for the displayed image but the actual recorded image should never change. | |
| u. | Log of user actions is maintained in read-only mode. The user should be provided with the password and ID to access the system along with user type (admin, user). | |
| v. | 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 behavior is recorded including (Red Light violation and Stop Line Violation) | |
| w. | Number plate should be readable automatically by the software/interface. There should be a user interface for simultaneous manual authentication/correction and saving as well. | |
| x. | Interface for taking prints of the violations (including image and above details). | |

**RLVD Camera Technical Specification:**

| # | Parameter | Minimum Specifications or better | Compliance (Yes / No) |
|---|---|---|---|
| | **Make:** | | |
| | **Model:** | | |
| 1 | Image Sensor | 1/2.8" 2MP Progressive Scan CMOS or better | |
| 2 | Day/ Night Operation | Yes with IR Cut Filter | |

| | | | |
|---|---|---|---|
| 3 | Minimum Illumination | Color: 0.03 lux or better ; B/W 0 Lux with IR | |
| 4 | Lens | 5.5-62 mm (+/- 1mm) Motorized Varifocal Lens or better | |
| 5 | Electronic Shutter | 1/5 to 1/50,000s or better | |
| 6 | Image Resolution | 1920x1080 or better | |
| 7 | Compression | H.265 or better | |
| 8 | Frame Rate and Bit Rate | Up to 60 fps with Controllable bit rate, frame rate and Maximum Bit rate | |
| 9 | Video Streams | Minimum 3 Nos, individually configurable simultaneous streams in H.265 @ 1920x1080 & 60 Fps | |
| 10 | Angular Field of View | H: 54.58°(Wide)~5.30°(Tele) / V: 32.19°(Wide)~3.00°(Tele) / D: 61.4(Wide)~6.06(Tele) | |
| 11 | Motion Detection | Built in 8 point polygonal zones areas in the video stream. | |
| 12 | Lens/ Barrel Distortion Correction & Corridor View | Built in feature required | |
| 13 | Wide Dynamic Range | 150 dB or better | |
| 14 | IR | 100 Meter (Built in or External) IR. | |
| 15 | Alarm | 1 Input & 1 Output | |
| 16 | Audio In | Selectable (Mic in/Line in), Supply voltage: 2.5VDC(4mA), Input impedance: 2K Ohm | |
| 17 | Audio Out | Line out, Max. output level: 1Vrms | |
| 18 | Audio Compression | G.711 u-law /G.726 Selectable<br>G.726(ADPCM) 8KHz, G.711 8KHz<br>G.726 : 16Kbps, 24Kbps, 32Kbps, 40Kbps<br>AAC-LC : 48Kbps at 16KH | |

| | | | |
|---|---|---|---|
| 19 | Analytics | Defocus detection, Directional detection, Fog detection, Face detection, Motion detection, Digital auto tracking, Appear/Disappear, Enter/Exit, Loitering, Tampering, Virtual line, Audio detection, Sound classification. Can be achieved via VMS and VA | |
| 20 | Event Triggers | Alarm input, Motion detection, Analytics, Network disconnect and others | |
| 21 | Event Actions | FTP, HTTP, Email notification, Edge Storage, Alarm Output | |
| 22 | Edge Storage | Micro SD/SDHC/SDXC 1 no. slot of 512GB capacity or better with min.512GB Memory card | |
| 23 | Protocols | IPv4, IPv6, TCP/IP, UDP/IP, RTP(UDP), RTP(TCP), RTCP,RTSP, NTP, HTTP, HTTPS, SSL/TLS, DHCP, FTP, SMTP, ICMP, IGMP, SNMPv1/v2c/v3(MIB-2), ARP, DNS, DDNS, QoS, PIM-SM, UPnP, Bonjour , LLDP, SRTP | |
| 24 | Security | HTTPS(SSL) Login Authentication, Digest Login Authentication, IP Address Filtering, User access Log 802.1X Authentication (EAP-TLS, EAP-LEAP) | |
| 25 | Firmware Upgrade | The firmware upgrade shall be done though web interface, The firmware shall be available free of cost | |
| 26 | Interface | RJ 45, 100 Base TX or better | |
| 27 | Memory | 1024 MB RAM, 256 MB Flash or better | |
| 28 | Enclosure | IK10 & IP67 or Nema4x or better | |
| 29 | Power requirements | Vendor to specify, POE Preferred | |
| 30 | Operating Temperature | 0 °C to 55°C or better | |
| 31 | Operating Humidity | 90% RH or better | |
| 32 | Certification | UL, CE, FCC, BIS, | |
| 33 | Application Programmers Interface | 1. The interface shall be available for integration with 3rd party analytics and applications in public domain<br>2. ONVIF | |
| 34 | Deleted | | |
| 35 | Mount | Wall Mount/ Pole Mount | |
| 36 | Warranty | Min. 5 Years | |

| | | | |
|---|---|---|---|
| 37 | Privacy Masks | Minimum 4 | |
| 38 | Red Light Detection | System shall be Non-Intrusive. It shall not be connected with traffic light and red light status is detected without any physical connection to traffic light. | |
| 39 | Fair System | Red light system shall be completely fair system with all evidences captured before and after the red light jumping infraction has happened. | |
| 40 | Lane Coverage | Each camera shall cover atleast one lane having width of 3.5m | |
| 41 | E-Challan | Integration with E-Challan system | |

**Countdown Timer**

| # | Parameters | Minimum Specifications or better | Compliance (Yes / No) |
|---|---|---|---|
| | **Make:** | | |
| | **Model:** | | |
| 1 | CPU | MicroController | |
| 2 | **Mechanical Specifications** | | |
| A | Structural Material | Polycarbonate strengthened against UV rays | |
| B | Body Color | Light Grey/Black | |
| C | Dimensions | 360mm x 370mm x 220mm or similar | |
| 3 | **Display Specification** | | |
| A | Lamp Diameter | 300mm | |
| B | Digit Height | 150 -165mm | |
| C | Display Type | Dual Coloured (Red & Green) | |
| D | No. of Digit | 3 | |
| 4 | **LED Specifications** | | |
| A | LED Diameter | 5mm LED | |
| B | Viewing Angle | 30° | |
| C | LED Wave Length | 630-640nm (Red), 505nm - 520nm (Blue- Green) | |

| | | | |
|---|---|---|---|
| D | LED Dice Material | AlInGap (Red), InGaN (Blue-Green) | |
| E | LED Warranty period | 5 years | |
| 5 | **Technical Features** | | |
| A | Power Consumption | 20 - 30 Watt Per Lamp | |
| B | Input Power | 85-260V AC, 50Hz | |
| C | Operating Temperature | -20 to + 60 °C | |
| D | Humidity | 0% to 95% Relative Humidity | |
| E | Water & Dust Ingress | IP 67 | |
| F | Standard | EN12966 Compliant | |

**Pedestrian Lamp Heads: Signal Controller Specification:**

| # | Component | Compliance (Yes / No) |
|---|---|---|
| | **Make:** | |
| | **Model:** | |
| | Key Features | |
| 1 | This pedestrian signal controller should be a 32-bit microcontroller-based unit or better. | |
| 2 | Should have GPS-based Real-Time Clock (RTC) with battery backup. | |
| 3 | Should have a minimum of 16 independent lamp outputs. | |
| 4 | Keyboard and LCD for easy junction programming | |
| 5 | Should have loop-based or Camera based detection module. | |
| 6 | Should be able to operate on 12/24 VDC and 230 VAC. | |
| 7 | Should have Ethernet- communication to have remote administration and monitoring from the central computer | |
| 8 | Should have a minimum of 16 programmable phases and stages | |

| | | |
|---|---|---|
| 9 | Should have the programmable facility for Hurry calls, week plans, holiday/special day plans | |
| 10 | Should be enclosed in IP65/67-grade box and should withstand temperatures up to 60C. | |
| 11 | Should have relevant certification like ERTL/STQC/CE/FCC etc. should have minimum 5 year warranty | |

**SIGNAL LIGHTS**

**A. Traffic lights (RED, AMBER, and Green)**

| # | Component | Compliance (Yes / No) |
|---|---|---|
| | **Make:** | |
| | **Model:** | |
| | Single Source LED type | |
| 1 | LED retrofits should comply with the EN12368 standards or other international standards | |
| 2 | The LED signal heads are to be compliant with Class A (-15 to + 60) for use in a class A environment, | |
| 3 | Should have the luminosity of intensity of 400cd | |
| 4 | Should have a medium intensity distribution, a luminous uniformity of 1:10 | |
| 5 | It should be phantom class 5 | |
| 6 | Should be impact resistance to 0.51kg dropped from a height of 1.3 meters. | |
| 7 | The minimum working life of LEDs should be at least 18,000 hours | |
| 8 | Should withstand temperatures ranging from 0 Degree Celsius to 70 Degree Celsius | |
| 9 | LED retrofits used to be of low power consumption-based | |
| 10 | Size 300 mm dia. Should have minimum 5 year warranty | |

**Pedestrian Graphical Count down timer**

| # | Component | Compliance (Yes / No) |
|---|---|---|
| | **Make:** | |
| | **Model:** | |
| 1 | 8-bit microcontroller based or better | |
| 2 | Housing should be made of polycarbonate and should be IP65/67 | |
| 3 | Dimensions 360 mmx 370mm x 220mm or similar | |
| 4 | | |

| | | |
|---|---|---|
| 5 | LED lifetime should be 1,00,000 Hrs. from the date of commissioning | |
| 6 | Full graphic and dual-color display | |
| 7 | The Vehicular countdown timer should be dual-color, Red for STOP or STP, and Green color for GO. | |
| 8 | These should have alternate Red and Balance Phase Time for STOP or | |
| 9 | STP in flashing. Alternate Green and Balance Phase Time for GO in flashing | |
| 10 | The Pedestrian Countdown timer should be the dual color with REDMAN & balance phase time in flashing and GREEN MAN & balance phase time in flashing. Should have minimum 5 year warranty | |

**Housing for Lights**

| # | Component | Compliance (Yes / No) |
|---|---|---|
| 1 | This is also called traffic signal aspects and should have the following features | |
| 2 | The color of the signal body and visors shall be black UV stabilized high impact or impact<br>a. Modified Polypropylene. | |
| 3 | It should be made of polycarbonate and should have adequate mechanical strength and durability to withstand the conditions of installation, operation, and maintenance. | |
| 4 | It shall be capable of withstanding winds of up to 145 km/h. | |
| 5 | It shall be made in such a way that it could be retrofitted with a 300 mm LED light in it. | |

| **Poles for Traffic Signals** | | | |
|---|---|---|---|
| **#** | **Component** | **Minimum Specification** | **Compliance (Yes / No)** |
| 1 | Material | GI Class 'B' pipe | |
| 2 | Paint | Hot Dip Galvanized after Fabrication with Silver coating of 86 micron as per IS:2629;Fabrication in accordance withIS-2713 (1980) | |
| 3 | Height | 5-10 Meters, as-per-requirements for different types of cameras & Siteconditions | |

| | | | |
|---|---|---|---|
| 4 | Pole Diameter | Min. 10 cm diameter pole (bidder to choose larger diameter for higher height) | |
| 5 | Cantilevers | Based on the location requirementsuitable size cantilevers to be considered with the pole | |
| 6 | Bottom baseplate | Minimum base plate of size 30x30x1.5cm | |
| 7 | Mounting facilities | To mount CCTV cameras, Switch, etc. | |
| 8 | Pipes, Tubes | All wiring must be hidden, through tubes/pipes. No wires shall be visiblefrom outside. | |
| 9 | 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 climaticconditions). Expected foundation depth of min.100cms. Please refer to earthing standardsmentioned in the RFP | |
| 10 | Protection | Lightning arrester at select sites as per the requirements | |
| 11 | Sign Board | Sign board describing words such as "This area under surveillance" (in English and Local language) | |

**Cables for Traffic Signals**

| # | **Component** | | **Compliance (Yes / No)** |
|---|---|---|---|
| | **Make:** | | |
| | **Model:** | | |
| 1 | No's of core | 7 and 14 core1.5 sq.mm. 3 Core 2.5 sq. mm. | |
| 2 | Materials | PVC insulated and PVC sheathed armored cable with the copper conductorof suitable size as specified in BOQ. | |
| 3 | Certification | ISI Marked | |
| 4 | Standards | Indian Electricity Act and Rules | |
| 5 | IS:1554 | PVC insulated electric cables (heavy-duty) | |

### 6.4.20 Automatic E Challan System:

- The proposed system is a comprehensive digital solution for Transport enforcement wing and Traffic Police delivered through an Android based mobile application and a web portal. The system will capture all challans information by infield officer using

  mobile device at the time of violation and capture information will be sync to centralized server.
- The system will be integrated with Vahan and Sarathi applications and provides several user-friendly features, covering all major functionalities of Enforcement System. An end-to-end digital solution for multiple stakeholders: ease of operations for Transport Enforcement Officers/Traffic Policemen, increased visibility in operations for the State Transport department and improved support in maintaining compliance for citizens should be considered.
- The system will self-analyze the confidence level of the ANPR conversion. In case the confidence level is above user-configured threshold, the violation will be pushed automatically for eChallan generation.
- It will be possible to store the e-Challans based on the functional and legal requirements in terms of the number of days. The system will not delete the e Challans which are under legal or court procedure. The system will have postal record maintenance facility to keep track of dispatched, returned, refused, etc. e-Challans sent to the violating individuals. The e-Challan generation system will be able to generate e-Challans in local language and English. The Operator will have the option to filter the violations based on the following criteria for generation of Challans:

a. Number of violations by the same vehicle multiple times

b. For a particular category (e.g., 4-wheelers) of vehicles

c. For a particular Thana / police jurisdiction

d. Paid/Unpaid Challans

e. Ageing Analysis of Pending Challans

- The system will generate end-of-the-day report of the e- Challans generated. Thereport will contain the number of e-Challans generated, number of e-Challans paid,pending e-Challans, etc. The system will have the capability to send such reports viaemail to the designated persons. The system will have robust search functionality to search the violations by violation types, date and time duration, police jurisdiction / thana, operator, hand held device, location, vehicle number, etc. The system will generate statistical reports in terms of bar charts based on various categories.

### 6.4.20.1 E Challan System application

| # | Minimum Requirements |
|---|---|
| **A.** | **General** |
| 1. | E-challan software shall work in client -server mode, where all handheld devices units will act as clients connected to the server through cellular network for data transfer. The system should be scalable to as many required number of devices, which may be added later on, server requirements to be calculated as per scalability for at least 500 devices initially, which may be added later on. |
| 2. | E-challan system shall be able to retrieve vehicle owners details and vehicle data from RTO data base to minimise data entry |
| 3. | 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 |
| 4. | 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 |
| 5. | A unique challan number should be generated through client software for each challan |
| 6. | 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 oris in the list of suspicious vehicle |
| 7. | The most frequent traffic offences should be kept at the top in the drop down menu and offence ingredients should be available if required by officer |
| 8. | Date, time and GPS coordinates of place of challan should be automatically populated in the relevant fields of client software |
| 9. | Compounding amount must populate in the field automatically from master table |
| 10. | The successful bidder should develop the GUI and functionality as per requirements of the Police |
| 11. | The GUI should be lingual i.e English and local state language |
| 12. | It should be possible to integrate payment gate way operator with the system for felicitation of payment |
| **B.** | **Handheld Device Software** |
| 1 | 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. |
| 2 | On switching on the hand-held device the system must give access only after validation through user ID and password. |
| 3 | The communication between the server and hand-held device would be through GSM/GPRS/ 3G/4G or better connectivity etc. |
| 4 | Every challan created must have a unique self-populated number. |
| 5 | The Handheld 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. |
| 6 | The Handheld device should be able to access data/ information on the basis of driving license number, vehicle registration number etc. from the main server data relating to previous offences. |

| | |
|---|---|
| 7 | 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 Police. |
| 8 | When a challan is issued, the name and ID of the officer should be printed on the challan. |
| 9 | The Handheld device must be able to input and print multiple offences on the same challan. |
| 10 | The Handheld 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. |
| 11 | When downloading application software or pop-up tables or lists to the Handheld, or uploading challan records to the Server, synchronization of Handheld system must be automatic, in order to minimize human intervention. |
| 12 | Uploading data to the Database Server should be automatic in consistent manner. |
| 13. | 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. |
| 14 | Software should capture the list of documents seized during prosecution and such list must be reflected on the printed court challan. |
| 15 | The handheld application software shall allow the user to generate a summary report to facilitate evaluation of his daily work. |
| 16 | Once the challan is complete and saved any further editing should not be possible unless so authorized by administrator. |
| 17 | Each hand-held device should be provided with original printed user manual and appropriate carry case for Handheld device with charger. |
| 18 | The application software should allow online payment |
| 19 | 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. |
| 20 | The software should update DL/RC smart card with the booked offence. |
| **C.** | **E-Challan Application Software** |
| 1 | The Application Software should work in a web based environment. |
| 2 | The application software should be user friendly, easy to operate even by police personnel with minimum qualification of that of a head constable. |
| 3 | The software must provide comprehensive data back-up and restoration capability. |
| 4 | The system will function in web-based system where the hand-held device shall work as a node. |
| 5 | The application software should maintain the logs of user activities to facilitate the audit trail. |
| 6 | The system should have sufficient security features such as biometrics, password protection, audit trail, etc. |
| 7 | The system 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. |
| 8 | The software should be able to generate various periodical reports, summaries, MIS reports, query reply etc. as per the requirements of Police. |
| 9 | Administrator should be able to modify the master tables as and when required and should have the capability to push the changes to hand-held devices. |

| | |
|---|---|
| 10 | Software up-gradation must be provided from time to time as per available technology without further cost impact to Police. |
| 11 | The Department will provide the entire data of vehicle ownership and driving license for integration with the vendor's application software. |
| 12 | All database tables, records etc. required for various dropdown menus etc. shall also be created. |
| 13 | The application software is to be provided to handle various processes of the prosecution required by the office of senior police officers, Courts etc. |
| 14. | The application software should have the capability to export records in CSV, SQL and binary format |

**6.4.20.2 Challan Handheld device**

| **Specifications** | | **Compliance (Yes / No)** |
|---|---|---|
| **Make:** | | |
| **Model:** | | |
| Processor : | latest high speed processor min 800 MHz with suitable operating System | |
| Memory : | 512MB RAM or higher, 1 GB Flash or higher, With expandable micro SD card Capacity min 32GB | |
| Interface : | Interface : RS232, USB 2.0 Host USB 2.0 Client | |
| Wireless : | Wireless : WLAN (IEEE 802.11 b/g/n) GSM/GPRS/EDGE/CDMA should support 3G/4G/5G | |
| Communication: | USB 2.0, Bluetooth | |
| Power : | must last for minimum 6 hrs of use in the field (Rechargeable battery) suitable mechanism for charging from 220V standard AC powersupply must be provided, Vehicle charger also to be provided | |
| Printing method: | Width Minimum 3" Print Technology: Direct Thermal, at least 200DPI Print Speed: 60 mm per Second or better Easy paper loading mechanism Media Type: Direct Thermal Receipt Paper | |
| Rugged Structure | Drop Specification: 5 ft multiple drop Ingress Protection: IP 65 or better | |
| Camera | 5MP Integrated Camera with flash or better | |

| | | |
|---|---|---|
| Display and Keypad | Minimum 3.5" color VGA 640 x 480 resolution<br>QWERTY keypad with long life buttons, touch screen with backlight, must also have option for virtual QWERTY keypad andshould be readable in sunlight. | |
| Indications | suitable indication on device for charging, low battery, connectivity etc | |
| Operating Conditions: | Operating Conditions: Temperature (0 – 50 deg C) 5 – 95% RH (Non condensing) | |
| Dimensions and Weight: | Lightweight and should be easy to hold in the palm | |
| Storage | expandable micro-SD card capacity min 32GB | |
| Global positioning System (GPS) | Integrated GPS with A-GPS | |
| Other Features | login through unique ID, password and biometric data captureReal time clock with Battery backup<br>Embedded e-challan Software<br>e-challan Application: - Required device client software should be developed and installed on each device by the vendor to perform E-challan process on line and off line mode with server as per user requirement.<br>Operating System and application drivers: - | |
| | Suitable operating system. | |
| Accessories | User manual , Device cover casing , USB Cable and e-challan Software CD. | |
| Reader | Contact & Contactless Smart Card Reader and MSR reader, Fingerprint scanner, Integrated Bar Code Reader (1D/ 2D) | |
| Payment Interface | The device should have IPCI , EMV certified PINPAD as per RBI guideline for accepting payment through Credit / Debit card/NPCI | |
| Warranty | 5 Years | |

**6.5 Enterprise Management System (EMS)**

| Sl. No | Technical Specification | Compliance(Yes / No) |
|---|---|---|
| | Make· <to be provided by the SI> | |
| | Model: <to be provided by the SI> | |
| 1 | Complete end to end fault & Performance monitoring<br>**1.** Fault & Performance Monitoring (Network, Server, Cloud, VMs, CCTV, Wi-Fi, all IP network)<br>**2.** Network configuration & Change management<br>**3.** Traffic analysis<br>**4.** Assets Management<br>**5.** Log management<br>**6.** Network zero trust Access<br>**7.** Reporting & Dashboarding with integration<br>**8.** Helpdesk ITSM Tool<br>**9.** IPAM (IP Address Management) | |
| 2 | The OEM should have a support center in INDIA | |
| 3 | The solution should be capable of running in Linux platform | |
| 4 | The tool must be certified by PinkVerify or equivalent for ITIL v3 on incident management, change management and availability management processes andcertificate must be provided when sought | |
| 5 | The solution should have dual-stack IP support (support both IPv4 and IPv6) andshould be completely vendor-agnostic in nature to be able to monitor a multi- vendor environment<br>The solution should be a unified system which can monitor networks, servers, appsand any IT | |
| 6 | or Non-IT Communicable device (ex.: RF device, etc.)<br>The solution should be completely multi-tenant where in every module and systembeing used | |
| 7 | can be assigned to a specific set of users or a group of users.<br>The system should be capable to retrieve and show fault, performance , inventoryand SLA | |
| 8 | data in a single dynamic view with option to export the views into PDF, Word, Excel, HTML etc. formats depending on the need. System should have capability to add any additional information about the nodes via custom fields. | |

| | | |
|---|---|---|
| 9 | System should have Node Tags for device grouping and resource/interface tagging for element grouping. Apart from Node Tags additionally system should have options to do device grouping based on default fields and customer fields | |
| 10 | Provides the option to have the portal account to the end customers with restricted views limits to their specific infrastructure. System should have the capability to be implement in DMZ and non-DMZ zone with adequate security. | |
| 11 | Tool must provide Role based Access Control option | |
| 12 | The system should have an integrated ITSM tool from the same OEM. In future, it should be possible to use the service management features like Incident Logging, Viewing, Assignment, Escalation, Reporting, SLA Management etc. in the Service Manager tool GUI. The integration should be bi-directional in nature. | |
| 13 | Tool must provide intelligent Email-to-Incident feature in which tool admin has the option to allow certain domains for automatic conversion of emails to tickets. Tool should merge all subsequent email communication for a particular email-to- incident ticket into the same ticket in the form of a message thread. Tool should be intelligent enough to understand email conversation chains for merging emails to a particular incidnt. Merging logic should be not only based on TicketID but also on<br>email sender, cc responses to that email chain | |
| 14 | Tool should be able to provide real-time Email, SMS Notification alerts to notify respective users about any changes in ticket state and status. Tool should provide Email Communication Interface to allow technicians to send replies to customers / end users from the tool GUI and Record all the Email Communication in Chronological Order | |
| 15 | The integrated ITSM module should have its own Android & IOS app | |
| 16 | System should have a bi-directional integrated NCCM tool with option to use NCCM features in future easily by enabling the license for it without having to do any additional installations. The integration should allow assets and topology to sync<br>from the NMS module to the NCCM features for helping in Root-Cause-Analysis of faults | |
| 17 | System should have option for multiple options for discovery including IP address based discovery, IP address range discovery, CSV based discovery for bulk discovery and it should allow options to add custom fields to support customer specific data to upload during discovery | |
| 18 | The system should fetch topology via SNMP for ARP tables from routers , MAC tables from layer 2 switches, cisco Discovery Protocol, Link Layer Discovery Protocol,<br>Foundry Discovery Protocol or SynOptics Network Management Protocol. The discovery should be automated and continuous. | |
| 19 | Discovery has to work intelligently by identifying the device in the network by the given IP range and categorize into network devices and servers with vendor and model details. | |
| 20 | Automatically learn devices that supports SNMP, HTTP, Ping, SMTP, POP3, WMI,JMX,SOAP, REST API,PDC, SSH and Telnet along with any required protocol to communicate to the devices. | |
| 21 | System should support global threshold and it should have option to define individual resource/interface statistics level threshold | |
| 22 | System should have built in self learning algorithms to auto baseline and auto calculate thresholds of components or nodes to enable tool admin to start the monitoring with zero threshold configurations | |
| 23 | Configurable parameters like frequency, data duration, resolution duration, sigma based polarity value, reset points should be available | |
| 24 | All thresholds should have set point , reset point, polarity , set point message and reset point message for ease of use. | |
| 25 | Detect & highlight faults (abnormal situations) in near real-time occurring anywhere within the monitored IT Infrastructure | |

| | | |
|---|---|---|
| 26 | Provides Filtering, De-duplication, Holding, Suppression and Correlation capabilityto let user focus on the critical event that affects the business and business processes | |
| 27 | Provides multi-level (preferably six-level) Severity definition, will handle events automatically and inform the designated person as per operational requirement | |
| 28 | System should support separate Rule Engine based alarms apart from the genericthreshold.<br>**a.** Should have capability to configure Device Group based, Node Based, Resources/Interface based, Aggregation link based.<br>**b.** On Selection of Nodes/Resources/Aggregation links it have flexibility to filterbased on fields available in node information<br>**c.** Rules should have option to apply configuration on top of performance value orbased on configured threshold alarms<br>**d.** Rules should have option configure the breach based on min, max and averagevalues<br>**e.** Should have option to configure rules n repeat counters<br>**f.** Should have options to select custom alarm and clear alarm messages forindividual configured rules<br>**g.** Should have option to send severity levels like error, warning and information<br>**h.** Notifications support based on configured rules | |
| 29 | Provides alarm suppression with hold time and aid in prevention of flooding | |
| 30 | Sends alert via E-mail, SMS, Execute Batch file, SNMP Trap, XML notification, Pop-upwindow and Audio alert | |
| 31 | Monitors all traffic from all the interfaces of the network device. Provides traffic Utilization based on individual interface level, nodes level or based on the group bylocation, branch, departments etc.... as an Avg, Min and Max bandwidth, utilization, throughput or any custom monitoring parameters. | |
| 32 | Provision to change the polling interval to any frequency depending on the priority till the individual component / resource level like each interface might have the different polling interval in the same device based of the criticality and importance of service customer | |
| 33 | System should have capability to configure business , non-business hours or customtime polling. These configuration should be available for every device as well as every component in the device. | |
| 34 | Provision to disable and enable the polling of specific type of devices | |
| 35 | System should have capability to configure the maintenance period for any device.When device is in maintenance period there is no polling done and the SLA clockon the device is stopped. | |
| 36 | SLA calculation / Isolation report should be made with the consideration of both thePrimary and Secondary link together instead of individual link based. The downtimecalculation will be measured when both the links are down for internal reporting and link based for ISP reporting. System should provide the flexible configuration inUI itself based on user needs | |
| 37 | Provide a notification mechanism that allows administrator to define what notification channel to be used in different time of days, and able to trigger multiplenotifications to alert multiple person and actions | |
| 38 | Provide standard reports that display current status of nodes and interfaces. Reports could be viewed on daily graph (5 minute average), weekly graph (1 hour averageminute average), monthly graph (1 hour average) and yearly graph (1 day average) | |

| | | |
|---|---|---|
| 39 | Provide online and offline reports that allow the user to view the present usage of their devices. Reports generates should be exportable in the format of HTML, PDF, Excel and CSV. Allows end-users to browse all reports using any web browser like Internet Explorer, Mozilla Firefox, Google Chrome etc. without the need to install any<br>report specific software | |

| | | |
|---|---|---|
| 40 | Automatically generate daily reports that provide a summary of the IT Infrastructure as well as custom Reports and that are automatically sent by email at a pre- defined schedule to any recipient or save into any specific folder or drive. | |
| 41 | Supports instant diagnosis of the node status through Ping, Telnet and SNMPwalk | |
| 42 | Support Real-Time report generation for checking continuous reachability of targetdevice | |
| 43 | System should provide many different types of topology representation. To performthe following:<br>**1.** Display physical connections of the different devices being monitored in thesystem<br>**2.** Display flat maps of the entire network or networks in a single view<br>**3.** Display customer maps based on user configurations<br>**4.** Display maps based on geo locations | |
| 44 | Automatically learn IP Networks and their segments, LANs, hosts, switches, routers,firewalls etc. and to establish the connections and to correlate | |
| 45 | Provides provision to draw & map user specific network diagram | |
| 46 | The tool should have Integrated Web based feature to build Network Diagram, No separate client window to configure network Diagram. The builder should be similarto MS Visio with all pre-loaded shapes and icons. | |
| 47 | It should be a Drag & Drop based Network Diagram builder, Dynamically UploadImages, Customizable objects to support multiple vendors, capability to export maps in an XML format and upload to any other system. | |
| 48 | Panel View<br>**a.** Panel view should look similar to the actual device front panel<br>**b.** System should automatically detect the device model display the right panel without any additional configuration<br>**c.** Panel should show all the monitored interface with status<br>**d.** Fan status with live fan icon and LED status for power | |
| 49 | Tool should have complete inventory information of the assets discovered along with an option to fetch the target network device EoL / EoS information if required | |
| 50 | Tool must support CLI-based network device configuration snapshot managementincluding backup of configuration files, traffic logs, messages etc. , pushing configuration files to target network devices, with option to perform remote<br>firmware upgrades. | |
| 51 | The configuration changes to be done on target network devices must follow anapproval-based system wherein changes can be performed only after required approvals are passed. Tool must have in-built approval mechanism along with option to integrate with Change Management module of other ITSM tools for theapproval process. | |
| 52 | Tool must provide option for target CLI-based network device vulnerability detection based on their model number and firmware version. It should also provide options to remedy the vulnerabilities with help of pre-configured scripts forcertain vulnearbility types. | |
| 53 | Tool must provide option to perform standard compliance checks like PCI-DSS, NIST, DISA etc. across all target CLI-based network devices | |

| | | |
|---|---|---|
| 54 | Tool must provide an option for taking remote access via Telnet / SSH to target CLI-based Network Devices with an option to record all sessions to capture all commands being executed on the remote devices. The tool must allow session relay wherein a higher-privileged user can view the ongoing CLI session of a lower- privileged user in real-time from the tool GUI. The sessions should be saved for historical analysis with flexible filter options like searching for sessions in which a particular command has been executed. | |
| 55 | The proposed monitoring solution should be able to monitor network traffic by capturing flow data from network devices, including Netflow v5 or v9, J-Flow, IPFIX,sFlow, NetStream data and also sampled Netflow data. Solution must be able to | |

| | | |
|---|---|---|
| | store ALL flows without any rollups or loss for retention period - for security and auditpurposes. | |
| 56 | Should identify which users, applications, protocols, countries, AS numbers, toprouters, and top interfaces are consuming the most bandwidth | |
| 57 | System should have capability to alternatively capture traffic data via packetcapture. | |
| 58 | Should be able to associate traffic coming from different sources to applicationnames | |
| 59 | Should be able to receive flows from non-SNMP-enabled devices, like VMwarevSwitch | |
| 60 | Should monitor Type of Service (ToS), Differentiated Services Codepoint (DSCP), andPer-Hop Behavior (PHB),BGP AS and NEXT HOP | |
| 61 | Should provide flow analysis with 1-minute granularity and The solution should beable to monitor up to 5 million flows per second, and should employs advanced optimization methods | |
| 62 | Tool should allow QoS monitoring of WAN links across multiple technologies likeIPSLA, RPM, NQA etc. across multiple protocols like HTTP, TCP, FTP, DNS etc. | |
| 63 | QoS paramters should include link response time, link-level latency, link-levelpacket loss, link-level jitter, Round-Trip-Time etc. | |
| 64 | Should monitor Class-Based Quality of Service (CBQoS) to find out if traffic prioritization policies are effective and if business-critical applications have networktraffic priority. Should also support CBQoS Nested policies | |
| 65 | Tool should have option to collect and store system logs from target devicesincluding firewalls, routers, switches, WLC, servers, applications & databases | |
| 66 | Tool should have multiple filtering options for incoming system logs based on targetdevice, log_ID, severity, level, message, OS type, application / database etc. | |
| 67 | Tool should have option to export specific syslog messages to users via email / SMS | |
| 68 | System should support VM, Hypervisor and Cluster monitoring from different vendorslike VMWare, Citrix, Nutanix, Linux etc. | |
| 69 | System licensing should be based only on Physical Hosts and not charge separately for individual guest VMs running on VM Hosts | |
| 70 | System show have capability to monitor availability and performance of industry standard web server like IIS / Tomcat / Apache / Jboss, email server like Exchange / Zimbra / Lotus Notes, and databases like Oracle / MSSQL / MySQL / PostgreSQLetc. | |
| 71 | System show have capability to monitor HTTP service,HTTPS service,FTP server statistics, POP/SMTP services,ICMP services or any customer specific port based systems | |
| 72 | Cover geographically distributed networks through multi-level scalable distributeddeployment architecture | |
| 73 | Ability to add new pollers at no extra cost. | |

| | | |
|---|---|---|
| 74 | The tool should have option to be deployed in HA mode (High Availability) forredundancy purpose | |
| 75 | Integration should provide the option in both north as well as south bound integration on each module level. Any fault details should be able to send to third party CRM, Customer Portal, UNMS or even EMS if needed using the Trap, XML andeven direct database query integration | |
| 76 | Provide open APIs in the system which can be used by customers for integrating their own systems. Integration should provide the option in both north as well as south bound integration using multiple options like RestAPI, XML, SOAP, Corba etc.on each module level. Any fault details should be able to send to third party CRM, Customer Portal, UNMS or even EMS if needed using the Trap, XML and even directdatabase query integration | |
| 77 | The system should allow remote access to the internal network via a Zero Trustsystem and no use of VPN or agents. | |

| | | |
|---|---|---|
| 78 | Only specific protocols like SSH, RDP, Telnet , VNC which are essential for remoteaccess should be allowed | |
| 79 | All the actions taken during the remote access should be recorded and haveability to audit them later. | |
| 80 | All remote access should be authenticated and all devices a user has accessshould be pre-allocated | |
| 81 | The system should have ability to authenticate access to any device via Single signon and password should not be exposed to users | |
| 82 | All CLI session should have command control, any command that is not authorizedcannot be used and session should be terminated | |
| 83 | Administrator should be able to view the live session of any ongoing session andcan terminate them also | |
| 84 | Any file being transferred should be via the Zero trust system. File will be scannedfor virus and only then be transferred to the target location | |
| 85 | Time based; temporary users should be configurable in the system | |
| 86 | IPAM solution should have complete IP discovery, IP management with historicaltracking | |
| 87 | IPAM should have IP Grouping, Subgrouping and role and privileged based access. | |
| 88 | Support both IPv4 and V6 along with IP Classes and VLSM based | |

**6.6 Citizen Engagement System : Creation of Online and Mobile Applications**

SMART captures the important attributes of Good Governance i.e., Simple, Measurable, Accountable, Responsive and Transparent governance.

ICT in governance has been experienced in the form of e-Governance, which redefined theway Governments work, share information, engage citizens and deliver services to externaland internal clients for the benefit of both government and the clients that they serve.

Governments harnesses information technologies to reach out to citizens, business, and otherarms of the government to: a)Improve delivery of services to citizens, businesses and employees b) Engage citizens in the process of governance through interaction c) Empowercitizens through access to knowledge and information and d) Make the working of the government more efficient and effective

This results in enhanced transparency, convenience and empowerment; less corruption; revenue growth; and cost reduction.

Authority intends to implement a robust Smart governance & citizen services solution for delivering efficient and effective citizen centric services as well as improving municipal finance/expense management and administrative functions.

The Smart governance solution, while modular, should be capable of providing all the functionality described in this section as an integrated platform.

The SI shall ensure that all the modules under Smart Governance are integrated with the overall project. SI shall create an enabling platform to link the relevant features with the Citizen Services.

The applications designed and developed for the departments concerned must follow best practice and industry standards. In order to achieve the high level of stability and robustnessof the application, the system development life cycle must be carried out using the industry standard best practices and adopting the security constraints for access and control rights.The solution should comply to the below standards as applicable:

(a) 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

(b) The Smart governance solution shall be of leading industry standards and as per requirements mentioned in IS 18006 (Municipal Governance Reference Architecture).

Shall comply to applicable elements of data layer reference architecture (IS 18002) as well as IS 18000 (UNIFIED DIGITAL INFRASTRUCTURE – ICT REFERENCE ARCHITECTURE (UDI-ICTRA), Section 8

Should build an integrated Collaboration Platform to provide all citizens services on a single platform. Services that are universally accessible and that follow an international standard for accessibility and operational or to be made operational by other Government or approved agencies shall be made available through the CCP. Citizen engagement and Grievance Redressal Management Systems with back-end workflow.

The principal objective of CCP is to create one all-inclusive system which allows citizens / tourists/ visitors/ stakeholders to access various government services and information. Key functionalities of CCP include:

- Improving delivery of services to citizen and tourists, businesses and employees
- Engaging citizens/ stakeholders in the process of governance
- Empowering citizens/ stakeholders through access to information
- Improving government functioning across departments – making it more efficient and effective The envisaged benefits post implementation of CCP include enhanced transparency and accountability, increased revenue, reduced cost, empowerment of citizen and lesser time for service delivery, ease of multi departmental operations for a cause.

By implementing CCP following benefits are envisaged, For

City Authorities

- Digital portfolio of city services
- Better citizen connect
- Efficient and effective delivery of citizen services
- Creating positive social impact
- Reduced cost of delivery of services for Citizens
- 24*7 Service Access
- Time saving
- Improved connect with city authorities
- 24*7 information dissemination
- Multiple services on a single platform
- Chatbot

The principal objective of CCP is to create one all-inclusive system which allows citizens / tourists/ visitors/ stakeholders to access various government services and information. Key functionalities of CCP include:

- Improving delivery of services to citizen and tourists, businesses and employees
- Engaging citizens/ stakeholders in the process of governance
- Empowering citizens/ stakeholders through access to information
- Improving government functioning across departments – making it more efficient and effective

The envisaged benefits post implementation of CCP include enhanced transparency and accountability, increased revenue, reduced cost, empowerment of citizen and lesser time for service delivery, ease of multi departmental operations for a cause.

Key Functional Requirements - Collaboration Platform

City Collaboration platform should provide below information in the form of Audio/ Video/ image/ GIS map/ text.

- "About Puducherry" will provide details about Puducherry city and will have dedicated sections for about the city, history of Puducherry, how to reach, climate, local cuisines, festivals, Important Business locations, places of interest, art and craft, facts at a glance, where to stay, where to eat, places of interest, heritage spots, weekend getaways, places to visit, best time to visit, gallery (Photos & videos), etc. few of these points have been elaborated below in detail.
- "Explore City" giving details about the city, history, how to reach, cuisine, festivals, Important Business locations, places of interest, Beaches, art and craft (Add to Favorite, Get Directions, About, get there nearby and each linked with City GIS Map and Photos of concerned location)
- "Facts at a Glance" giving details about area, population, religion, linking roads, postal code, longitude, latitude, area, altitude, population, literacy rate, STD code, average rainfall, villages, language and the different seasons and reasons to visit.
- "Tourism destination" giving details on tourism experience (Add to Favourite, Get Directions/Driving Directions, About, get there nearby and each linked with City GIS Map and Photos of concerned location) heritage spots, pilgrim destination, nature discovery, heritage, highway, adventure spots, Beaches, Nearby places to visit, Places to Stay etc.
- City Collaboration Platform will provide the web-link of Tourism Development Corporation (PTDC) portal for booking the Puducherry State tourism packages.
- City has many artifacts, memoirs and items with historic perspectives and are available in designated markets in and around the many important places of interest in the city. A list of unique memoirs and the connected stores are to be listed through mobile apps showing distances from current location, etc.
- "Cultural events calendar" section will provide the list of cultural events within city including dates, venues and details of the event.
- "Tenders" will provide the list of PSCDL tenders in downloadable format.
- "Key Personnel-staff directory" will have the details (such as emails, contact information, designation, job profile, office address etc.) of PSCDL stakeholder members, Elected Political Members, Mayor, Municipal Commissioner and all Officials
- "Important GOs / Policies" section will have the list of all important and relevant government orders and policies.
- "Downloads" section will provide the list of important document in downloaded format to the user.
- "Recruitment" section will provide the current job openings in PSCDL and their stakeholders departments.
- "Educational Institutions" listings, including location, contacts, courses etc.
- "Sports Facilities" will provide the details of facilities available within the city including list of play grounds, details on in-door or out-door facilities, list of tournament / event dates etc. Please note that this section will provide only information.
- "Ward Information" section will provide the below information:

- Municipal officers contact.
- Water supply information / announcements.
- Power supply information / announcements.
- Garbage collection schedule.

List of schools, community centres, playing ground, parks etc. and the contacts for bookings.

- "Health Services" will provide the details of hospitals including contacts, address, emergency contacts, available facilities and OPD timings. It will also provide the list of ambulance services available in the city with contact numbers.
- "Emergency Services" module will have the contact details of below emergency services.

- Ambulance
- Fire
- Police
- Traffic

All the contacts shall support for "dial to call feature" from a page.

- "Social Networking & City-wide Collaboration" will help citizens to communicate through social networking platform such as Twitter / Facebook / WhatsApp etc.

- Current news, events will enable citizens to get live feeds of various activities & events in the city.
- Feedback/ inputs / opinions will help citizens to collaborate and provide inputs/ opinions on various policy related aspects, local governance aspects, feedback on specific issues etc.
- Search tools will enables citizens / tourists to search for desired information available in the City Collaboration Platform.

Collaboration platform should be integrated with below modules but not limited below list.

- Environment information from nearest available Environment sensor.
- Citizen / Tourists can view their e-challan in case of any traffic violation.
- Integration with Property Tax System
- Water Supply and sewerage system
- Birth and Death, Marriage Registration, Trade Licensing etc.

**Key Functional Requirements - Collaboration Platform**

| Sl. No. | Specifications | Compliance (Yes / No) |
|---|---|---|
| | **Citizen Engagement Application** | |
| 1 | The application shall accept requests or inquiries from the citizens and track those requests from different channels such as phone, e-mail, SMS, Web Portal, Chatbot, VoIP Call, Smart Phone Application (City App) & social media (Facebook, Twitter.) etc. | |

| | | |
|---|---|---|
| 2 | It should integrate all service requests through Voice & IVR based system for efficiently managing the citizen grievance request | |
| 3 | The operator should be able to chat/reply to any queries raised through different channels via the same channel | |
| 4 | The application shall allow the user to select service request category type or use auto-filled information for incident creation. A unique service transaction number should be assigned for each incident after a service request is created. | |
| 5 | The application shall auto-populate fields based on previous calls or known data from other channels. | |
| 6 | The application shall capture different types of input data, including but not limited to: date, citizen profile data, issue type, issue description, time of day the grievance occurred, location, etc. | |
| 7 | The platform should have the ability to view map of service requests on top of a City GIS base map and display service requests and associated data (service request number, status, short description, field assets and workforce) on the same map. | |
| 8 | The application should provide information regarding the exact location of the service request (e.g., actual location of garbage or downed tree). | |
| 9 | The application should automatically determine duplicate requests and associate a request with multiple citizens. | |
| 10 | The application must have the ability to display the citizen's previous interactions from different channels using search feature and view citizen's previous service request status. | |
| 11 | The application should have the ability to display "top" grievance types based on historical trends ranked according to the most viewed and most relevant service request. | |
| 12 | The application should provide the operator the ability to view and attach files (such as PDF) and other documents (e.g., images) | |
| 13 | The application should prevent a request from being closed until all associated actions are completed. | |
| 14 | The application should have the ability to dispatch a service request to the workforce, a particular department or an outside agency. | |
| 15 | The application should provide a set of standard reports that will provide statistical reporting for open, closed, escalated, priority, completion time, based on address and location. | |

| | | |
|---|---|---|
| 16 | The application should have a dashboard module that can give a quick and easy view to know overall Grievance details: trend, status, channels, incident trends, response of department and feedback. | |
| 17 | The application should provide the dispatch the incident to City Command Centre, City Emergency Operation Centre, relevant department application based on the nature of the grievance/complaint. | |
| 18 | The application should provide the operator with the facility to view all dialled, missed, received calls. | |
| 19 | The application should allow the administrator to define SLAs for all the incidents. | |
| 20 | The application should allow the administrator to add, edit and delete various department | |
| | **Citizen Mobile App** | |
| 21 | It shall integrate the Citizen Service request and also provide visibility to the citizen of the various city notifications. | |
| 22 | Key Features of the app should include: | |
| 23 | • Incident Reporting | |
| 24 | • Complaints Tracking | |
| 25 | • City Services – Parking, Transport | |
| 26 | • e-Governance Services | |
| 27 | • Bills Payment | |
| 28 | • News | |
| 29 | • Events | |
| 30 | • Notifications | |
| 31 | • Emergency | |
| 32 | • Chatbot | |
| 33 | The Application shall integrate Citizen Grievance and Compliant from various channels – social media through Keywords, Mobile App based reporting as a crowd source, Citizen Calls, etc. | |
| 34 | Citizen app shall provide capability to citizen to report incidents across various grievances covering emergency, garbage collection, accidents, water leakage, electricity outage etc. Such requests shall be integrated with ICCC platform, and the service delivery will be automated through the ICCC functions. | |

| | | |
|---|---|---|
| 35 | City App should allow to make SOS calls with location and video snapshot | |
| 36 | City App should be capable to schedule waste collection from Citizen's location | |
| 37 | City App should allow to search the parking space across the city | |
| 38 | City App should allow to view different modes of transport available for Citizen in the city | |
| 39 | City App should allow the citizens to receive the traffic related notification and be updated about the traffic condition in selected areas | |
| 40 | City App should allow citizens to pay utility bills and taxes | |
| | **City Web Portal** | |
| 41 | It should provide a single view to the citizen for engaging with the city departments. | |
| 42 | It should provide live update of the City Service and also act as a foundation for Citizen to register the identity and download the Citizen App. | |
| 43 | It should also provide interface for the citizen to request through Email, Chat Services so that the citizen can also call for service through these channels. | |
| 44 | Email and chat services: service request and distribution to the right operators. | |
| 45 | Portal should allow citizen to use different City services by selecting services categories | |
| 46 | The Web portal should provide the citizen the facility to report Civic grievances by selecting grievance categories and subcategories by attaching Image or Video to support the Grievance request | |
| 47 | The citizen can view the history and status of all the complaints that have been requested. | |
| 48 | The Citizen should be able to see the GIS view of the city and can find POIs as when required | |
| 49 | The web portal should have Content Management System to create content and publish content and it will integrate with all public Channels for News and other feeds. | |
| 50 | The web portal should have CMS that shall provide a role-based user access mechanism where an administrator can create and manage users, user groups, roles, and role permissions. | |

| | | |
|---|---|---|
| 51 | The CMS should support login module using which content authors will be able to login. | |
| 52 | Login module should have forgot password mechanism. In case user forgets the password/wish to reset a link should be sent to user's registered Email address from where password can be reset. | |
| 53 | CMS should support integration with Directory Services (supporting LDAP) to manage users and their preferences. CMS should also support latest security certificates like SSL 3.0 | |
| 54 | CMS should be able to publish content to any external portal apart from its native portal | |
| 55 | CMS shall support the creation, modification, and deletion of templates to enable easy management of site and page layout and navigation | |
| 56 | CMS should contain a WYSIWYG editor and provide standard Word authoring features (also known as a Rich Text Editor) to enable an editor to add and format text, links, and images to content areas, create tabular layouts within a text area and apply styles without needing HTML skills | |
| 57 | CMS should support drag and drop feature to enable easy management of content. The CMS shall support the following minimum preview and publication functions: - | |
| 58 | a) Preview only on CMS (not visible to users) | |
| 59 | b) Save as unpublished (draft) | |
| 60 | c) Preview on Portal | |
| 61 | d) Send for approval | |
| 62 | e) Approve | |
| 63 | f) Publish after approval (i.e., after successful completion of the approval workflow) | |
| 64 | g) Unpublish (save as unpublished, not visible to users) | |
| 65 | h) Publication scheduling | |
| 66 | i) Publication expiration date (automatic unpublish) | |
| 67 | CMS shall contain a content approval workflow to enable the approval of modifications (create, modify, delete) before publication (i.e., before becoming visible to the public) | |
| 68 | CMS shall support Administrator (or a designated user with an appropriate permission level) to assign and reassign users to workflow tasks (i.e., define the targets within the workflow) | |

| | | |
|---|---|---|
| 69 | CMS shall support the creation and application of styles using Cascading Style Sheets (CSS) enabling the swift alteration of the look and feel (colour, font, image size and positioning, link attributes, table properties). Graphics should be avoided altogether regarding navigation (e.g., no navigation buttons - these should be text, which gets its look and feel through CSS). | |
| 70 | CMS shall include a social media integration module that allows configurable publishing of content (pages, interactive data visualizations, images, videos) to a variety of social media (Facebook, Twitter, Google+, LinkedIn, Pinterest, Tumblr, etc. CMS should also support publishing of content specific to mobile app if required | |
| 71 | The CMS should have the capability to create and deploy content on different portals with same or different branding | |
| 72 | The CMS shall support the Unicode character set (UTF-8) | |

### 6.7 Smart Poles Proposed

**ICT Solution:**

It is now proposed to install smart poles in different locations of the city which shall be in turn connected to the ICCC. The various components that are envisaged in the said smart poles are as follows:

- Fixed Box Camera
- Smart Lighting
- AQM : (Environmental Sensor, Weather Sensors, Rain Gauge Sensors )
- Public Address System
- Digital Bill Board
- Emergency call box
- Wi-Fi
- 5 G ready

**Scope of work:**

The scope includes procure, supply, install and commission smart poles including allcivil foundation works and provide the data and power connectivity for the said poles.

### 6.7.1 Smart Pole Specification

| No | Specification | Compliance (Yes / No) |
|---|---|---|
| | **Make:** | |
| | **Model:** | |
| 1. | Smart pole should be able to meet city aesthetic requirement and it should visually appealing. It should easily blend-in into city street pole master plan. | |
| 2. | Pole Height requirement is 12-15 meters. TRAI and DOT guidelines to be followed as the pole will be used as a telecom site. | |
| 3. | It should be able to support telecom technologies like 5G, GSM, WCDMA, LTE and Wi-Fi. | |
| 4. | It should be possible to support LED luminaries from reputed OEMs. | |
| 5. | Smart pole should be designed as per telecom standards of India and specifically Puducherry weather conditions such as wind speed, climate, aesthetic. | |
| 7. | The allowed diameter will be as per the BIS regulations and wind speed requirement | |
| 8. | All cabling, cooling/heating etc should either be via/inside the pole or should be camouflaged (aesthetically concealed) so that it is not visible from outside. | |
| 11. | The minimum power backup requirement is 1 hrs for all equipment | |
| 12. | It should be possible to provide multiple color options as asked by city Authority as per city light pole colors | |
| 13. | It should be possible to house radio units with integrated antenna, MW /optical transmission unit, SMPS (AC to DC convertor), batteries, controllers, power distribution etc. either inside the smart pole or should be camouflaged (aesthetically concealed) so that it is not visible from outside | |
| 15. | It should be possible to provide light connection in daisy chain with separate MCB for lighting | |
| 20. | The cabinet where electrical electronics equipment is store should be IP 67 compliance or better | |
| 22. | The ambient temperature requirement is 0-50 degrees | |

| | | |
|---|---|---|
| 23. | The overall power budget for smart pole should not exceed 2KW ( lights) or as per standards. | |
| 24. | It should support minimum two light arm per smart pole. However, the same may vary depending on location to be surveyed and finalized by the selected bidder. | |
| 25. | The minimum life requirement of above smart pole structure is 10 years | |
| 26. | The Concessionaire should not use any banned /restricted material as per Indian regulations. Should have 5 year warranty | |

### 6.7.2 Anti-Climb Galvanized Poles for Mounting Camera etc.

| S.N. | 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. 10cm diameter pole (SI to choose larger diameter for higher height) |
| 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 300mmx300mmx15mm (or) 30cmx30cmx1.5cm |
| 6. | Mounting facilities | To mount CCTV cameras, 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)<br>Expected foundation depth of min. 100cms.<br>Please refer to earthing standards mentioned elsewhere in the RFP. |
| 9. | Protection | Lightning arrester at select sites as per the requirements |
| 10. | Sign-Board | A sign board describing words such as "This area under surveillance" (in English and Hindi) |

### 6.7.3 Digital Bill Board

| No | Specification |
|---|---|
| 1 | The Bill boards should be hanged at the height of at least 5 meters or above, however the uniformity should be maintained on all the poles. Should have minimum 5 year warranty |

| | |
|---|---|
| 2 | The Smart Billboard will be operated from Command & Control Center |
| 3 | It should have provision for incoming power input cables and fiber connectivity |
| 4 | It should be Vandal Proof ; IP Level IP67 or better |
| 5 | It should have display of minimum (80 Inches +/- 5%) , Rectangular shape (2mx1m )+/- 5% as per city regulations. |
| **No** | **Specification** |
| 6 | It should be Aesthetical & Camouflaged finish with respect to environment |
| 7 | Pixel Pitch 10 mm or Lower, Lower pixel pitch is better, LED Configuration RGB 3 in 1 SMD |
| 8 | Pixel Density Minimum 10,000 pixels per sqm or higher |
| 9 | Viewing distance Suitable for readability from 40 Mtrs. or more at the character size of 240mm, from moving vehicles |
| 10 | Viewing Angle H 140 deg / V 90 deg or better with Refresh Rate>1920 Hz or better |
| 11 | Temp Range 0 to +50 Degrees C or better; Gray Scale Processing 12 Bit or better |
| 12 | Brightness (Calibrated) 5000 cd/m2 or better; Contrast Ratio 2500:1 or better |
| 13 | Maximum Power Consumption 825 w/sqm or lower; Power Input 100 ~ 240 VAC |
| 14 | Dimming Capability Auto dimming capability to adjust to ambient light level (sensor based automatic control) |

#### 6.7.4 Environmental Sensors

Environmental pollution, particularly of the air, is nowadays a major problem that unknowingly affects lives in the cities. Air Pollution is defined as the presence of contaminants or pollutant substances in the air that Interfere with human health or welfare, or produce other harmful environmental effects and it is important that the 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.

Environmental Management solutions can be used to determine the quality of air (And water, SWM, Energy,) and the environmental parameters to enable a deeper understanding of the polluting sources like vehicles, industries, construction or natural reasons etc.

It is recommended to deploy Environment Sensing Units spread across a region, to create a larger data pool leading to better understanding of spatial and temporal trends in air pollution to take measures for corrective actions.

**Key Issues**

Rapid urbanization, which strains basic infrastructure, coupled with more frequent and extreme weather events linked to global climate change is exacerbating the impact of environmental threats. Common environmental threats include flooding, tropical cyclones (to which coastal cities are particularly vulnerable), heat waves and epidemics.

Owing to the physical and population density of cities, such threats often result in both devastating financial loss and deaths. Making cities more resilient against these environmental threats is one of the biggest challenges faced by city authorities and requires urgent attention.

Indicative Key Outcomes and KPIs

- Improved monitoring of city environmental Parameters
- Temperature, Humidity
- Ambient Light
- Level of Noise Pollution
- CO, NO2.
- Water quality of public surface water bodies
- City to add/ update based on city objective.
- Improved communication with citizens through other city solutions like City App, PA system, ECB etc. based on city environmental parameters
- Improved management of pandemic situations in the city

**Key components**

A typical Environment Management solution may consist of the following components. One may not need all of these or may be even more than these based on the technology and design used.

Sensors to measure the pollutants and other environmental parameters

Electronic displays to communicate the measured levels to the citizens

IoT gateways, network switches, copper, fiber optic or wireless connectivity to interconnect the local system components and also to the datacenter/cloud.

Desktop application for administration, operation and service/repair.

**Functional Requirements**

The SI shall;

**a)** Install environment sensors (as per the functional requirement) to display environment related information at various strategic locations through variable message display (VMD) system.

**b)** The environment sensors shall be integrated with the ICCC to capture and display/ provide feed on Temperature, Humidity, Pollutants like So[X], No[X], Co[X], PM2.5, PM10, Noise Pollution, etc. The data it collects should be location-marked.

**c)** Various environment sensors should sense the prevailing environment conditions and send the data to the ICCC where real time data resides and the same shall be made available

to various other departments and applications for decision making.

**d)** This information should be relayed instantaneously to signage – large, clear, digital-display screens which let citizens know regarding the prevalent environmental conditions.

**e)** Environmental sensors recorded data shall be used by Smart Environment Mobile application to enable user for alarm management and notification of environmental details on real time basis.

**f)** Mobile app should be developed for Grievance Redressal of Citizen – 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.

**g)** The system should provide ability to ;

i. View Air Quality Index across city, levels of various constituents (CO, CO2,SO2,NO2, PM10) etc.
ii. Correlate the data emanating from various Environmental sensors in different areas of city with respect to city mobility/traffic
iii. Communicate the levels of AQI and Noise in locality to citizens, businesses and industry on daily basis via Citizen Mobile App.
iv. View the hotspots across various areas in city where high noise cases are reported by citizens
v. Predict the poor quality of air and water on various dimensions like timelines, seasons where there is high density of markets, industry or shops.
vi. Spread awareness at chronic location/spots identified over VMD, website, mobile app, WhatsApp etc.
vii. Allocate and monitor noise complaint to the on-field squad to take intervention as per defined SoPs.
viii. View the heat-map of noise pollution over different dimensions
ix. Educate the masses using bulk SMS, email and messages about best practices
x. Send the aggregated data of AQI and Noise to concerned authority to address the problems through policy.
xi. Address the noise issue by issuing advisory to local businesses, marriage gardens etc.
xii. View hospitals and staff/beds/medicine availability in real time.
xiii. Provide City wide Hot-Spot Analysis based on lab reports.
xiv. Correlate cause like the impact of water quality, air quality, stress on diseases reported at primary, secondary and tertiary care.
xv. Do the predictive analytics over the past data to predict the outbreak of disease in community
xvi. Coordinate with Hospitals, Labs and on-field staff in real time using handheld devices etc. Ability to coordinate with Hospitals, Labs and on-field staff in real time using handheld devices etc.
xvii. View heat-map of different diseases on different dimensions over city maps
xviii. Provide awareness drive for citizens in targeted areas through email, SMS, WhatsApp, VMD etc. as per preventive healthcare SoPs
xix. Coordinate with Sanitation Department and other line department to take corrective action.

Install environment sensors (as per the functional requirement) to display environment related information at various strategic locations through variable message system

- The environment sensors shall be integrated with the ICCC to capture and display/ provide feed on Temperature, Humidity, Pollutants like SoX, NoX, CoX, etc PM2.5, PM10, Noise Pollution. The data it collects is 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 data should be collected in a software platform that allows authorized 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.
- SI can also make use of the nearby Variable messaging displays wherever possible (need to be finalized post detailed survey of locations).
- The sensor management platform should allow the configuration of the sensor to the network and location details etc.

**Functional Requirements (AQM on smart Pole and standalone Environmental Sensor)**

| S. No. | Description | Compliance (Yes / No) |
|---|---|---|
| 1 | Shall be ruggedized enough to be deployed in open air areas on streets and park | |
| 2 | Environmental Sensor station shall be housed in a compact environmentally rated outdoor enclosure. It shall be an integrated module which shall monitor overall ambient air, noise quality, weather etc. | |
| 3 | Mounting of the environmental sensor module shall be co-located on streetlight pole or shall be installed on a tripod/standalone pole. | |

| | | |
|---|---|---|
| 4 | Environmental sensor station shall monitor following parameters and include the following integrated sensors inside one station:<br><br>• Carbon Monoxide (CO) sensor<br>• Ozone (O3) sensor<br>• Nitrogen Dioxide (NO2) sensor<br>• Sulphur Dioxide (SO2) sensor<br>• Carbon Dioxide (CO2) sensor<br>• Particulate/SPM Profile (PM10, PM2.5, and TSP) sensor<br>• Temperature sensor<br>• Relative Humidity sensor<br>• Wind Speed sensor<br>• Wind Direction sensor | |
| | • Rainfall sensor<br>• Barometric Pressure sensor and<br>• Noise sensor | |
| 5 | Solution shall display trends of environmental parameters based on user specific time periods. | |
| 6 | Data shall be collected in a software platform that allows third party software applications to read that data. | |
| 7 | Solution shall display real time and historical data in chart and table views for dashboard view of the Client. | |
| 8 | Alarms shall be generated for events where the environmental parameters breaches the safe or normal levels. | |
| 9 | The sensor management platform shall allow the configuration of the sensor to the network and also location details etc. | |
| 10 | The platform shall comprise of an Industrial PC running latest version OS and compatible software. | |
| 11 | Data logging with central Monitoring System will be through GPRS/TCP-IP from all the AQMS system and shall have an ability to program and log channels at different intervals and shall have a capability of averaging and displaying real time data and averaged data over a period of 1 min, 10 min, 30 min, 1 hr, 4 hr, 8, hr, 24 hr and so on. | |
| 12 | Real time or averaged data can be viewed quickly and easily through a remote interface on the central computer. | |
| 13 | System shall be able to perform nested calculations vector averaging and rolling averages | |
| 14 | The platform shall have a feature for viewing instantaneous and historical data in the form of tables and graphs either locally or from a remote client. | |
| 15 | Data retrieval from CMS via USB shall be possible. | |
| 16 | Generation of reports as per requirement of customer etc. | |
| 17 | Alarm annunciation of analyzer/sensor in abnormal conditions | |

| | | |
|---|---|---|
| 18 | The environment sensors shall be integrated with the integrated command and control centre system to capture and display/ provide feed. The data it collects is location-marked. | |
| 19 | 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. | |
| 20 | Information shall be relayed to signage – large, clear, digital-display screens which let citizens know regarding the prevalent environmental conditions. | |
| 21 | Further environmental sensors recorded data shall be used by Mobile application to enable user for alarm management and notification of environmental details on real time basis. | |

**Technical Requirements**

| S. No. | Description | Compliance(Yes/No) |
|---|---|---|
| 1 | **Carbon Monoxide (CO) Sensor**<br>• CO sensor shall measure the carbon monoxide in ambient air<br>• Range of CO sensor shall be between 0 to 1000 PPM<br>• Resolution of CO sensor shall be 0.001 PPM or better<br>• Lower detectable limit of CO sensor shall be 0.040 PPM or better<br>• Precision of CO sensor shall be less than 3% of reading or better<br>• Linearity of CO sensor shall be less than 1% of full scale or better<br>• Response time of CO sensor shall be less than 60 seconds<br>• Operating temperature of CO sensor shall be 0°C to 60°C<br>• Operating pressure of CO sensor shall be ±10%. | |
| 2 | **Ozone (O3) Sensor**<br>• O3 Sensor shall measure the ozone in ambient air<br>• O3 Sensor shall have a range of at least 0-1000 PPB<br>• Resolution of O3 sensor shall be 0.001 PPM or better<br>• Lower detectable limit of O3 sensor shall be 0.001 PPM or better<br>• Precision of O3 sensor shall be less than 2% of reading or better<br>• Linearity of O3 sensor shall be less than 1% of full scale<br>• Response time of O3 sensor shall be less than 60 seconds<br>• Operating temperature of O3 sensor shall be 0°C to 60°C<br>• Operating pressure of O3 sensor shall be ±10% | |

| | | |
|---|---|---|
| 3 | **Nitrogen Dioxide (NO2) Sensor**<br><br>• NO2 Sensor shall measure the Nitrogen dioxide in ambient air<br>• NO2 Sensor shall have a range of at least 0-10 PPM<br>• Resolution of NO2 sensor shall be 0.001 PPM or better<br>• Lower detectable limit of NO2 sensor shall be 0.001 PPM or better<br>• Precision of NO2 sensor shall be less than 3% of reading or better | |
| | • Linearity of NO2 sensor shall be less than 1% of full scale<br>• Response time of NO2 sensor shall be less than 60 seconds<br>• Operating temperature of NO2 sensor shall be 0°C to 60°C<br>• Operating pressure of NO2 sensor shall be ±10% | |
| 4 | **Sulphur Dioxide (SO2) Sensor**<br><br>• SO2 Sensor shall measure the Sulphur dioxide in ambient air<br>• SO2 Sensor shall have a range of at least 0-20 PPM<br>• Resolution of SO2 sensor shall be 0.001 PPM or better<br>• Lower detectable limit of SO2 sensor shall be 0.009 PPM or better<br>• Precision of SO2 sensor shall be less than 3% of reading or better<br>• Linearity of SO2 sensor shall be less than 1% of full scale<br>• Response time of SO2 sensor shall be less than 60 seconds<br>• Operating temperature of SO2 sensor shall be 0°C to 60°C<br>• Operating pressure of SO2 sensor shall be ±10% | |

| | | |
|---|---|---|
| 5 | **Carbon Dioxide (CO2) Sensor**<br><br>• CO2 Sensor shall measure the carbon dioxide in ambient air<br>• CO2 Sensor shall have a range of at least 0-5000 PPM<br>• Resolution of CO2 sensor shall be 1 PPM or better<br>• Lower detectable limit of CO2 sensor shall be 10 PPM or better<br>• Precision of CO2 sensor shall be less than 3% of reading or better<br>• Linearity of CO2 sensor shall be less than 2% of full scale<br>• Response time of CO2 sensor shall be less than 60 seconds<br>• Operating temperature of CO2sensor shall be 0°C to 60°C<br>• 6Operating pressure of CO2 sensor shall be ±10% | |
| 6 | **Particulate Profile Sensor**<br><br>• Particulate profile sensor shall provide simultaneous and continuous measurement of PM10, PM2.5, SPM and TSP (measurement of nuisance dust) in ambient air | |
| | • Range of PM2.5 shall be 0 to 230 micro gms / cu.m or better<br>• Range of PM10 shall be 0 to 450 micro gms / cu.m or better<br>• Lower detectable limit of particulate profile sensor shall be less than 1 µg/m3<br>• Accuracy of particulate profile sensor shall be <± (5 µg/m3 + 15% of reading)<br>• Flow rate shall be 1.0 LPM or better<br>• Operating temperature of the sensor shall be 0°C to 60°C<br>• Operating pressure of the sensor shall be ±10% | |
| 7 | **Temperature Sensor**<br><br>• Temperature sensor shall have the capability to display temperature in °Celsius<br>• Temperature range shall be -10° to +80°C<br>• Sensor accuracy shall be ±0.3°C (±0.5°F) or better<br>• Update interval shall be 10 to 12 seconds | |

| | | |
|---|---|---|
| 8 | **Relative Humidity Sensor**<br><br>• Range of relative humidity sensor shall be 1 to 100% RH<br>• Resolution and units of relative humidity sensor shall be 1% or better<br>• Accuracy of the sensor shall be ±2% or better<br>• Update interval shall be less than 60 seconds<br>• Drift shall be less than 0.25% per year | |
| 9 | **Wind Speed Sensor**<br><br>• Wind speed sensor shall have the capability of displaying wind speed in km/h or knots<br>• Range of sensor shall be 0-60 m/s<br>• Accuracy of wind speed sensor shall be ±5% or better<br>• Update interval shall be less than 60 seconds | |
| 10 | **Wind Direction Sensor**<br><br>• Range of the wind direction sensor shall be 0° to 360°<br>• Display resolution shall be 16points (22.5°) on compass rose, 1° in numeric display<br>• Accuracy shall be ±3% or better<br>TR 6.70 Update interval shall be 2.5 to 3 seconds | |
| 11 | **Rainfall Sensor**<br><br>• Rainfall sensor shall the capability of displaying level of rainfall in inches and milli meter | |
| | • Daily Rainfall range shall be 0 to 99.99" (0 to 999.8 mm)<br>• Monthly/yearly/total rainfall range shall be 0 to 199" (0 to 6553 mm)<br>• Accuracy for rain rates shall be up to 4"/hr (100 mm/hr) or ±4% of total<br>• Update interval shall be less than 60 seconds<br>• 0.02" or (0.5mm) of rainfall shall be considered as a storm event with 24 hours without further accumulation shall end the storm event | |

| | | |
|---|---|---|
| 12 | **Barometric Pressure Sensor**<br><br>• Barometric pressure sensor shall have the capability of displaying barometric pressure in Hg, mm Hg and hPa or mb<br>• Range of barometric pressure sensor shall be 540 hPa or mb to 1100 hPa or mb<br>• Elevation range of the barometric pressure sensor shall be -600 m to 4570 m<br>• Uncorrected reading accuracy shall be ±1.0 hPa or mb at room temperature or better<br>• Equation source of the sensor shall be Smithsonian Meteorological tables<br>• Equation accuracy shall be ±0.01" Hg (±0.3 mm Hg, ±0.3 hPa or mb) or better<br>• Elevation accuracy shall be ±10' (3m) to meet equation accuracy specification or better.<br>• Overall accuracy shall be ±0.03" Hg (±0.8 mm Hg, ±1.0 hPa or mb) or better.<br>• TR 6.85 Update interval shall be less than 60 seconds | |
| 13 | **Noise Sensors**<br><br>• Noise sensor shall detect the intensity of the ambient sound in a particular area<br>• Noise Sensors shall be installed for the outdoor applications<br>• Noise sensor shall be able to identify the areas of high sound intensity ranging from 30 dBA to 120 dBA<br>• Noise sensor shall have resolution of 0.1 dBA | |
| 14 | Integration with ICCC platform, City Portal and Mobile applications | |

### 6.7.5 Emergency Call Box:

| No | Specification | Compliance (Yes / No) |
|---|---|---|
| 1 | ECBs to be installed one each at smart poles. | |
| 2 | They shall mostly be mounted on a pole in a housing with a canopy along with the ECB. | |
| 3 | The unit shall preferably have a single button which when pressed, shall connect to the ICCC or to the nearest/any of the control room having the local control console. | |
| 4 | These should also be capable of being used for Public Address. | |
| 5 | The PA control desk to be used for communicating with ECB | |
| 6 | Construction: Cast Iron/Steel Foundation, Sturdy Body for equipment | |
| 7 | Call Button: Watertight Large backlit PushButton, Visual Feedback for button press and call indication | |
| 8 | Connectivity: Ethernet | |
| 9 | Sensors: For tampering/ vandalism | |
| 10 | IP66 as per EN 60529, IK09 Protection EN 62262 or better | |
| 11 | Operating Temperature 0 to 60° C | |
| 12 | Speaking Distance as per site requirement | |
| 13 | Inbuilt Class D Amplifier, 99db SPL | |
| 14 | Minimum 3 Inputs and 2 Output relay contacts | |
| 15 | ECB should be able to make calls to the PA system | |
| 16 | Transmission Bandwidth 16000 Hz | |
| 17 | Front panel: stainless steel of minimum 3 mm | |
| 18 | Software Client for making/receiving Calls to ECB | |
| 19 | Automatic Volume Control, Call recording | |

### 6.7.6 IoT Gateway Specification

| Sl.No. | Description | Compliance (Yes / No) |
|---|---|---|
| 1 | Should be Linux / Windows latest version based operating system powered gateway or microcontroller based gateway. | |
| 2 | Gateway routers Single Board Computer running at 1.2GHz or better. Should have a 1GB RAM | |
| 3 | The receiver on the gateway should use a 867 Mhz or higher range and follow a multi hop mesh networking protocol | |
| 4 | The gateway should periodically update the central management server at ICCC about the diagnostics status of each sensor, LED, controller and display | |
| 5 | The gateway should use secure http protocol to communicate with the cloud server | |
| 6 | The gateway should be able to control the sensors or IOT devices | |
| 7 | The gateway should ensure the display data sync at all locations and floors where they are placed | |
| 8 | Should have Wi-fi on board, Ethernet connector on board | |
| 9 | Should have Bluetooth Low Energy (BLE) on board for future tech integration | |
| 10 | Should have multiple USB ports for communication via USB GSM/3G/4G dongle | |
| 11 | Should use micro SD port for loading your operating system and storing data | |
| 12 | Should have a Micro USB power source (up to 2.4 Amps) | |

### 6.7.7 Public Address System

| Sl.No | Minimum Specification | Compliance (Yes / No) |
|---|---|---|
| | **Make :** | |
| | **Model:** | |
| 1 | IP based PAS to be used for automated announcements or for paging announcements from ICCC or from the local area as per city traffic regulations. Should have 5 year warranty | |

| | | |
|---|---|---|
| 2 | Each site will have multiple speakers connected to one IP amplifier | |
| 3 | A local paging microphone ("Control Desk, Local") shall also be provided for doing local announcements | |
| | **Outdoor Horn Speaker** | |
| | **Technical Specifications** | |
| 1 | Speaker – Minimum 30 Watts | |
| 2 | Protection – IP66 and preferably IK10 or better | |
| 3 | Frequency Range – 350 to 10Khz | |
| 4 | Maximum Sound pressure level @1 m – 110 db or above | |
| 5 | Operating Temperature - -10 to + 55 C | |
| 6 | Construction – ABS Self Extinguishing | |
| | **IP PA Amplifier** | |
| | **Technical Specifications** | |
| 1 | **Amplifier: 120 Watt or above, Class D** | |
| 2 | Should have the capability to control individual PAS i.e. to make an announcement at select location (1:1)<br>or multiple locations (1: many). The PAS should also support both, Live and Recorded inputs | |
| 3 | Native IP connectivity, no convertors to be used | |
| 4 | 0 to 55 C Temperature rating for Amplifier | |
| 5 | Frequency Response: 70 Hz to 15000 Hz for Amplifier | |
| 6 | Minimum 2 Inputs and 1 Output relay contacts in Amplifier for connecting external beacon | |
| 7 | Speaker: Minimum 3 Speakers 30 W capacity per location | |
| 8 | Line Monitoring Facility for speakers | |
| 9 | 180-240 V mains input supply | |
| 10 | Compliant: CB/CE/EN/UL and BIS/IEC | |
| | **Control Desk** | |
| | **Technical Specifications** | |
| 1 | Should have the capability to control individual PAS i.e. to make an announcement at select location (1:1)<br>or multiple locations (1: many). | |
| 2 | Noise cancelling in built microphone with audio monitoring | |

| | | |
|---|---|---|
| 3 | Frequency range – 200Hz – 16Khz | |
| 4 | Display – 8 lines X 14 characters or better | |
| 5 | Connectivity- IP Based, POE powered | |
| 6 | Amplifier – Inbuilt 2.5W or better class D | |
| 7 | Operating temperature - 0 to 50C | |
| 8 | It should have RJ-45 Information Outlet, Minimum Dual Port (1 Uplink and 1 downlink) | |
| | **PAS Central Software** | |
| | **Specifications** | |
| 1 | The system shall deliver pre-recorded and live messages to the loudspeakers attached to them for public announcements. | |
| 2 | The system shall contain an IP based amplifier and uses power that could drive the speakers. | |
| 3 | The system shall also contain the control server that could be used to control/monitor all the components of the system that includes Controller, Calling Station & Amplifier. | |
| 4 | Central Server operating on 2 or more network interfaces 1Gbps or more data rate Compliance – UL 62368-1 | |
| 5 | Integration with ICCC and any other component if required | |
| | **PAS Central Server** | |
| | **Technical Specifications** | |
| 1 | Central Server operating on authorized operating system | |
| 2 | 2 network interfaces | |
| 3 | 1Gbps data rate | |
| 4 | Compliance – UL 62368-1 | |

### 6.7.8 City Public Wi-Fi

It is proposed to set up city wide public Wi-Fi across Puducherry City at the designated locations and connected to ICCC using the OFC proposed. The minimum expected Public Wi-Fi systems specifications are as follows. Outdoor AP should have controller license from day one and should be integrated with WLC at DC.

| Sl. No | Technical Specification | Compliance (Yes / No) |
|---|---|---|

| | | |
|---|---|---|
| | Make | |
| | Model | |
| 1 | Access Points proposed must include dual radios (2.4 GHz and 5 GHz) and should cover a distance of 250 meters in open area. Outdoor (IP67 rated or better) Wi-Fi6 802.11ax WLAN AP with Tilt bracket & PoE Injector | |
| 2 | The access point should be light weight and should support installations on walls or light poles without disturbing the aesthetics of the area. | |
| 3 | LED should be available for activity indication | |
| 4 | The Access Point should have auto-sensing 100/1000 Mbps RJ45 port. | |
| 5 | Must support 2x2 multiple-input multiple-output (MIMO) with Radio 1: 2.4GHz: 2x2 with 2SS or better and Radio 2: 5GHz: 2x2 with 2SS | |
| 6 | Should have dual Radios and should support 200 clients | |
| 7 | Should support 1 Gbps data rates on dual concurrent radio operations | |
| 8 | Should support 1024-QAM, and 20/40/80 MHz Channels | |
| 9 | Minimum conducted transmit power shall support 23 dBm or more on both 2.4 and 5 GHz. | |
| 10 | AP shall have integrated/ external antenna with minimum gain of 5dBi or more for 2.4 GHz and 5dBi or more for 5 GHz radios for Omni Directional Antenna device. | |
| 11 | The access point or the controller should support DHCP relay | |
| 12 | Must have a dynamic or smart RF management features which allows WLAN to automati-cally and intelligently adapt to changes in the RF environment | |
| 13 | WLAN Solution should support Mesh capabilities | |
| 14 | Along with a controller the Access Points should support fast roaming feature | |
| 15 | The access point should provide wireless IPS sensor support on both radios | |
| 16 | The WLAN Solution should support IP filtering | |
| 17 | WLAN Solution must support Application Visibility/Control | |
| 18 | WLAN Solution must support WPA3, WPA2 (CCMP, AES, 802.11i), WPA2 with open ac-cess public WLAN. | |
| 19 | Security solution must provide Rogue AP detection and protection | |
| 20 | System should support Authentication via 802.1X, mac authentication to local database or external RADIUS Server. | |
| 21 | For troubleshooting purposes, the administrator should have the ability to remotely packet capture and / or 802.3 frames from an access point without disrupting client access | |

| | | |
|---|---|---|
| 22 | WLAN solution should provide features that provides no touch AP discovery, adoption, provisioning and should be from same OEM | |
| 23 | WLAN solution should provide features that provides other management functions including AP management and configuration, firmware push and statistics reporting | |
| 24 | Must support telnet and/ or SSH login to Aps directly for troubleshooting flexibility | |
| 25 | Access point should have Integrated PoE and power injector Support | |
| 26 | AP shall Support Surge Suppression of up to 4 Kv. | |
| 27 | Operating Temperature: 0°C to 65°C and Operating Humidity up to 90% RH non-condensing. | |
| 28 | The Access Points should support WMM, WMM-UAPSD, 802.1p, Diffserv and TOS | |
| 29 | Support for Voice-over-wireless LAN (VoWLAN), quality of service (QoS). | |
| 30 | Access point must be supported for a minimum of 5 years by the hardware vendor with software updates and upgrades without additional cost. | |

### 6.8 Geographical Information System

It is envisioned that location-based GIS applications are critical for PSCDL and plays major role in disseminating information & data to stakeholders, visitors / tourists. Keeping view of this it is proposed to deploy integrated GIS Engine in ICCC Platform which can be further integrated with the MAPs like Google, Open Street Etc.

- It should be possible to visualize all the Assets (Sensor, Devices, Vehicles, Cameras, other city resources) on map.
- The Assets must be provided as layers with ability to switch these layers and visualize the assets of only selected layers.
- The GIS Maps should provide interactive visualization of travel time and traffic based on the sensor data and data ingested from 3rd party sources.

☐ GIS Platform shall support GIS Maps in following file format PDF, JPG, PNG, Vector PDF Map, Web Map Service (WMS), GeoJson defined by the Open Geospatial Consortium (OGC), Google Map-aerial; terrain, Bing Map, aerial, satellite, hybrid, ArcGIS/ESRI and Open Platform GIS Applications etc

☐ GIS platform should provide a picture-in-picture map view capability,

- Upon the availability of GPS positioning of a file, the user should be able to quickly alternate between the video and map view within the video player.
- The application must be able to ingest and present either a static location (e.g., for a fixed camera) or dynamic location (e.g., for mobile cameras) that allows users to validate the location where the video was recorded at the time of the event.

- GIS platform should support different layers like
- Ward Boundary Layer
- Zone Boundary Layer
- Street Boundary Layer etc.

### 6.9 Flood Sensors & Alert System

#### a) Proposed ICT Solution:

The storm flooding usually creates havoc and panic situation to the people residing in urban areas. High intensity rainfall events and flooding in urban areas are increasing every year. In the past two decades, migration to urban areas and rise in urban population in cities are experiencing a tremendous growth. Urban flood scenario is increasingly witnessed due to rapid urbanization in the city. Flood disaster is causing huge economic and social losses and has resulted in disturbed daily living for the public.

The proposed Flood Sensors & Alert System shall consist of

1. Flood alerts integrated with ICCC

The proposed methodology shall be developed for Urban Flood Sensors and Alerts System have two stages.

Stage 1: Rainfall and Runoff module Stage

2: Flood Alert

**The flood monitoring warning dissemination system:** It is proposed to install Flood Sensors. District at locations covering a geographical spread of 64 Sq. Km of city area. It is proposed to install Flood sensors in the identified areas like major canals and junctions.

The rain water level data (in millimeters) is recorded at every 15-minute interval by default and configurable as required and will be transmitted to the application server through telemetric GPRS enable system. These water level data shall be used to validate the depth of water obtained as an output from hydrologic model. The data on Temperature, Relative Humidity, Wind Speed, Wind Direction, Rainfall Intensity and amount of Rainfall from telemetric rain gauges and weather sensors are also being collected every 15 minutes and must be configurable as required. The near-real time data collected through the network shall be analyzed, and real time maps and reports shall be generated. A GIS and ground truth analysis along with historical flood event study in the city shall be conducted for finalizing and mapping of frequently flood vulnerable locations.

**Warning System – Published over ICCC**

The high intensity rainfall alerts and Flood forecast, warnings, Reports and Advises shall be disseminated through email, Social media, SMS to the mobile phones of Zonal heads, ward level officers of city corporation and also to all the connected line department in the city.

To disseminate the flood forecast and warnings to the city public, A dashboard shall be developed and integrated with ICCC would be the single interface which shall give the insight about urban flooding in the city. To disseminate weather related information, forecast and related advises directly to the general public a 24x7 to City Mobile app. The near-real time data collection, report generation and dissemination shall help the City administrative authorities in planning and executing disaster management and mitigation plans at microlevel and finally reducing the risks involved due to the flood disasters.

**Major scope of Early Warning and Dissemination System:**

1. Warning and Dissemination system development in collaboration with DRDM.
2. Mobile application for citizens & Dashboard development for administrators.
3. Integration with ICCC.

| S. No. | Description |
|---|---|
| 1. | Flood monitor must be capable to monitor flood levels in water bodies, streams and rivers |
| 2. | Flood monitoring application must be integrated with flood sensors and should be able to communicate with them. |
| 3. | Flood monitoring application must be web based with mobile app |
| 4. | The system should be able to send accurate and instant warnings to make informed decisions |
| 5. | The measured data should be sent to flood monitoring application |
| 6. | The flood monitoring application should have intuitive dashboards providing real-time monitoring information |
| 7. | The flood monitoring application must be able to integrated with various third party applications via APIs |
| 8. | The application must be able to do real-time continuous measurement |
| 9. | The application must be able to send instance notifications via SMS, Email and/or push notifications to a mobile app |

| | |
|---|---|
| 10. | The solution should also provide a mobile app working in at least Android or iOS |
| 11. | The application must provide intelligent analytics based on data captured |
| 12. | The application must have custom reporting capabilities |
| 13. | The application must be able to provide forecasts and trends |
| 14. | The application must be able to provide real-time notifications |
| 15. | The application must be able to be deployed on cloud or on-premise |

**Technical Specifications**

| Sl.No | Component | Description | Compliance (Yes / No) |
|---|---|---|---|
| | **Make:** | | |
| | **Model:** | | |
| | Body | | |
| 1 | Build | Polymer/Metal | |
| | **Range Options** | | |
| 2 | Max Range | 3 ft (91cm) | |
| | | 30 ft (9.1m) | |
| | | 50ft (15.2m) | |
| | **Communication Capability** | | |
| 3 | Wireless | | |
| | GSM | 2G/3G/4G/5G/NB-IOT | |
| | LoRa (Optional) | 865-867 MHz | |
| | Wi-Fi | 802.11 b/g//n (2.4GHz) | |
| | Wired | | |
| | Ethernet | 1-Port 10/100 FE PHY | |
| | RS485 | Modbus Protocol | |

| | | | |
|---|---|---|---|
| | **Power Options** | | |
| 4 | Input | 230V, 50 Hz | |
| | | | |
| | | Solar Powered | |
| | **Operating Environment** | | |
| 5 | Temperature | -0 to 60° C | |
| | Humidity | 0% to 100% RH | |

**6.10 City Surveillance System**

Primarily the function of police, these refer to operations to enhance the safety of the publicand provide necessary surveillance information to Police for both reactive and predictive policing. CCTV surveillance has been an important component across multiple cities with increasing usage of video analytics to aide police in spotting potential incidents and managing them as they happen.

**Key Issues**

The main challenges of surveillance in urban ecosystem are as follows:

- The rate of urbanization is increasing and with city growth comes an increase in crime and safety concerns due to concentrated populations
- Lack of surveillance cameras on a Pan City basis results in delays in crime detection and response
- Riots and vandalisms go undetected on a real time basis in lieu of absence of CCTV cameras at important places
- Lack of intra department real-time coordination, with voice and multimedia services
- Need for intelligent analytical capabilities by police
- Fragmented decision making due to lack of inter-departmental collaboration
- Citizens do not have access to a dedicated Emergency Response System

**Indicative Key Outcomes and KPIs**

- Supporting law enforcement agencies in 24x7 surveillance and monitoring
- Emergency Services Response Time: Average response time for Emergency Services o Number of CCTV cameras installed in the city per unit of road length
- Number of recorded crimes per lakh population
- Extent of crimes recorded against women, children and elderly per year o Location wise analysis of crimes in the city
- Creation of emergency corridor/ passage for passing of fire response / police/ ambulance teams
- Proactive identification of security issues leveraging intelligent analytics from the

surveillance system

- Supporting active response during emergency & disaster situations
- Providing secured access to video at any time from any network location
- Situation/Rule based alerts based on user inputs
- Automated response based on events including communication of alerts to relevant authorities like Fire, Hospitals, etc. for swift response in case of emergencies;
- Access to historic video data for investigative purposes
- Improved Crowd management and Security Breach handling

**Surveillance System**:

I. The Surveillance System shall be a fully distributed solution, designed for large multi-site and multiple server installations requiring 24/7 surveillance.
II. The solution shall offer centralized management of all devices, servers and users.
III. The Surveillance System should not have any limit on the number of cameras to be connected for Surveillance, Monitoring and recording. Any increase in the no. of cameras should be possible by augmentation of Hardware components
IV. The Surveillance System shall support distributed viewing of any camera in the system using Video walls or big screen displays
V. The Surveillance System shall support alarm management. The alarm management shall allow for the continuous monitoring of the operational status and event-triggered alarms from system servers, cameras and other external devices
VI. It should be possible to integrate the Surveillance System with 3rd-party software, to enable the users to develop customized applications for enhancing the use of video surveillance solution. (e.g., integrating alarm management to initiate SMS, E-Mail, VoIP call etc.)
VII. Rule Management: 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.
VIII. The system shall support rule-initiated actions such as:

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

**Video Management Capabilities**

The system shall allow an operator to view live / recorded video from any camera on the IP

Network. It should allow switching of video streams across the system.

ICCC/Police personnel shall have followed access to the video feeds of the cameras of their jurisdiction:

- Viewing rights to all the live Camera Feeds

- Viewing rights to the stored feeds
- Access to view Alerts / Exceptions / Triggers raised
- Trail Report on specific person / object / vehicle for a specific period / location
- Personalized Dashboard (depending upon grade of police officer)
- Accessibility to advanced analytics on recorded footages
- Advanced search based on various filters like alarm / event, area, camera, etc.
- Event Handling Capabilities:
- The camera shall be capable of recording an event as pre and post event images to on-board SD Media Card and share it with ICCC
- Events may be triggered using camera motion detection or from an external device input such as a relay.
- Support for various type of Logs such as System Log, Audit Log Alert Log Event Log should be available.

**Recording and Storage:**

- 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

Audit trail of the system to be maintained on permanent basis / as per the backup policydefined.

The Recording System shall run independently of the Video Management system and continue to operate in the event that the Management system is off-line.

**Investigation Scene Rebuilding**

- It should be possible to select the cameras for synchronized and simultaneous archived viewing. It should be possible to record the videos being rendered from these cameras into a single video. Such a single video should support up to eight such cameras in vertical, horizontal or overlay fashion. An easy feature of cloning the time stamp from one camera to multiple other cameras for synchronous archived viewing should be available.

- For quick investigation of the alerts, it should be possible to configure cameras in small functional group/s. In case of an alert in any one camera in the group, live video from other cameras in the group should be popped up automatically on the operator screen.

The system should enable tracking of the vehicle on a GIS map to locate any suspicious / identified vehicle. The Cameras should transmit quality video feed (clear, un-blurred, jitter free, properly lit, unobstructed, etc.).

The network design should ensure that the Packet losses are less than 0.5%. Integration with

ECB and Citizen App for SOS Management should be available. Integration with ICCC

Integration of all the IT systems and solutions deployed for the Surveillance management with ICCC should be through APIs

The alerts generated in ICCC should be handled in a coordinate manner with following;

a. Rule engine module for event/alarm handling
b. SOP (Standard Operating Procedure) tool for administrator to configure the SOP responses based on each alert.
c. Integration with the Incident Management system for the users to log in the incidents and the alerts, view the report from the module about the incidents etc.
d. Alert processing such as Acknowledging the alert, emergency response, SOP for the alert.
e. Connecting the next steps as per the SOP like informing Police\Fire departments based on the incident etc.

**Technical Requirements**

**c)Proposed ICT Intervention.**

The core objective is to create a supporting mechanism for the city agencies through 24x7 surveillance and
monitoring throughout the city as well as enable proactive identification of issues leveraging intelligent analytics from the surveillance system.

This module proposes implementation of a holistic City Asset Surveillance and Service monitoring system across the city including:

- Installation of PTZ cameras, Fixed Box cameras
- Centralized AI based intelligent Video analytics at data center for all the cameras installed
- Centralized AI based intelligent Video analytics for all the feeds received from Department of Police cameras, where these will provide the feed of CCTV cameras up to ICCC data centre.
- Develop a full-fledged command and control center for ensuring 24X7 monitoring and enabling effective action to be taken in case of law and order, Municipal services disruption , emergency disaster situations
- Integration with existing safety & surveillance systems already implemented like existing cameras installed, existing command & control centre as Police Station, etc.

It is proposed to have surveillance cameras and a dedicated video analytic system for incident monitoringbased on events. Further, with a view to share the video to other Stake Holders as well a dedicated VMS isbeing proposed with a distributed architecture.

### 6.10.1 Video Management System:General Requirements

| # | Technical Specification | Compliance (Yes/ No) |
|---|---|---|
| | **Make** :<to be provided by the bidder> | |
| | **Model** :<to be provided by the bidder> | |
| 1 | The VMS architecture should support centralized or de-centralized deployment. The VMS should be modular in design and should have components such as Management Server, Recorder Server, Streaming Server, Database Server and Integration Server. All hardware / software should have 5 year warranty' | |
| 2 | All the communication among the servers and clients should be secured and the VMS should support the SSL /TLS communication. It should have option of encryption with AES 128/256 and RSA 1024/2048 encryption standards. The VMS should also support secure communication between the camera and the server using SRTP/RTSP protocols. The VMS software should have been tested for vulnerabilities and should have been penetration tested as per the OWASP guidelines. Certificates from the CERT – IN empaneled auditor from the respective country of origin clearly indicating the encryption and VAPT test should be available. | |
| | | |
| | **System Architecture** | |
| 1 | The Video Management Software should be enterprise class application based on client-server architecture and should support unlimited cameras by augmenting recorder, management and database servers. | |
| 2 | The single master server should handle unlimited cameras, unlimited recording servers and unlimited users. | |
| 3 | The VMS should be compatible with Microsoft Windows/Unix/Linux Operating Systems. | |

| | | |
|---|---|---|
| 4 | The VMS should run on all the leading virtualisation platforms. | |
| 5 | VMS should be agnostic to database servers For example it should work on Microsoft SQL, MySQL, PostgreSQL and Oracle. It should also support NoSQL databases. | |
| 6 | VMS should have ONVIF Profile S, G , M and T compliance. Certificate to this effect should be available on the ONVIF website. | |
| 7 | The VMS should work on Commercially off the Shelf hardware and storage systems. | |
| 8 | The VMS should have an independent media streaming service which can be installed on a separate server to support scaling up of the clients without affecting the recorder server performance. | |
| 9 | The VMS should have manual and automatic mode of assigning cameras to the available recorder servers. In automatic mode, the cameras should be assigned based on the compute capability of the recorder server. In manual mode, the system should allow the administrator to assign the cameras to a recorder server. | |
| 10 | The VMS should provide multiple redundancy options in the platform for the following components: | |
| 11 | The VMS should have a provision for adding Master and Auxiliary Master Server to provide the native failover functionality. As a failsafe configuration, the system should work with limited functionality, without affecting the recording of cameras, even without the Master server. | |
| 12 | The VMS shall provide redundant recorder server for single or a group of recorder servers. In case of the failure of the Recording Server, the VMS should automatically assign the cameras on the failed recording server to other operational recording servers on the network. The camera recordings shall be synchronized back to the original Recording Server once it is back online. | |

| | | |
|---|---|---|
| 13 | Each recorder server should have independent storage configuration for local and network storage including NAS, SAN storage and Object Storage from popular cloud platforms such as Amazon AWS, Microsoft Azure, Wasabi, etc. Option of mirroring the storage of camera feeds should be available in the system. Back up storage on cloud/DC secondary storage for 60 days post local storage of 30 days. | |
| 14 | The VMS should have configurable DC-DR Functionality. The system should have configurable data retention policies for each DR setup to select what data to move and how long the data to be retained in DR before recycling the storage space. | |
| 15 | The VMS should have multiple options for selecting the business continuity requirements. Following options should be available in an easy to configure grid such as | |
| 16 | Data Replication Policy grid should allow selection of data such as video data, event messages and incident alerts, event video and the video segments tagged by the operator. It should be possible to select all or a group of cameras for such replication. | |
| 17 | The Business Continuity Policy should allow selecting all or a group of cameras which should switch over to DR for recording and viewing of videos. | |
| 18 | The user access policy should allow the granular control for various categories of users for functions such as login to the DR site, live video viewing and recorded video replay. | |
| 19 | The VMS should have federated architecture with centralised monitoring of the videos, video analytics and system health alerts. | |
| 20 | The VMS should have a unified API interface to expose various system functionalities, including, but not limited to, Analytics event alerts, live and archived video, PTZ control, system health alerts over HTTP protocol to external systems such as Integrated Command and Control Application, | |

| | | |
|---|---|---|
| 21 | Deleted | |
| 22 | The VMS should support unicast and multicast streaming for live viewing and recording functions. | |
| | **Centralized Management** | |
| 1 | The VMS should support multi-site deployments with centralized monitoring of the videos, video analytics and system health alerts. The centralised monitoring platform shall have the following features: | |
| 2 | Should support matrix view at full framerate with support for H.265, H.264, MPEG4 and MJPEG video compression. | |
| 3 | Drag and drop of cameras and live viewing of cameras from a mix of cameras from all the locations, group of locations, single location. | |
| 4 | Support digital zoom of the cameras from central site. | |
| 5 | Control remote PTZ cameras from central monitoring client application and digital zoom on remote fixed or PTZ cameras. | |
| 6 | Ability to pick and choose the selected cameras from remote sites. | |
| 7 | Ability to search and retrieve the archived video from the remote site with intelligent motion based search | |
| 8 | Download multiple video segments from multiple sites easily | |
| 9 | Multi-layer maps with support for static maps or GIS maps. | |
| 10 | System health dashboard for all connected systems. | |
| 11 | Central site management features with Role based User management, dynamic site management, video feeds aggregation, event information management and distribution, system administration with full audit trail and logs | |
| 12 | Shall support secure and encrypted transmission of video files to cloud as per requirement. | |

| | | |
|---|---|---|
| 13 | Receive alerts from the remote site with event metadata received first and then the users can request image and video clips to ensure effective bandwidth management. | |
| 14 | Dashboard of all connected devices and the health status of the devices. | |
| 15 | Resource utilization of the system and statistical reports for the remote sites. | |
| 16 | Camera SLA report with camera connection and uptime information | |
| 17 | Scheduling of reports | |
| | **Cloud Readiness of the VMS** | |
| | | |
| 1 | The VMS should be cloud deployment ready and agnostic to the cloud environment - be it a private, public or a hybrid cloud. It should work on the bare metal servers of the cloud solution providers with in-built intelligent video streaming and resource orchestration services. The VMS should allow using various tiers of object storage to optimize the storage requirements and data retrieval times. The VMS should be capable to integrate with Video Analytics functions powered by the Artificial Intelligence and Deep Learning technologies on cloud infrastructure. | |
| 2 | The VMS should allow adding network storage location by giving path to the network storage device and authentication credentials. This feature should also allow adding storage locations on the cloud platforms such as AWS, GCP, Azure, Wasabi etc. | |
| 3 | The VMS should have native support for Object Storage from popular cloud platforms such as Amazon AWS, Microsoft Azure, GCP, Wasabi, etc. The system should support pushing the recorded video file on a definable schedule to the Object Storage. | |
| | **Information Security** | |

| | | |
|---|---|---|
| 1 | The system should have multiple levels of authentication and access control mechanisms: A. Role based Authentication<br>B. Session control using encrypted tokens<br>C. User stickiness to a particular hardware workstation<br>D. Dual Factor Authentication with provision to receive the OTP via text message on the registered mobile of the user and through the registered email address<br>E single sign-on based on LDAP and Active Directory. | |
| 2 | System configuration data should be stored in encrypted files with checksum and there should be user selectable encryption algorithms such as MD5, RSA and SHA. | |
| 3 | The data at rest should be stored in a encrypted format. | |
| 4 | The videos downloaded from the system should be watermarked with an option to export with non-tamper format. | |
| 5 | The software should maintain audit trails of user interaction | |
| 6 | The system should have built-in audit tool which generates reports such as report describing health of network connectivity and the throughput of storage devices against each server. | |
| 7 | The software should be OS agnostic. | |
| 8 | Data in the system should encrypted with either MD5 or SHA256 cryptographic hash functions and video data are stored in encryptedformat when at rest | |
| | **Storage & Recording Functions** | |
| 1 | The VMS should allow creation of customised recording profile with day and hour granularity and an option to add recording profile for special days. It should be possible to create unlimited recording schedules with option of selecting various streams, Frame rate and compression available from the cameras. The recording configuration should have the following options: | |
| | - Redundant recording | |

| | | |
|---|---|---|
| | - Edge recording | |
| | - Selection of SRTP or RTSP protocols | |
| | - Recording schedule based on motion only recording, FIFO and specific retention period. | |
| 2 | Each recorder server in the system should have independent configuration for database and storage servers. | |
| 3 | The VMS should periodically check the gaps in live recording of the cameras and should check with the on-board storage of the camera. In case of a gap, the VMS should synchronize the video recording on the on-board storage with the VMS storage. Such synchronized storage should be displayed with different color for quick attention of the operator. | |
| 4 | The event and the associated video clips should have the facility to be marked for non-delete flag to protect the event and metadata from being wiped out by the data retention policy. Additional option should be available | |
| | not to delete the event till a specific date. After that, the event should be wiped out as per the data retention policy. | |
| 5 | The system shall have the capability of recording video at a lower frame than is received from the camera (frame rate reduction mode). | |
| 6 | VMS should support H.265, H.265+, H.264, and MJPEG streams for both Live view and Recording. | |
| 7 | The client should offer below three options for operator-specific recordings: | |
| 8 | Record Matrix Videos: Record a matrix of the videos being displayed on the screen. | |
| 9 | Record Stitched Videos: Stitch and record the stitched video matrix either in horizontal or vertical direction. Any number of cameras can be added in the stitched video. | |
| 10 | Record Screen: Record the entire screen of the operator including any matrix of cameras visible and other desktop activity being performed by the user outside of the VMS client. This functionality can be achieved using in-built or third party tools. | |

| | | |
|---|---|---|
| | **General VMS Functions** | |
| 1 | The system, once configured, should work seamlessly, without any configuration, after the server/s pass through the power on-off cycle. | |
| 2 | The VMS should offer feature rich desktop client for Microsoft Windows/MAC /Linux OS. It should also have a browser agnostic web client and mobile client available on Android and IOS platforms. | |
| 3 | The VMS should have site-wide, hierarchical tree of cameras visible to all the operators with appropriate rights and should also have operator specific, unlimited hierarchical grouping of cameras as per the area or functions. | |
| 4 | The VMS should allow grouping of cameras as per the Group Name or Location for flexibility of camera management. | |
| | **VMS User Management & Administration** | |
| 1 | The VMS should support Microsoft Active Directory or Lightweight Directory Access Protocol (LDAP) for enterprise wide user management. | |
| 2 | For additional security and accountability, it should be possible to restrict the operator to a particular workstation. | |
| 3 | The VMS should allow addition of new user based on five different profiles. It should be possible to assign various configuration and operation functions for each profile as required in a user-friendly matrix view. | |
| 4 | The VMS should seek answers for the multiple selectable security questions to each user logging-in for the first time. The answers to the security questions should be validated by the VMS in case the user wants to change the password. The VMS should not allow using the last three passwords while selecting the new password. | |

| | | |
|---|---|---|
| 5 | The system should have collaborative vigilance functions. It should offer chat room for exchange of information such as text messages, user selectable files, archived video link, camera layouts, incident snap, clip and VA alerts for collaboration among the operators. The chat window should show color coded status for messages which are sent, delivered and read. The administrator should have access to all the messages being exchanged among the operators. To assist in collaborative investigation of an event, the operator should have the function of sharing the camera matrix with a mix of live as well as playback videos to the fellow operators or to the Supervisor. This function should also allow sharing an event along with event video, stitched video of a matrix recorded on the operator workstation, any other video clips received from external sources, etc. | |
| 6 | The system should allow camera permissions to the users based on individual camera, group of cameras and all cameras. | |
| 7 | VMS should allow the Administrator to import any active users screen on the video pane by drag and drop to watch the operator's activity on-line in a matrix layout. Operator should be able to drag a user group on the screen to watch their desktop activity at one go. Administrator should be able to record the matrix view for the desired duration if required. | |
| | **VMS Client and Operator Functions** | |
| 1 | The unified VMS client should provide all the configuration functions for Video Management Server, Video Recorder Servers, Storage and Video Analytics for creating rules. | |
| 2 | The VMS should allow multi-monitor support for the client workstation. It should allow setting up of different layouts on different monitors such as camera matrix, map view, VA alerts view, for example. | |
| 3 | It should be possible to select cameras for synchronised and simultaneous archive viewing. It should be possible to record the videos being rendered from these cameras into a movie clip. This operation should be possible in a matrix recording or stitched recording options. | |

| | | |
|---|---|---|
| 4 | The VMS should retain the VMS client screen state (including Video Analytics alert window, message window, Video Matrix, etc.) in case of an accidental shut down of the machine and should offer the exact same screen to the operator upon logging back into the system. | |
| 5 | The client should have configuration option to view the live videos directly from camera or from the media server. In case of the video feed coming directly from the camera, the live view should be available even if the servers are not reachable. | |
| 6 | The live view window of a particular camera should allow the operator to view the archived video. The operator should be able to go back in the time by selecting quick shortcuts for 5, 10, 20, 30 seconds, 1, 5 minutes, 1, 5 hours. Operator should also be able to select the exact date and time though the calendar widget. | |
| | **Virtual Workspace Functions** | |
| 1 | The VMS should present the functional dashboard of the system to the operator like a virtual workspace. The Dashboard should allow the operator to view and manage the cameras, operator specific camera matrix views as per the functional requirements, map views for the geo-aware vigilance, video analytics alerts, and information and alerts from the integrated devices. | |
| 2 | When the operator drags a camera group on to the virtual workspace, the VMS should dynamically select and display the number of tiles in the virtual matrix based on the number of cameras available in the group. | |
| 3 | Deleted | |
| 4 | It should be possible for the operator to configure the virtual workspace using the virtual matrix by assigning the matrix to display alerts and information from a combination of systems such as live and archived videos, | |
| | **Map Functions** | |

| | | |
|---|---|---|
| 1 | The VMS should support geo-aware vigilance with the use of layered maps using standard picture files, City GIS maps and online maps such as Google, Bing, OpenStreetMap's. It should be possible to drag and drop the cameras on the map for easy navigation. In case of multi-layered maps, the system should show all the available maps in a drop down list for easy selection. The VMS should allow viewing of live and playback videos, event notifications on the map view with event tracking functionality from multiple cameras. | |
| 2 | The VMS should support a geo-fence based vigilance functionality. The VMS should show the cameras within the selected geo-fence. It should be possible to associate a base camera within the geo fence with other neighborhood cameras to form a group for situational awareness of the neighborhood. In case of an alert in the base camera, live feeds from all the cameras in the group should be popped up. The window should show the live video and the alert video clip from the base camera where the alert is generated, the neighborhood cameras and the location of the incident on the map within the same window. | |
| 3 | It should be possible to export the map view to the desired screen in case of multiple screens available. The system should show all the available screens in a dropdown. | |
| 4 | The system should have an easy to use pencil tool /similar easy to use feature to quickly select the cameras on the map (static or GIS) for simultaneous viewing for both live and playback videos. | |
| 5 | It should be possible to forward the map view including the camera streams, live or playback to another user in the system for easy collaboration of geo-spatial viewing. | |
| 6 | The map view should allow searching of the camera by name or IP address to quickly find out the camera on the map. This is useful in emergency situations when an operator wants to pull the live video on the screen quickly. | |
| 7 | The VMS should show event notification from the cameras on the map itself. The operator should be able to click on the event notification of a particular | |

| | | |
|---|---|---|
| | camera on the map and the VMS should open the event window on the operator screen. | |
| | **Investigation and Tracking Functions/Video Synopsys Tool.** | |
| 1 | The operator should be able to recreate a scene by arranging the cameras and their respective time-stamped archived videos. The operator should be able to save such a recreated scene through collection of cameras for quick access and should also be able to share such collection to the other users or supervisors. | |
| 2 | The operator should be able to associate all neighborhood-view cameras to a base camera for tracking an activity for investigation. When an alert is generated in the base camera, the VMS should pop up a screen widget/ similar easy to use interface which shows live video of the base camera, playback of the base camera from the pre-buffer of the alarm and live view of the associated cameras along with the map view. This entire screen should be used for forensic investigation and should be recorded as all-in-one evidence for export and sharing. This event window should be configured to pop-up on the event hot-spot monitor. | |
| 3 | The VMS should allow tracking the movement of a suspect or a motorcade through live view from the cameras on the map by using a simple pencil tool/similar easy to use feature on the screen. With the tool/feature, the operator should be able to draw a line on the map touching one or more cameras and the cameras touched/selected by the tool/feature should appear for live view on the screen. | |
| 4 | The VMS should have PTZ camera control options in a separate PTZ control widget. The widget should show all the available presets, allow pan, tilt and zoom of the camera, and also allow creation of a preset. It should also support 3-axis USB joysticks for PTZ camera control. | |

| | | |
|---|---|---|
| 5 | The VMS should allow creation of a PTZ tour based on the presets available from the PTZ camera. The VMS should allow setting the hover time for each preset depending on the functional requirement. It should be possible to attach such a tour to any of the associated video analytic use case. The creation of a PTZ tour should be the function of the VMS without any external dependency | |
| 6 | The system should offer multiple playback mechanisms (including single frame playback) for ease of auditing and investigation, including zooming and panning simultaneously. | |
| 7 | The system should allow ease of tagging of exceptions/audit/investigation findings and creating an institutional library of the same for future reference. | |
| 8 | The VMS on integration with Video Analytics software should provide forensic search operation based on the powerful attribute search analytics feature. The operator can select any person in the camera field of view and search for the appearance of the selected person based on the attire attributes in the selected cameras for the selected duration. The attribute search should show persons with matching attributes in a grid. It should be possible to click on any match to view the playback video of that instant. | |
| 9 | The VMS on integration with Video Analytics software should allow the operator to select an unidentified object with a selection tool on the screen to identify who left the object in the scene. The analytic should search the video and show the video frame when someone left the object in the scene. | |
| | **Event and Alert Functions** | |
| 1 | The VMS should allow sending the event alert to the designated person or a group of designated persons through SMS or Email. These rules should be available with configurable priority of the alert. | |
| 2 | The VMS should allow monitoring of archived video of the selected camera under categories such as events, motion or continuous recording. The VMS should also show a report of cameras indicating recording status for the selected duration, critical video data and Incident Video data. | |

| | | |
|---|---|---|
| 3 | Live events should be shown on the event hotspot monitor and retained for the configured time. This should alert the operator of the current events. The unattended events should be queued to be taken up by the operator one-by-one later. | |
| 4 | The events dashboard should be available with multiple filter parameters such as - by camera, by use case, by camera groups, and the easily selectable duration such as today, last 7 days, last 30 days, and calendar widget, etc.. Reports should be exported in formats such as excel and CSV. The dashboard should also have the graphical representation of the reports in terms of the bar charts and pie charts. | |
| 5 | It should be possible to pass the specific alarm intimation to specified users rather than sending all alarms to every user. | |
| | **Camera Management and Viewing Functions** | |
| 1 | VMS should allow configuring the cameras in multiple groups independently. It should be possible to assign all, single or multiple groups to operators. At least 100 such groups should be possible with an unlimited number of cameras in each group. It should be possible to assign camera/s to single or multiple groups simultaneously. | |
| 2 | The operator should have the ability to use digital zoom where the zooming is performed on any number of cameras simultaneously - for live and playback videos. This functionality should be the default for fixed cameras. The use of digital zoom should not affect the recording. | |
| 3 | Client viewer should allow the same camera to be viewed on multiple display tiles; one may be digitally zoomed, or on high resolution stream. | |
| 4 | The VMS should allow restricting the users who are authorized to view the camera feeds to a single camera and to the group of cameras. | |
| 5 | The system should allow creation of operator specific camera groups comprising of live video views and archived video views. It should be possible to share such groups with other users and administrators. The recipient of such information should be able to see the exact layout of live view and archived video view. | |

| | | |
|---|---|---|
| 6 | The camera matrix for live and archived videos should support simultaneous viewing of cameras in multiple grids ranging from 2x2 to up to 8x8 and should allow operator to configure as per requirement . A simple click should allow enlarging any of the cameras in the multi-screen displays into a full screen and full resolution display of the camera. On clicking again on the enlarged display, multi-screen display should reappear. | |
| 7 | The VMS should allow the operator to create multiple camera matrix comprising of live and archive videos from multiple cameras and create a sequence of such multiple matrix to be displayed in a cycle with configurable display duration for each matrix. It should be possible to export such a sequence to any of the connected cameras or the video wall. | |
| 8 | It should be possible to drag and drop cameras from the camera directory to the display screen. | |
| 9 | The Client Viewer should offer the capability of browsing recordings from cameras on the same panel where other cameras are displayed live. | |
| 10 | VMS should have smart management of video streams from camera. It should select lower resolution stream when viewed in a matrix and should automatically switch to the high resolution stream when viewed full screen. | |
| 11 | The Client Viewer should display a time line for each camera to represent recorded video sequences. The Client Viewer should indicate whether the video was recorded due to motion activation or recorded without motion or pre and post alarm video. The time line band should be highlighted based on the camera view selected in the display. | |
| 12 | The camera type should be shown with specific camera icon and the state should be displayed in different colours to indicate whether the camera is in live mode, in recording mode, in stopped mode or video analytics alerts. | |
| 13 | From the Client Viewer it should be possible to: | |
| 14 | Bookmark an important event for easy search and retrieval later. | |
| 15 | Bookmark the display layout with selected distribution of cameras across the panel with a mix of live and archived video. | |

| | | |
|---|---|---|
| 16 | Use sound notifications and external annunciators for attracting attention to detected motion or events. | |
| 17 | Get quick overview of sequences with detected motion. | |
| 18 | Get quick overviews of detected alerts or events. | |
| 19 | The Client Viewer should have the capability to receive multicast streams if a preset number of clients are requesting the same live view camera. The Operator should have the option to configure the system to always receive unicast streams at the discretion of the system administrator. The system should have the capability to detect if the network becomes unreliable and to automatically switch to unicast to ensure that the operator is able to receive video. | |
| | **The Client Viewer should have the following audio functions at specified locations.** | |
| 1 | The Client Viewer should allow an operator to play live audio from a camera's microphone and play back recorded audio. The audio on/off option should be available on the camera display matrix for each camera. | |
| 2 | The operator should have a "press to talk" option which should send the microphone input from the operator out to the speaker attached to the camera. The microphone button should be available on the camera display matrix for each camera. | |
| 3 | The VMS should have integration with the IP speakers and should be able to send the audio message for the selected IP speaker. | |
| 4 | It should be possible to export the video clip of selected duration for export. The VMS should allow export of a single video clip or multiple clips to a cart. For downloading a single clip, it should have encryption option for the exported clip and should ask to select the export format such as AVI, MJPEG, MP4 and AVF. | |
| | **Video Export Functions** | |
| 1 | It should be possible export the video clip in a tamper-proof format by adding watermark and encryption to the exported video to verify the authenticity of the video. | |

| | | |
|---|---|---|
| 2 | Export of single frame of video in BMP, GIF, TIF, JPG and PNG formats and export of video files in commonly used video formats and Print images, with optional comments. | |
| 3 | VMS should allow the users to download multiple segments of the video from single or multiple cameras from the archive with an option to tag each downloaded segment with text messages. The Video segments should be downloaded in a single folder along with excel spreadsheet where details of each of the video segments are listed as hyperlinks to the exported video. | |
| 4 | The Client Viewer should allow an operator to export audio together with video in the AVI or other standard format. | |
| | **Web and Mobile Clients** | |
| 1 | The VMS should have web client which should work on all the leading browsers immaterial of the operating system. | |
| 2 | The VMS should have mobile client for Android and IOS platforms and should be available from the respective Play Store and App Store. | |
| 3 | The web application should support HLS and MJPEG streaming. | |
| 4 | It should be possible to track mobile app users on GIS map from a central location. The Mobile App user should be able to track the other Mobile App users on the GIS Map. | |
| 5 | It should have view link sharing within authenticated users from the web application. The VMS web interface user can forward video link URL by email to another user. | |
| 6 | The mobile client should allow uploading of the snaps and video clips from within the application to the central VMS. The central VMS should show the uploaded snaps and videos from the mobile users. | |
| 7 | The VMS should have push notifications for the alerts for the mobile and web clients to push the event notifications from the central VMS. The alert notification should also stream the video clips associated with the alert. | |
| | **Health Monitoring, Audit Trail, Problem Reporting Functions** | |

| | | |
|---|---|---|
| 1 | The system should support CCTV video footage auditing & investigation to reduce the data size for disaster recovery purposes , Create a well-categorized searchable institutional library & Report in PowerPoint/Word/PDF/Excel | |
| 2 | The system should have capability to sit as a 'stack' over any live or recorded video feed from multiple cameras and convert the same into images by capturing screenshots in the background, at an interval of one or more seconds, thereby reducing the number of frames to be viewed, i.e., creating a summary without missing any scene, and creating huge reduction of data size for disaster recovery | |
| 3 | The desktop client should show system health dashboard with vital system parameters for Database Server, Recorder Servers, Local Workstation and all the available storage locations. The client should show real time CPU Core Usage and RAM Utilization. | |
| 4 | The system should be able to generate incident/audit finding reports in PowerPoint that deliver data analytics (business intelligence) in Excel. | |
| 5 | The system should be able to import any kind of photo/image and offer a template for easy sharing of mugshots in Word/PDF. | |
| 6 | The system should allow ease of tagging of exceptions/audit/investigation findings and creating an institutional library of the same for future reference. | |
| 7 | The VMS should show the real time workstation CPU and Memory utilization on the screen along with the color changing System Health Status icon which indicates real time health updates from the surveillance system. | |
| 8 | The systems should have following features for reporting and system health: | |
| 9 | Camera SLA report showing uptime, recording percentage, recording status, critical events, incident video, etc. | |
| 10 | Detailed listing of all active or incoming alarms with filtering options time period, alarm source, operator and alarm state. | |
| 11 | Generate audit trail reports by incident. | |
| 12 | Give full audit trail of the user activities in the system. | |

| | | |
|---|---|---|
| 13 | The system log should be searchable by Level, Source and Event Type. | |
| 14 | The Audit Log should record remote user activity searchable by User name, Audit ID, Source and Location | |
| 15 | The Alert Log should record alerts triggered by rules and searchable by Alert type, Source and Event type | |
| 16 | The Event Log should record event-related information searchable by Service Name, Source and Event Type | |
| 17 | The Rule Log should record rules in which the Make new <log entry> action been specified (searchable by Service name, Source, Event type and Rule name) | |
| 18 | The VMS should allow raising support tickets from the Help menu. It should be possible to attach a screenshot of the error for effective communication of the problem being reported. | |
| 19 | The VMS should allow recording of the desktop activity into a movie clip to effectively explain the problems being faced to report the support related issue. | |
| 20 | The VMS should allow the administrator or an operator to record an activity happening in multiple cameras into a single movie clip which help in improving the security function and the security SOP creation activity. | |
| 21 | The VMS should allow the administrator to record the screen activity into a movie clip to create visual manual to explain various functionalities to the new users for training purpose. | |
| 22 | API and Integration Functions | |
| 23 | The VMS should be able to integrate with external devices such as various types of Cameras, Access Control, Perimeter Intrusion Detection, IP Speakers, , etc. | |
| 24 | The system should be able to push the images to the user's cloud. Such images can also be used to train AI models. | |

| | | |
|---|---|---|
| 25 | The VMS should show integrated devices in a list on the operator screen. The events generated from the integrated devices should be available for viewing. | |
| 26 | The VMS should allow easy configuration options to connect to the external devices for integration and should also have granular control on the alert types to receive based on the information exposed by the external devices through the API or SDK calls. | |
| 27 | The VMS should provide an Open API based integration gateway without any additional cost or licensing. The API should be able to send the information about various aspects of the VMS system to the external application requesting the information. The API should provide functions such as: | |
| 28 | Find servers, registered users, alert types and alerts, available channels, channel ID, count, status, type, PTZ cameras and PTZ controls, get event count, event search, event snap ID, event video clip, camera live video play, playback video play, trigger an event, activate or suspend a device, etc. | |
| 29 | The API should support HTTPS based REST API with cryptographic controls to establish secure connection between web and mobile users. | |

**Video Analytics :**

**Below functionalities can be achieved on integration of VMS with in-built/third party VA.**

- System shall have the capability to provide various alarms & triggers and should notified if any incidence/violation happens.
- The System shall be a real-time video analytics engine that utilizes advanced image processing algorithms to turn video into actionable intelligence.
- The system shall provide configurable detection zones and lines to detect events of interest, Detection zones define an area of interest and Detection lines define a perimeter instead of a region.
- The system shall facilitate creating multiple zones and lines in a single scene to trigger various alerts
- The system shall allow the configuration of applicable rules and manage them
- The system shall also enable editing the Zones and lines to the desired shape or size.
- The triggers generated by the applied rules shall provide visual indicators to identify the event. Such as a Green colored Bounding Box changing the Bounding Box colour to Red on event

- The system shall enable detecting rules in the defined areas (zones/ lines)
- The system shall provide functionality for configuring timelines for various events such as Crowd Detection, Loitering Detection etc.
- The system shall allow classification of different objects like animals, vehicles and people
- VAS should allow to add, edit, delete or disable and enable Policies.
- System shall have a sophisticated rule-based engine with powerful analytics capabilities that provides automatic event notification.
- Proposed system needs to have the capability to deploy intelligent video analytics software on any of selected cameras. This software should have the capability to provide various alarms & triggers.
- Following video analytics and features should be supported based on licensing:

| |
|---|
| **Perimeter Trip wire/Crossing Virtual line** |
| • Should capture zoomed image of the object causing the Perimeter Breach and raises appropriate alarm. |
| • Should also stores the time duration between the pre and post event of the Perimeter Breach. |
| • Should have the Option Drawing Single/Multiple Lines along with Defining Logic for the Multiple Lines. |
| **Loitering Detection** |
| • Should automatically detect objects/Person that has moved continuously within the camera field of view for a configurable period of time. |
| • The VA System should have the capability to detect loitering incidents in crime hotspot areas. |
| **AI Based Unattended Object Detection** |
| • Should detect and generate an alert highlighting Suspicious detected when carried into the scene and planted by a person as well as when dropped or thrown into the scene for a Period of time that is considered suspicious by the user. |
| • Should be able to Detect Multiple object that are left Stationary in a Scene, the System shall be to detect multiple objects each with its own timer as per the predefined detection time. Alarms of each Individual Objects Abandoned shall be alerted Individually. |
| • The VA should be intelligent to understand the existing objects within the camera field of view and should generate an alert only when a new object is detected for more than the preconfigured duration of time. |
| **AI Based Classification of objects like person, vehicle, or animals** |
| • VA can perform object classification once the camera has been calibrated. Object classification is based on properties extracted from the object including object area and speed. |
| **AI Based Tripwire/intrusion detection** |
| • Detection of intruder entering/exiting a given area of interest. |

| |
|---|
| • Once verified and confirmed by operator that it is a rouge object, the system shall be able to track the person across various cameras and to find the origin of such person. |
| **AI Based Camera Tampering Detection** |
| • 1. Alert to be generated when camera is tampered by way of change of Field of view of camera, blurring of view, blocking of view by cloth or obstruction, camera disconnection, blinding of camera by laser or flashlights. |
| • 2. Once alert is generated, the incident should be flagged, and system should have the capability to trace the person responsible for the sabotage in other cameras and send notification to concerned authority. |
| **AI Based asset protection, Grouping, crowding and Person waving.** |
| **AI based no helmet detection, Triple ride detection, no seat belt detection and accident detection** |
| **System must be capable to support below use cases**<br>**Garbage Bin Full and Cleared Detection**<br>**Detection of Debris on the Road**<br>**Detection of Stray Animals on Road** |
| **Attribute search Analytics (Search person by Dress , Attire, appearance , age etc)** |
| **Video Summarisation** |

**6.10.2 City Surveillance fixed Camera Specifications**

| # | Parameter | Minimum Specifications or better | Compliance (Yes / No) |
|---|---|---|---|
| | Make: | | |
| | Model: | | |
| 1 | Image Sensor | 1/2.8" 2MP Progressive Scan CMOS or better | |
| 2 | Day/ Night Operation | Yes with IR Cut Filter | |
| 3 | Minimum Illumination | Color: 0.015 lux or better ; B/W 0 Lux with IR | |
| 4 | Lens | Auto IRIS 2.8-12 mm (+/- 1mm) Motorized Varifocal Lens or better | |
| 5 | Electronic Shutter | 1/10 to 1/12,000s or better | |
| 6 | Image Resolution | 1920x1080 or better | |
| 7 | Compression | H.265 or better | |
| 8 | Frame Rate and Bit Rate | Upto 60 fps with Controllable bit rate, frame rate and Maximum Bit rate | |

| | | | |
|---|---|---|---|
| 9 | Video Streams | Minimum 3 Nos, individually configurable simultaneous streams in H.265 @ 1920x1080 & upto 60 Fps | |
| 10 | Angular Field of View | H: 119.5°(Wide)~27.9°(Tele), V: 62.8°(Wide)~15.7°(Tele), T: 142.1°(Wide)~32.0°(Tele) | |
| 11 | Motion Detection | Built in 8 point polygonal zones areas in the video stream. | |
| 12 | Lens/ Barrel Distortion Correction & Corridor View | Built in feature required | |
| 13 | Wide Dynamic Range | 150 dB or better | |
| 14 | IR Viewable Length | 50 Meter or better (Built in or External) IR | |
| 15 | Alarm | 1 Input & 1 Output | |
| 16 | Audio In | Selectable(Mic in/Line in), Supply voltage: 2.5VDC(4mA), Input impedance: 2K Ohm | |
| 17 | Audio Out | Line out, Max. output level: 1Vrms | |
| 18 | Audio Compression | G.711 u-law /G.726 Selectable<br>G.726(ADPCM) 8KHz, G.711 8KHz<br>G.726 : 16Kbps, 24Kbps, 32Kbps, 40Kbps<br>AAC-LC : 48Kbps at 16KH | |
| 19 | Analytics | Can be achieved via VMS and VA:<br>Defocus detection, Directional detection, Fog detection, Face detection, Motion detection, Digital auto tracking, Appear/Disappear, Enter/Exit, Loitering, Tampering, Virtual line, Audio detection, Sound classificationand others. | |
| 20 | Event Triggers | Alarm input, Motion detection, Analytics, Network disconnect | |
| 21 | Event Actions | FTP, HTTP, Email notification, Edge Storage, Alarm Output, Handover | |
| 22 | Edge Storage | Micro SD/SDHC/SDXC minimum of 512GB capacity or better | |
| 23 | Protocols | IPv4, IPv6, TCP/IP, UDP/IP, RTP(UDP), RTP(TCP), RTCP,RTSP, NTP, HTTP, HTTPS, SSL/TLS, DHCP, FTP, SMTP, | |
| | | ICMP, IGMP, SNMPv1/v2c/v3(MIB-2), ARP, DNS, DDNS, QoS, PIM-SM, UPnP, Bonjour , LLDP, SRTP | |
| 24 | Security | HTTPS(SSL) Login Authentication, Digest Login Authentication, IP Address Filtering, User access Log 802.1X Authentication(EAP-TLS, EAP-LEAP) | |

| | | | |
|---|---|---|---|
| 25 | Firmware Upgrade | The firmware upgrade shall be done though web interface, The firmware shall be available free of cost | |
| 26 | Interface | RJ 45, 100 Base TX or better | |
| 27 | Memory | 1024 MB RAM, 256 MB Flash or better | |
| 28 | Enclosure | IK10 & IP67 or Nema4x or better | |
| 29 | Power requirements | Vendor to specify, POE Preferred | |
| 30 | Operating Temperature | -30 °C to 55 °C or better | |
| 31 | Operating Humidity | Max 90% RH or better | |
| 32 | Certification | UL, CE, FCC,BIS, | |
| 33 | Application Programmers Interface | 1. The interface shall be available for integration with 3rd party analytics and applications in public domain<br>2. ONVIF | |
| 34 | Deleted | | |
| 35 | Mount | Wall Mount/ Pole Mount | |
| 36 | Warranty | Minimum 5 Years | |
| 37 | Defog | Available | |

### 6.10.3 City Surveillance PTZ Camera Specifications

| S. No. | Description | Desired Parameter | Compliance (Yes / No) |
|---|---|---|---|
| | Make: | | |
| | Model: | | |
| 1 | Imaging Device | 1/2.8" 2MP Progressive scan CMOS or better | |
| 2 | Resolution | 1920x1080, 1280x1024, 1280x960, 1280x720, 1024x768, 800x600, 800x448, 720x576, 720x480, 640x480, 640x360, 320x240 or better | |
| 3 | Max. Framerate | H.265 or better/H.264: Max. 60fps/50fps(60Hz/50Hz) MJPEG: Min. 30fps/25fps(60Hz/50Hz) | |
| 4 | Min. Illumination | Color: 0.02Lux(F1.6, 1/30sec) BW: 0Lux(IR LED) | |
| 5 | Focal Length (Zoom Ratio) | 4.45~222.4mm or better<br>30x Optical Zoom, 10X digital zoom or better | |
| 6 | Max. Aperture Ratio | F1.6(Wide)~F6.5(Tele) | |
| 7 | Angular Field of View | H: 58.6°(Wide)~1.23°(Tele) / V: 34.8°(Wide)~0.71°(Tele) | |
| 8 | Lens Type | DC auto iris, Varifocal or better | |
| 9 | Pan Range | 360° Endless | |
| 10 | Pan Speed | Preset: 400°/sec, Manual: 0.024°/sec~250°/sec | |
| 11 | Tilt Range | 95°(-5°~90°) | |
| 12 | Tilt Speed | Preset: 250°/sec, Manual: 0.024°/sec~250°/sec | |
| 13 | Sequence | Preset(300ea), Swing, Group(6ea), Trace, Tour, Auto Run, Schedule | |
| 14 | Preset Accuracy | ±0.2° | |
| 15 | Day & Night | Auto(ICR) | |
| 16 | Backlight Compensation | BLC, HLC, WDR, SSDR | |
| 17 | Wide Dynamic Range | 120dB or better | |
| 18 | Digital Image Stabilization | Support (built-in gyro sensor) | |

| | | | |
|---|---|---|---|
| 19 | Defog | Available | |
| 20 | Motion Detection | 8ea, polygonal zones Support | |
| 21 | Privacy Masking | 24ea, rectangular zones | |
| 22 | White Balance | ATW / AWC / Manual / Indoor / Outdoor | |
| 23 | Electronic Shutter Speed | Minimum / Maximum / Anti flicker (2~1/12,000sec) | |
| 24 | Analytics | Defocus detection, Directional detection, Fog detection, Face detection, Motion detection, Digital auto tracking, Appear/Disappear, Enter/Exit, Loitering, Tampering, Virtual line, Audio detection, Sound classification, Shock detection and others. Can be achieved via VMS and VA | |
| 25 | Interface | RS-485/Ethernet | |
| 26 | Alarm I/O | Input 4ea / Output 2ea | |
| 27 | Alarm Triggers | Analytics, Network disconnect, Alarm input | |
| 28 | Alarm Events | File upload via FTP and e-mail Notification via e-mail<br>SD/SDHC/SDXC or NAS recording at event triggers Alarm output<br>PTZ Preset | |
| 29 | Audio In | Selectable(mic in/line in)<br>Supply voltage: 2.5VDC(4mA), Input impedance: 2K Ohm | |
| 30 | Audio Out | Line out, Max. output level: 1Vrms | |
| 31 | IR Viewable Length | 500m or better | |
| 32 | Auto Tracking | Available | |
| 33 | Ethernet | RJ-45(10/100BASE-T), SFP(Optional) | |
| 34 | Video Compression | H.265/H.264: Main/Baseline/High, MJPEG | |
| 35 | Audio Compression | G.711 u-law /G.726 Selectable G.726(ADPCM) 8KHz, G.711 8KHz<br>G.726: 16Kbps, 24Kbps, 32Kbps, 40Kbps AAC-LC: 48Kbps at 16KHz | |
| 36 | Bitrate Control | H.264/H.265: CBR or VBR MJPEG: VBR | |
| 37 | Streaming | Unicast (20 users) / Multicast Multiple streaming (Up to 10 profiles) | |

| | | | |
|---|---|---|---|
| 38 | Protocol | IPv4, IPv6, TCP/IP, UDP/IP, RTP(UDP), RTP(TCP), RTCP, RTSP, NTP, HTTP, HTTPS, SSL/TLS, DHCP, FTP, SMTP, ICMP, IGMP, SNMPv1/v2c/v3(MIB-2), ARP, DNS, DDNS, QoS,<br>PIM-SM, UPnP, Bonjour | |
| 39 | Security | HTTPS(SSL) Login Authentication Digest Login Authentication<br>IP Address Filtering User access log<br>802.1X Authentication (EAP-TLS, EAP-LEAP) | |
| 40 | Application Programming Interface | ONVIF | |
| 41 | Edge Storage | Micro SD/SDHC/SDXC 1 no. slot of 512GB capacity each or better with minimum 512GB memory card. | |
| 42 | Operating Temperature / Humidity | minus 50°C~+55°C / Less than 90% RH | |
| 43 | Ingress Protection Shock and Vibration Resistance | IP66, IK10 | |
| 44 | Input Voltage | 24VAC, HPoE | |
| 45 | Power Consumption | 24VAC: Max. 92W HPoE: 60W | |
| 46 | Certification | UL, CE, FCC, BIS, EMC, UL CAP, | |
| 47 | Warranty | Minimum 5 years | |

### 6.11 Smart Kiosks

| S. No. | Indicative Requirement Description | Compliance (Yes / No) |
|---|---|---|
| | **Make:** | |
| | **Model:** | |
| 1 | Self Service Kiosks shall have integrated: | |
| | · Emergency Call Box function (with Camera and Microphone) | |
| | · MIFARe or equivalent Card Reader | |
| | · Contact less EMV Card reader | |
| | · Touch Screen for availing services with in-built interactive platform | |

| | | |
|---|---|---|
| | · Speaker | |
| | · Onscreen Keyboard | |
| | · Printing of any receipts and bus tickets etc. | |
| | · Kiosk structure (shell) | |
| | · 3G/ 4G /5G/ Wi-Fi Module | |
| | · QR code / Bar code Interface | |
| | All these components shall be supplied as part of the integrated multi services digital kiosk. | |
| 2 | Self-service Tourist Information Kiosk shall be fixed units, embedded inside the ground that shall be weather-proof | |
| 3 | The design of Kiosk terminal shall be based on the City's heritage theme | |
| 4 | The Emergency Call Button (ECB) shall have the capability to trigger emergency communications with Integrated Command and Control Centre (ICCC). As the Emergency Call Button is pressed, the call should land up to the operator at ICCC from where it may be routed to the concerned department. | |
| 5 | The ICCC shall able to monitor the video of the user who triggered the ECB. Automatic video recording shall be enabled when ECB button is pressed at Self-service Tourist Information Kiosk. | |
| 6 | The user-interface panel shall built-in capacitive touch screen for interactive purposes including but not limited to: | |
| | · **City Guide**: This component displays the city information, about city, business hubs etc. Places near me services which may include hotels, government offices, shops, tourist attraction, etc. | |
| | · **Tourist Destination**: This component displays the list of tourist destinations in the city along with the navigation map | |
| | · **View Hotels**: This component displays the list of hotels in the city with facilities and tariffs etc. with relevant filters | |
| | · **View Restaurants**: This component displays the list of hotels in the city with facilities and tariffs etc. with relevant filters | |
| | · **View Tourist Packages**: This component describes the available tourist packages | |
| | · **Helpline**: This component displays the helplines of Police, Fire, Ambulance, Railways enquiry, Public Transport and Tourist Information Centre etc. | |

| | | |
|---|---|---|
| | · **Events**: This component shall have schedule of events in the city with facility to book the tickets online | |
| | · **Emergency call:** This component shall allow registered users to make emergency call to the nearest police station based on the current location of the app user | |
| | · **Public Transport Route**: This component shall list Public transport route and schedule | |
| | · **Content Management to be available to admin users**: This component be used to create, update, delete content. It also covers review and approval of content by the respective content owner | |
| | · Weather related information | |
| 7 | Self-service Tourist Information Kiosk shall have capabilities for making digital payments for: | |
| | · Tickets for the events around the city | |
| | · Hotel accommodation | |
| | · Railway and Bus tickets | |
| | The selected Agency is required to use third party portal integration for Hotel, Travel and Event ticket booking services. | |
| 8 | Self-service Tourist Information Kiosk shall have in-built receipt/ticket printer having the functionality of printing of receipts, any other tickets, etc. | |
| 9 | Self-service Tourist Information Kiosk shall have the space for providing the static advertisement. For publishing of any advertisement, necessary approvals shall be obtained from Purchaser | |
| 10 | Self-service Tourist Information Kiosk shall be multilingual i.e. it shall support languages such as English, Hindi and regional language | |
| 11 | Self-service Tourist Information Kiosk shall be upgradable through a central system remotely over internet | |
| 12 | It shall be possible to monitor critical parameters related to health of kiosk device remotely using the network. | |
| 13 | Battery Backup of minimum 1 Hour | |
| 14 | Shall accept all the leading RBI approved wallets and UPI payments | |
| 15 | Kiosk enclosure shall have the space to house all the hardware equipment required for the Kiosk including switches, batteries, printer for receipts and other associated accessories. | |

| | | |
|---|---|---|
| | All the wiring shall be concealed within the Kiosk enclosure and shall not be visible from outside | |
| **16** | **Kiosk Content Management Application:** | |
| | Following functionality is envisaged in the Kiosk Content Management Application: | |
| | · Provide role-based user access mechanism where an administrator can create and manage users, user groups, roles, and role permissions | |
| | · Shall provide login module using which content authors will be able to login and enable the creation, modification, and deletion of templates to enable easy management of Kiosk User interface/site and page layout and navigation | |
| | · Shall provide a WYSIWYG (What you see is what you get) editor and provide standard Word authoring features (also known as a Rich Text Editor) to enable an editor to add and format text, links, and images to content areas, create tabular layouts within a text area and apply styles without needing HTML skills | |
| | · Shall support drag and drop feature to enable easy management of content. The editor shall support the following minimum preview and publication functions: - | |
| | • Preview only on content editor (not visible to users) | |
| | • Save as unpublished (draft) | |
| | • Preview on Portal | |
| | • Send for approval | |
| | • Approve | |
| | • Publish after approval (i.e. after successful completion of the approval workflow) | |
| | • Unpublish (save as unpublished, not visible to users) | |
| | • Publication scheduling | |
| | • Publication expiration date (automatic unpublish) | |
| | • Shall contain a content approval workflow to enable the approval of modifications (create, modify, delete) before publication (i.e. before becoming visible to the public) | |
| | • Shall support Administrator (or a designated user with an appropriate permission level) to assign and reassign users to workflow tasks (i.e. define the targets within the workflow) | |

| | | |
|---|---|---|
| 17 | • Layout and content shall be managed separately (i.e. it must be possible to create and edit content without having to amend or create a template) | |
| | • Shall support creation of navigation, breadcrumb and sitemap that will be published and rendered on Kiosk User Interface | |
| | • Shall support version control (check-in, check-out, number of versions) and it must be possible to restore previous versions of a content item | |
| | • Shall support creation of content in different languages (namely English, Hindi & regional language | |
| | • Shall support hierarchical creation of sites (i.e. parent/child sites in the same domain) and enable the child site to either inherit the look & feel of the parent site or have its own style and branding | |
| | • Shall be capable of storing and categorizing documents, images, video and audio files. | |
| | • CMS shall support the creation of an alert in response to a specific event, such as: | |
| | • Content amendment | |
| | • Content expiration date approaching | |

**6.12 Local Processing Units (LPU):**

| Sl.No | Specification | Compliance (Yes /No) |
|---|---|---|
| | **Make** :<to be provided by the bidder> | |
| | **Model** :<to be provided by the bidder> | |
| 1 | Local Processing Unit shall be of Aluminium Alloy Casing | |
| 2 | Compute: Intel Core i7, 7th Gen or better | |
| 3 | LPU should have 2*Intel I210AT PCIe Gig. Ethernet | |
| 4 | It shall support GPU Intel® HD Graphics 630 min. | |
| 5 | Memory- DDR4 up to 16GB | |
| 6 | Display Port- 1 nos. VGA, 1 nos. HDMI, 1 nos. DP | |
| 7 | It shall support Secondary Storage 1*1TB 3.5”SATA HDD | |
| 8 | It shall support USB- 6 nos. USB 3.0 and 2 nos. USB 2.0 | |

### 6.13 External IR Illuminator (Optional)

| Technical Specifications -External IR Illuminator | | |
|---|---|---|
| **Sr. No.** | **Item Description** | **Compliance (Yes/No)** |
| 1 | Type: External IR illuminator with high performance LED (42 Pcs. high brightness IR LED), high efficiency, energy saving and environmental protection. | |
| 2 | Wavelength: ≥850 nm (Infrared) | |
| 3 | Coverage Area: 1 Lane (standard for ANPR), up to 4 lane for Surveillance | |
| 4 | Illumination Range: up to 100 Mtrs. | |
| 5 | Protection Level: IP66, IK10 | |
| 6 | IR Power: 80 W | |
| 7 | Adjustable angle to appropriately focus at the number plate. | |
| | Beam Angle: multiple options- 10 degree (standard), 15, 30, 45 Degrees | |
| 8 | Surge level: Common mode 6KV, Differential mode: 3 KV | |
| 9 | **Deleted** | |
| 10 | Protection function: Transient over peak suppression | |
| 11 | Housing material: Die-casting aluminum alloy | |
| 12 | User Interface: RS485 | |
| 13 | Working Temperature: -40 +70 C (working humidity 10% - 95%) | |
| 14 | Proposed IR Illuminator should be IP66, IK10, CE, FCC, RoHS and Eye & Skin safety test report IEC-62471 certified. | |

**Power- Voltage Input: DC6~48V**

| **Sl.No** | **Specification** | **Compliance (Yes /No)** |
|---|---|---|
| | **Make** :<to be provided by the bidder> | |
| | **Model** :<to be provided by the bidder> | |
| 1 | AC Input: External Adapter (Option) | |
| 2 | Voltage Input: 100VAC~240VAC@50~60Hz | |
| 3 | Temperature- -20°C ~ 70°C | |

| | | |
|---|---|---|
| 4 | It shall withstand vibrations | |
| 5 | It shall withstand shock | |
| 6 | Hardware / software should have minimum 5 year warranty | |

### 6.14 Network Connectivity - OFC

It is proposed to setup city wide OFC network connectivity as the field components increases data transfer, size also increases hence there is need for fast data transfer with high availability.

**Surveillance and Security**

In order to improve the quality of life for residents, the first step is safety for any city to evolve as a Smart City. In the past few years, implementation of surveillance cameras has improved public safety and prevented crime. However, today new types of sensors are installed and those are way too advanced than basic surveillance cameras and requires high data transmitting speed. Thus, Fiber optics play a very crucial role here.

**Traffic Control**

Traffic is one of the most significant challenges in the cities that are experiencing rapid growth. Thus, the need for fiber Optics is increasing, as it's used at many places in order to tie together the enormously complex networks that control sensors like the Automatic traffic lights, Variable message sign board, cameras and ATCS systems technology. The sensors at Junctions and video with analytic functionality provide real-time data on Traffic congestion while the traffic control cameras are connected by fibre optics to the transport authority. They can monitor traffic in real time, making the control centre more efficient and intelligent for them to increase or reduce the frequency of green lights according to the traffic conditions.

**Integrated Command and Control Center**

ICCC can be connected with City field components through fiber optic internet. ICCC have the ability to provide centralized services, security, climate control, etc. Here fiber optic cables provide the best means of handling this data and transmitting it around a facility.

Cities around the globe have been transforming from traditional to smart cities that will benefit everyone. Fibre optics and IoT are substantial and helping us get one step closer to this reality. Reliability, security and speed are key to the efficient implementation of Smart cities and IoT and fibre optics are one of the first real time solutions available today.

**Network Layers**

**Street Layer**

All the access layer devices like outdoor network access points, cameras for surveillance, environmental sensors, VaMS, PAS including other Smart city initiatives will connect to ruggedize industrial grade access switches in street cabinets and will create street layer architecture. Street layer architecture should be built considering the harsh outdoor deployment environment and should be flexible to connect various devices/ sensors to the

citywide transport network.

**City Network Layer**

The city network layer aggregates street access switches and access points and connects to the data center and other locations used for monitoring and managing the infrastructure. Network layer will create transport network for City and will laid down the foundation for all the present and future urban services. This layer will provide City scalability to both expand existing services and roll out new services as and when required without any dependency on any service provide bandwidth operation cost. Also this layer provides the flexibility to run multiple concurrent services with required segregation and prioritization.

**Data Center Layer**

The data center layer includes all our WAN routers, core switches, servers, and storage resources for citywide applications and service. Data center layer will be the heart of City operation will host all the Citizen services and provide the centralized processing for the same.

**Considering the above requirement new OFC network is proposed as per BoM.**

## 7 Approach and methodology to be adopted for implementation:

- The SI shall first carry out a detailed survey to identify & finalize the locations, requirements vis-a-vis proposed solutions.
- Post completion of Survey the SI shall consult the various Stake Holder of the project, in consultation with the Authority, and revalidate the scope mentioned in this document. Upon freezing the scope requirement, the SI shall detail out the final functional requirement for each of the proposed ICT intervention and get a sign off from the user department and the Authority.
- Post finalization of the SRS and FRS the SI shall submit a High-Level Design Document which shall cover the broad architecture and a solution document for each of the proposed ICT interventions. The HLD will comprise of the compute, storage and the OS requirements.

- Post HLD, the SI shall be submitting the Low-Level Design Document with the good for construction drawing, network connectivity drawing, LPU details, if any, API for integration, communication protocol etc.
- Upon approval of LLD by the Authority, the SI shall implement the said ICT intervention.
- While implementing the ICT intervention the SI shall adopt the following:

**Scalability -** The system should also support both vertical and horizontal scalability. There must not be any system- imposed restrictions on the upward scalability in number of field devices, or other smart city components. The Applications proposed for various vertical solutions shall be capable of handling 50% growth for the next 5 years. SI shall clearly quantify the expansion capabilities of the application software without incurring additional cost.

**Availability** -. The SI shall make the provision for high availability for all the services of the system. Redundancy has to be considered at the core components level. The SLA for various solutions is explained under each solution itself .

**Security-** The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc. SI must make provisions for security of field equipment as well as protection of the software system from hackers and other threats. 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. There should also be an endeavour to make use of the SSL/VPN technologies to have secured communication between Applications and its end users.

Field equipment installed through this Project would become an important public asset. During the contract period of the Project the SI 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.

The security services used to protect the solution shall include: Identification, Authentication, Access Control, Administration and Audit and support for industry standard protocols. 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. The overarching requirement is the need to comply with ISO 27001 standards of security. The application design and development should comply with OWASP top 10 principles. All the field devices will be X.509 certified for compliance to policy change management and to ensure that there is no default password.

**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.

**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.

**Open Standards -** Systems should use open standards and protocols to the extent possible

**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.

**Support for 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 SI 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 SI 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 and /or as per standards mentioned in the technical specifications

**Application Architecture**

i. The applications designed and developed for the departments concerned must follow best practice and industry standards. In order to achieve the high level of stability and robustness of the application, the system development life cycle 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. Standards should (a) at least comply with published e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and (b) be of leading industry standards and /or as per standards mentioned in the technical specifications

ii. 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 client 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.

iii. SI shall design and develop the Smart City System as per the Functional and System requirement specifications finalized.

iv. The Modules specified will be developed afresh based on approved requirement.

**8 Lifecycle of implementation of ICT intervention:**

Following are the main activities to be carried out I:

1. Project Planning, execution and Management
2. Assessment and Gap analysis of requirement for all smart city components under scope.
3. Solution Design, System Customization and development for all components mentioned in this volume.
4. ICT items Procurement, deployment and commissioning
5. Site Preparation including required civil work, LAN Networking
6. Application and general awareness Training
7. Business Process Reengineering for the selected applications/ services, if required
8. STQC Certification
9. UAT & Go live
10. Capacity Building
11. Technical Support
12. Operation & Maintenance (O&M) for 5 Years.

## 9 Detailed Technical and Non-Technical Manpower:

The project requires being setup initially in an implementation phase spanning about nine months and to be operated and maintained for a further 60 Months period to transform the departments of stakeholders of PSCDL into a fully digitized way of operations. This requires a highly skilled expertise in all the envisioned ICT technical function areas both during the implementation phase and in the operations and maintenance phase.

The Key experts are listed in the table below along with their functional roles and an approximate period of implementing the envisioned solution.

To implement and successfully execution of project below is the man months required for both Implementation and O&M phase

| 1 | Manpower for Implementation Phase and O&M | TYPE | UoM | QTY |
|---|---|---|---|---|
| 1.1 | Project Manager - 1 no | Service | Number | 1 |
| 1.2 | Solution Architect and Cloud expert - 1 no | Service | Number | 1 |
| 1.3 | ICCC / command center Expert - 1no | Service | Number | 1 |
| 1.4 | Network Architect - 1 no | Service | Number | 1 |
| 1.5 | Security Infrastructure and CCTV specialist - 1 each | Service | Number | 1 |
| 1.6 | GIS Expert - 1 no | Service | Number | 1 |
| 1.7 | Data Management Expert / Analyst - 1 no | Service | Number | 1 |

| | | | | |
|---|---|---|---|---|
| 1.8 | Business Analyst/Use case/SOP Expert - 1 no | Service | Number | 1 |
| 1.9 | Server / Storage/ Database Expert - 1 no | Service | Number | 1 |
| 1.10 | ITMS & ATCS Expert - 1 no | Service | Number | 1 |
| 1.11 | Electrical Engineer - 1 Person | Service | Number | 1 |
| 1.12 | Electrical Technician - 2 Person | Service | Number | 2 |
| 1.13 | OFC Expert - 1 no | Service | Number | 1 |
| 1.14 | Helpdesk operator (20 no) | Service | Number | 20 |
| 1.15 | Security staff (4 no) | Service | Number | 4 |
| 1.16 | Civil Technician - 2 person | Service | Number | 2 |
| 1.17 | Civil Engineer - 1 no | Service | Number | 1 |
| 1.18 | Field Engineer - 5 Persons | Service | Number | 5 |
| 1.19 | Office staff, Reception (3 no) | Service | Number | 3 |

**10 Use cases to be deployed / integrated:**

| # | **Use cases to be deployed** |
|---|---|
| 1 | ICCC Platform |
| 2 | Intelligent Traffic Management System |
| 3 | City Surveillance with video analytics |
| 4 | Variable Message Display |
| 5 | PA system |
| 6 | Environmental Sensors |
| 7 | Smart Poles (with CCTV, Wi-Fi, AQM, Smart Street Light, ECB, PA, Digital Billboard) |
| 8 | Citizen Mobile App and Web Portal with Tourist/Visitors platform |
| 9 | City Data Collaboration Platform |
| 10 | Smart Kiosk |
| 11 | Smart Parking (Additional Deployment as per requirement of DRDM/ PSCDL) |
| 12 | EMS |
| 13 | Flood monitoring through Flood sensors and cameras |
| 14 | GIS Platform |
| 15 | OFC |
| 16 | Social Media |
| 17 | Chat bot |
| 18 | Digital assistant Application with ICCC platform Integration |
| 19 | Configurable Dashboard |

| Sl.No | Integration of Existing Applications |
|---|---|
| 1 | Applications hosted by NIC |
| 2 | E-Governance Platform (Property Tax, Building Approval, Birth/Death, Marriage etc.,) |
| 3 | Electrical SCADA |
| 4 | e-Health |
| 5 | Websites hosted by Puducherry Municipality and Oulgaret Municipality |
| 6 | Solid waste Management |
| 7 | Water/ Sewage SCADA |
| 8 | ERSS (Dial 100/112) |
| 9 | Applications hosted by Disaster Management |
| 10 | Transport Monitoring Centre |
| 11 | Integration with RTO |
| 12 | Any other integration as suggested by the Puducherry authorities (up to 12 months from the date of issue of LOA to the SI) |

### 10.1 Digital Assistant Application

In order to ensure that the impact of Smart City investments impacts the common man and creates smart livelihoods a platform for enabling unemployed youth to be digital entrepreneur is envisaged While connectivity is the first stage of digital inclusion , enabling digital transactions would be the right metric to evaluate the access to digital services . Statistics indicate that only about 3% of the population actually carry out transactions and reap the benefits of digital world.

It is proposed to depute one technical engineer at one of the smart kiosk location as " Digital assistant "to assist the local community to carry out transactions on the net for E-governance services, tickets, assisted E- commerce , last mile aggregation services and " Phygital " interface for other upstream services such as finance , credit , health care etc.

## 11 Training, Audit and Change Management Plan:

Training and Change Management is highly critical component for implementation of Smart City Solutions. The objective of Training and Change Management initiatives is to empower the direct users and other stakeholders of DRDM and Puducherry Smart City Corporation Limited to optimally use the system and ensure achievement of end objectives of various Smart City Solutions.

In order to strengthen the staff, structured capacity building programs shall be undertaken for multiple levels in the organizational hierarchy like foundation process/ soft skills training to the staff for pre-defined period. Also, refresher trainings for integrated Command Control Centre, City Operation Staff and designated departments shall be a part of Capacity Building. It is important to understand that training needs to be provided to each and every staff personnel of ICCC. These officers shall be handling emergency situations with very minimal turnaround time. Some directions with regards to the training and change management plan which will need to be prepared by the implementing solution provider are as follows:

1. Appropriate training shall be carried out as per the User Training Plan prepared in detail stating the number of training sessions to be held per batch of trainees, course work for

the training program, coursework delivery methodologies and evaluation methodologies in detail.

2. End user training shall include all the equipment including but not limited to all the applications and infrastructure at ICCC, ITMS, Safety and Surveillance and other smart solutions. End user training shall be conducted at a centralized location or any other location as identified by PSCDL.
3. Imparting operational and technical training to internal users on solutions being implemented to allow them to effectively and efficiently use the surveillance system.
4. Preparation of the solution specific training manuals and submit the same to purchaser for review and approval. Training Manuals, operation procedures, visual help-kit etc. shall be provided in English language.
5. Ensuring that all concerned personnel receive regular training sessions, from time to time, as and when required. Refresher training sessions shall be conducted on a regular basis.
6. An annual training calendar shall be prepared and shared with the Client along with complete details of content of training, target audience for each year etc.
7. Updating training manuals, procedures manual, deployment/Installation guides etc. on a regular basis (Quarterly/ Biannual) to reflect the latest changes to the solutions implemented and new developments.
8. Ensuring that training is a continuous process for the users. Basic computer awareness, fundamentals of computer systems, basic, intermediate and advanced application usage modules shall be identified by the solution provider.
9. Systematic training shall be imparted to the designated trainees that shall help them to understand the concept of solution, the day-to-day operations of overall solution and maintenance and updating of the system to some extent. This shall be done under complete guidance of the trainers provided by the solution provider.
10. Training sessions and workshops shall comprise of presentations, demonstrations and hands-on mandatorily for the application modules.

## 12 Proposed Governance Model:

The proposed project governance structure would comprise the following:

- High level steering committee, Board members of PSCDL, DRDM and Senior Executives of RailTel
- Project specific working group, comprising the respective departmental functional, RailTel Project Manager and select team members for the respective module(s).
- Core team members, domain specialists and designated counterpart staff from PSCDL/ concerned Government Agency for individual modules.
- Support team

The steering committee would meet once every month to take important decisions and approve any strategic decisions to ensure timely implementation and address identified bottlenecks. The project specific working groups would convene on a weekly or a bi-weekly basis to discuss progress and address any issues pertaining to implementation.

## 13 Exit Management Under Contract Completion:

1. Provide a comprehensive exit management plan.
2. Before 6 months prior to the contract ending, SI shall ensure fully train Puducherry

Authorities' staff or any other agency designated by Puducherry Authorities who is designated to take over the maintenance of the System.

3. The SI shall ensure for transferring all the knowledge regarding the Systems, technically and operationally to enable the new agency/ Puducherry Authorities to carry out the requisite functions.
4. All latest operations & technical manuals, configuration files, software, licenses, as-built drawings etc. shall be handed over to Puducherry Authorities at least 3 months before contract completion.
5. The Parties may, if mutually agreed, extend the contract in accordance with the terms and conditions.
6. **All source codes/API**, backup data, Puducherry Authorities specific information shall be handed over to Puducherry Authorities as part of exit management.
7. All ICT systems shall be properly handed over to Puducherry Authorities in operational state as part of exit management.
8. The SI shall be responsible for providing the tools for import /export of VMs & content and the SI shall be responsible for preparation of the Exit Management Plan and carrying out the exit management / transition.
9. SI shall be responsible for migration of the VMs, data, content and any other assets to the new environment and ensuring successful deployment and running of the Puducherry Authorities' solution on the new infrastructure by suitably retrieving all data, scripts, software, virtual machine images, and so forth to enable mirroring or copying to industry standard media
10. The format of the data transmitted from the cloud service provider to the new environment created by the Puducherry Authorities should leverage standard data formats whenever possible to ease and enhance portability.
11. The SI shall transfer the organizational structure developed during the Contract Duration to support the delivery of the Exit Management Services. This will include: Document, update, and provide functional organization charts, operating level agreements with Third-Party contractors, phone trees, contact lists, and standard operating procedures. Transfer physical and logical security processes and tools, including cataloguing and tendering all badges and keys, documenting ownership and access levels for all passwords, and instructing Puducherry Authorities or its authorized representative in the use and operation of security controls.
12. Retain the data at the end of the Contract.
13. Once the exit process is completed, remove the data, content and other assets from the cloud environment and destroy the VM, Content and data of Puducherry Authorities.
14. The ownership of the data generated upon usage of the system, at any point of time during the Contract or expiration of the Contract, shall rest absolutely with Puducherry Authorities.
15. This sets out the provisions, which will apply on expiry or termination of the Master Service Agreement, the Project Implementation, Operation and Management SLA.
16. In the case of termination of the Project Implementation and/or Operation and Management, the Parties shall agree at that time whether, and if so during what period, the provisions of this Schedule shall apply.
17. The Parties shall ensure that their respective associated entities carry out their respective obligations set out in this Exit Management Schedule.

## 14 Detailed work Phases and considerations

### 14.1.1 Phase 1(Implementation Phase)

#### 14.1.1.1 Requirement Survey Phase

The SI must perform the detailed assessment of the IT Solution requirements as mentioned in this RFP. Based on the understanding and its own individual assessment, SI shall develop & finalize the System Requirement Specifications (SRS) in consultation with RAILTEL / DRDM/ PSCDL and its representatives. While doing so, SI at least is expected to do following:

i. SI shall develop the FRS and SRS documents.
ii. SI shall develop and follow standardized template for requirements capturing and system documentation.
iii. SI must maintain traceability matrix from SRS stage for the entire implementation.
iv. SI must get the sign off from the various departments of Puducherry.
v. Prior to starting the site clearance, the SI shall carry out survey of field locations as specified in Annexure VIII, for buildings, structures, fences, trees, existing installations, etc.
vi. All existing road signs which are likely to be affected by the works are to be carefully taken down and stored. Signs to be re-commissioned shall be cleaned, provided with new fixings where necessary and the posts re-painted in accordance with PSCDL guidelines. Road signs, street name plate, etc. damaged by the SI during their operation shall be repaired or replaced by SI at no additional cost.

#### 14.1.1.2 Design Phase

The SI shall build the solution as per the Design Considerations detailed in Section 6. The solution proposed by SI should comply with the design considerations requirements as mentioned therein.

#### 14.1.1.3 Project Development Phase

Software (Configuration and Customization). Following need to be adhered:

1) SI will be responsible for supplying the application and licenses of related software and installing the same so as to meet project requirements.
2) The SI shall perform periodic audits to measure license compliance against the number of valid End User software licenses consistent with the terms and conditions of license agreements, volume purchase agreements, and other mutually agreed upon licensed software terms and conditions. The SI shall report any exceptions to license terms and conditions at the right time to PSCDL/DRDM. However, the responsibility of license compliance solely lies with the SI. Any financial penalty imposed on PSCDL/DRDM during the contract period due to license non-compliance shall be borne by SI.

3) SI shall also supply any other tools & accessories required to make the integrated solution complete as per requirements. For the integrated solution, the SI shall supply:

a) Software & licenses.
b) Supply tools, accessories, documentation and provide a list of the same. Tools and accessories shall be part of the solution.
c) System Documentation: System Documentation both in hard copy and soft copy to be supplied along with licenses and shall include but not limited to following.Documentation to be maintained, updated and submitted to PSCDL/DRDM/RailTel regularly:

- Functional Requirement Specification (FRS)
- High level design of whole system
- Low Level design for whole system / Module design level
- System Requirements Specifications (SRS)
- Any other explanatory notes about system
- Traceability matrix
- Technical and product related manuals
- Installation guides
- User manuals
- System administrator manuals
- Toolkit guides and troubleshooting guides
- Other documents as prescribed by PSCDL/DRDM/RailTel
- Quality assurance procedures
- Change management histories
- Version control data
- SOPs, procedures, policies, processes, etc. developed for PSCDL/DRDM/RailTel
- Programs
- Entire source codes
- All programs must have explanatory notes for understanding
- Version control mechanism
- All old versions to be maintained
- Test Environment
- Detailed Test methodology document
- Module level testing
- Overall System Testing
- Acceptance test case

These documents need to be updated after each phase of project and to be maintained updated during entire project duration. The entire documentation will be the property of PSCDL/DRDM.

#### 14.1.1.4 Integration Phase

The Command-and-control center should be integrated with feeds of all component under the ICCC Project. The SI shall provide the testing strategy including traceability matrix, test cases and shall conduct the testing of various components of the software developed/customized and the solution-as-a-whole. The testing should be comprehensive and should be done at each stage of development and implementation.

#### 14.1.1.5 Go-Live Preparedness and Go-Live

i. SI shall submit signed-off UAT report (issue closure report) ensuring all issues raised during UAT are being resolved prior to Go-Live.

ii. SI shall ensure that Go –Live criteria as mentioned in User acceptance testing of Project is met and SI needs to take approval from the Authorities on the same.

#### 14.1.1.6 Project Management & Facilities Management Services

The SI will be required to provide facilities management services to support the PSCDL/DRDM/RailTel and stakeholder department officials in performing their day-to-day functions related to this system.

SI is required to depute a dedicated, centralized project management and technical team for the overall project management and interaction with PSCDL and stakeholder departments.

#### 14.1.1.7 Provision of the Operational Manpower & Contact Center

Manpower to view the various data feeds and call center operations at ICCC
The SI is required to provide suitable manpower to monitor the data feeds ICCC and support PSCDL/DRDM/RailTel, Traffic Police and other stakeholder departments for operationalization of smart solutions of the project. The exact role of these personnel and their responsibilities would be defined and monitored by PSCDL/DRDM/RailTel and respective departmental personnel. SI shall be required to provide such manpower meeting following requirements:

i. All such manpower shall be minimum graduate pass
ii. All such manpower shall be without any criminal background / record.
iii. PSCDL/DRDM/RailTel reserves the right to carry out background check of the personnel proposed on the Project for verification of criminal record, at the beginning of deployment or during deployment.
iv. SI shall have to replace any person, if not found suitable for the job.
v. All the manpower shall have to undergo training from the SI for at least 15 working days on the working of project. Training should also cover dos & don'ts and will have few sessions from PSCDL/DRDM/RailTel and Stakeholders/End User Department officers on right approaches for monitoring the feeds & providing feedback to PSCDL/DRDM/RailTel, Stakeholders/End User Department officers and other associated government agencies.

Detail operational guideline document shall be prepared during implementation which shall specify detail responsibilities of these resources and their do's & don'ts.

#### 14.1.1.8 Basic Infrastructure Services

Following services shall be provided by the SI under the basic infrastructure services:

i. Ensure availability of the infrastructure (both physical and IT) including but not limited to Power, Cooling, Racks, Storage and other peripheral equipment installed at the time of Project commissioning as per the SLAs.
ii. Ensure scalability in terms of availability of racks and supporting infrastructure.
iii. Proactive and reactive maintenance, repair and replacement of defective components (physical and other peripheral IT infrastructure) installed for the Project through this RFP. The cost for repair and replacement shall be borne by the SI.
iv. Any component (Physical & IT installed at the time of Project commissioning) that is reported to be faulty / non-functional on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame agreed upon in the Service Level Agreement (SLA).
v. Proactive monitoring of the entire basic infrastructure installed.
vi. SI shall maintain records of the maintenance of the basic infrastructure and shall maintain a logbook on-site that may be inspected by the PSCDL/DRDM/RailTel, Police department and other stakeholder departments/end users at any time.

#### 14.1.1.9 Network Monitoring Services

The activities shall include:

i. SI shall provide services for management of ICCC Project to maintain performance at optimum levels on a 24 x 7 basis.
ii. SI shall monitor and administer the network.
iii. SI shall create and modify VLAN, assignment of ports to appropriate applications and segmentation of traffic.
iv. SI shall carry out break fix maintenance of the LAN cabling or maintenance work requiring civil work.

#### 14.1.1.10 Integration Testing

This shall be a black-box testing role primarily to ensure that the application to be deployed does not disrupt the Puducherry operations and affect other Puducherry infrastructure in terms of performance and security. The technical tasks to be carried out shall be as follows:

i. Functional Testing: Ensuring that the application functionality as described by the PSCDL/DRDM/RailTel, Police department and other stakeholder departments/end users. The functional testing of application will necessarily be minimal as this is a core responsibility of the Supplier.
ii. Performance Testing: Ensuring that the application meets expressed performance requirements on the Puducherry servers by using performance test tools and performance monitoring tools.
iii. Security Testing: Testing for exploitable application security weaknesses that undermine the application security or the security of the infrastructure.

#### 14.1.1.11 Vendor Management Services

The activities shall include:

i. Coordination with all the project stakeholders to ensure that all Puducherry activities are carried out in a timely manner.SI shall coordinate and follow-up with all the relevant vendors to ensure that the issues are resolved in accordance with the SLAs agreed upon with them.
ii. SI shall also ensure that unresolved issues are escalated to respective departments.
iii. SI shall maintain database of the various vendors with details like contact person, telephone nos., escalation matrix, response time and resolution time commitments etc.
iv. SI shall draw a consolidated quarterly SLA performance report across vendors for consideration of the PSCDL/DRDM/RailTel, Police department and other stakeholder departments/end users.

#### 14.1.1.12 Network Management

The objective of this service is to ensure continuous operation and upkeep of the Network infrastructure of the project including all active and passive components. The selected SI shall be responsible to coordinate with Network Service Provider for network related issues between ICCC, DC and other sub systems. The services to be provided for Network Management include:

i. Ensuring that the network is available 24x7x365 as per the prescribed SLAs for the 5 years of operations after final acceptance testing of all equipment's and services.
ii. Attending to and resolving network failures and snags.
iii. Support and maintain the overall network infrastructure including but not limited to LAN passive components, routers, switches etc.
iv. Configuration and backup of network devices including documentation of all configurations.
v. 24x7x365 monitoring of the network to spot the problems immediately.
vi. 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.
vii. Ensuring timely information to the PSCDL/DRDM/RailTel, Police department and other stakeholder departments/end users pertaining to issues of Network Backbone

#### 14.1.1.13 Physical Infrastructure Management and Maintenance Services

All the devices that will be installed in the Project as part of the physical infrastructure should be SNMP enabled and shall be centrally and remotely monitored and managed on a 24x7x365 basis. Industry leading infrastructure management solution should be deployed to facilitate monitoring and management of the Infrastructure on one integrated console. The physical infrastructure management and maintenance services shall include:

i. Proactive and reactive maintenance, repair and replacement of defective components (IT

and Non-IT/ Hardware and Software). The cost for repair and replacement shall be borne by the SI.

ii. The SI shall have to stock and provide adequate onsite and offsite spare parts and spare component to ensure that the uptime commitment as per SLA is met. To provide this service it is important for the SI to have back to back arrangement with the OEMs. The SI needs to provide a copy of the service level agreement signed with the respective OEMs.

iii. Component that is reported to be down on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame indicated in the Service Level Agreement (SLA). In case the selected SI fails to meet the above standards of maintenance, there will be a penalty as specified in the SLA.

iv. The selected SI shall also maintain records of all maintenance of the system and shall maintain a logbook on-site that may be inspected by the PSCDL/DRDM/RailTel, Police department and other stakeholder departments/end users at any time.

### 14.1.2 Phase-2 (Operations and Maintenance)

Success of the Project would lie on how professionally and methodically the entire Project is managed once the implementation is completed. From the SI perspective too, this is a critical phase since the quarterly payments are linked to the SLA's in the post implementation phases. SI shall provide operations and maintenance services for the software, hardware and other IT and Non-IT infrastructure installed as part of the project after Go-Live for a period of 5 years. Warranty period of the product supplied under project i.e. hardware, software, IT/Non-IT etc., will be considered after phase wise Go-Live.

### 14.1.3 Project Management and Governance

#### 14.1.3.1 Project Management Office (PMO)

A Project Management office will be set up during the start of the project. The PMO will, at the minimum, include a designated full time Project Manager from SI. It will also include key persons from other relevant stakeholders including members of PSCDL/DRDM/RailTel and other officials/representatives by invitation. The operational aspects of the PMO need to be handled by the SI including maintaining weekly status, minutes of the meetings, weekly/monthly/project plans, etc.

PMO will meet formally on a weekly basis covering, at a minimum, the following agenda items:

i. Project Progress
ii. Delays, if any – Reasons thereof and ways to make-up lost time
iii. Issues and concerns
iv. Performance and SLA compliance reports;
v. Unresolved and escalated issues;
vi. Project risks and their proposed mitigation plan
vii. Discussion on submitted deliverable
viii. Timelines and anticipated delay in deliverable if any
ix. Any other issues that either party wishes to add to the agenda.

During the development and implementation phase, there may be a need for more frequent meetings and the agenda would also include:

i. Module development status
ii. Testing results
iii. IT infrastructure procurement and deployment status
iv. Status of setting up/procuring of the Helpdesk, DC hosting
v. Any other issues that either party wishes to add to the agenda.

Bidder shall recommend PMO structure for the project implementation phase and operations and maintenance phase.

#### 14.1.3.2 Helpdesk and Facilities Management Services

The SI shall be required to establish the helpdesk and provide facilities management services to support the PSCDL/DRDM/RailTel and stakeholder department officials in performing their day- to-day functions related to this system.

The SI shall setup a central helpdesk dedicated (i.e. on premise) for the Project, which shall be supported by individual smart city command centres, implemented and proposed to be setup under Puducherry Smart City Programme. This helpdesk would be operational upon implementation of the Project. Providing helpdesk/support services from a shared facility of any other party/provider is not permitted.

Functional requirements of the helpdesk management system fully integrated with the enterprise monitoring and network management system. The system will be accessed by the stakeholder department officials for raising their incidents and logging calls for support. The detailed service levels and response time, which the SI is required to maintain for provisioning of the FMS services are described in the Service Level Agreement of this Tender.

SI shall deploy Manpower during implementation and O&M phases. The deployed resource shall report to PSCDL/DRDM/RailTel's Project In-charge for Smart City Project and work closely with Program Management Office of the project. Following are the minimum resources required to be deployed in the Project, however SI may deploy additional resources based on the need of the Project and to meet the defined SLAs in this RFP:

Note: Numbers provided for staff providing 24*7 support is excluding relievers.

#### 14.1.3.3 Project Monitoring and Reporting

The SI shall circulate written progress reports at agreed intervals to PSCDL/DRDM/RailTel and other stakeholders. Project status report shall include Progress against the Project Management Plan, status of all risks and issues, exceptions and issues along with recommended resolution etc.
Other than the planned meetings, in exceptional cases, project status meeting may be called with prior notice to the Bidder. PSCDL/DRDM/RailTel reserves the right to ask the bidder for the project review reports other than the standard weekly review reports.

#### 14.1.3.4 Risk and Issue management

The SI shall develop a Risk Management Plan and shall identify, analyze and evaluate the project risks, and shall develop cost effective strategies and action plans to mitigate those risks.

The SI shall carry out a Risk Assessment and document the Risk profile of PSCDL/DRDM/RailTel based on the risk appetite and shall prepare and share the PSCDL/DRDM/RailTel Risk Register. The SI shall develop an issues management procedure to identify, track, and resolve all issues confronting the project. The risk management plan and issue management procedure shall be done in consultation with PSCDL/DRDM/RailTel.

The SI shall monitor, report, and update the project risk profile. The risks should be discussed with PSCDL/DRDM/RailTel and a mitigation plan be identified during the project review/status meetings. The Risk and Issue management should form an agenda for the Project Steering Committee meetings as and when required.

#### 14.1.3.5 Governance procedures

SI shall document the agreed structures in a procedure's manual.

#### 14.1.3.6 Planning and Scheduling

The SI will prepare a detailed schedule and plan for the entire project covering all tasks and sub tasks required for successful execution of the project. The SI has to get the plan approved from PSCDL/DRDM at the start of the project and it should be updated every week to ensure tracking of the progress of the project.

The project plan should include the following:

i. The project breaks up into logical phases and sub-phases;
ii. Activities making up the sub-phases and phases;
iii. Components in each phase with milestones;
iv. The milestone dates are decided by RailTel in this RFP. SI cannot change any of the milestone completion dates. SI can only propose the internal task deadlines while keeping the overall end dates the same. SI may suggest improvement in project dates without changing the end dates of each activity.
v. Key milestones and deliverables along with their dates including those related to delivery and installation of hardware and software;
vi. Start date and end date for each activity;
vii. The dependencies among activities;
viii. Resources to be assigned to each activity;
ix. Dependency on PSCDL/DRDM/RailTel

#### 14.1.3.7 License Metering / Management

The SI shall track software usage throughout the IT setup so as to effectively manage the

risk of unauthorized usage or under-licensing of software installed at the ICCC. This may be carried out through the use of standard license metering tools.

### 14.1.4 Change Management & Control

#### 14.1.4.1 Change Orders / Alterations / Variations

i. The SI agrees that the requirements given in the Bidding Documents are minimum requirements and are only indicative. The SI would need to fetch out the details at the time of preparing the design document prior to actual implementation. It shall be the responsibility of the SI to meet all the requirements of technical specifications contained in the RFP and any upward revisions and/or additions of quantities, specifications sizes given in the Bidding Documents required to be made during execution of the works, shall not constitute a change order and shall be carried out without a change order and shall be carried out without any time and cost effect to Purchaser.

   Further upward revisions and or additions required to make SI's selected equipment andinstallation procedures to meet Bidding Documents requirements expressed and to make entire facilities safe, operable and as per specified codes and standards shall not constitute a change order and shall be carried out without any time and cost effect to Purchaser.

ii. Any upward revision and/or additions consequent to errors, omissions, ambiguities, discrepancies in the Bidding Documents which the SI had not brought out to the Purchaser's notice in his bid shall not constitute a change order and such upward revisions and/or addition shall be carried out by SI without any time and cost effect to Purchaser.

#### 14.1.4.2 Change Order

i. The Change Order will be initiated only in case (i) the Purchaser directs in writing the SI toinclude any addition to the scope of work covered under this Contract or delete any part of the scope of the work under the Contract, (ii) SI requests to delete any part of thework which will not adversely affect the operational capabilities of the facilities and if thedeletions proposed are agreed to by the Purchaser and for which cost and time benefitsshall be passed on to the Purchaser, (iii) the Purchaser directs in writing the SI to incorporate changes or additions to the technical specifications already covered in theContract.

ii. Any changes required by the Purchaser over and above the minimum requirements given in the specifications and drawings etc. included in the Bidding Documents beforegiving its approval to detailed design or Engineering requirements for complying with technical specifications and changes required to ensure systems compatibility and reliability for safe operation (As per codes, standards and recommended practices referred in the Bidding Documents) and trouble free operation shall not be construed to be change in the Scope of work under the Contract.

iii. Any change order as stated in this RFP comprising an alteration which involves changein the cost of the works (which sort of alteration is hereinafter called a "Variation") shall be the Subject of an amendment to the Contract by way of an increase or decrease inthe schedule of Contract Prices and adjustment of the implementation schedule if any.

iv. If parties agree that the Contract does not contain applicable rates or that the said ratesare inappropriate or the said rates are not precisely applicable to the variation in question, then the parties shall negotiate a revision of the Contract Price which shallrepresent the change in cost of the works caused by the Variations. Any change ordershall be duly approved by the Purchaser in writing.

v. Within ten (10) working days of receiving the comments from the Purchaser or the drawings, specification, purchase requisitions and other documents submitted by the SI for approval, the SI shall respond in writing, which item(s) of the Comments is/are potential changes(s) in the Scope of work of the RFP document covered in the Contract and shall advise a date by which change order (if applicable) will be submitted to the Purchaser.

**14.1.5 Testing and Acceptance Criteria**

i. SI shall demonstrate the following mentioned acceptance criteria prior to acceptanceof the solution as well as during project operations phase, in respect of scalability andperformance etc. The SI may propose further detailed Acceptance criteria which thePSCDL/DRDM will review. Once PSCDL/DRDM provides its approval, the Acceptance criteria can be finalized. In case required, parameters might be revised by PSCDL/DRDMin mutual agreement with bidder and the revised parameters shall be considered for acceptance criteria. A comprehensive system should be set up that would have the capability to log & track the testing results, upload & maintain the test cases and log &track issues/bugs identified.

ii. The following table depicts the details for the various kinds of testing envisaged for the project:

Note:

a. Bidder needs to provide the details of the testing strategy and approach including details of intended tools/environment to be used by SI for testing in its technical proposal. RAILTEL/ DRDM/ PSCDL does not intend to own the tools.

b. The SI shall work in a manner to satisfy all the testing requirements and adhere to the testing strategy outlined. The SI must ensure deployment of necessary resources and tools during the testing phases. The SI shall perform the testing of the solution based on the approved test plan, document the results and shall fix the bugs found during the testing. It is the responsibility of SI to ensure that the end product delivered by the SI

meets all the requirements specified in the RFP. The SI shall take remedial action based on outcome of the tests.

c. The SI shall arrange for environments and tools for testing and for training as envisaged. Post Go-Live; the production environment should not be used for testing and training purpose. If any production data is used for testing, it should be masked, and it should be protected. Detailed process in this regard including security requirement should be provided by the SI in its technical proposal. The process will be finalized with the selected bidder.

d. All the Third-Party Auditors (TPA) as mentioned above will be appointed and paid by RAILTEL / DRDM/ PSCDL directly. All tools/environment required for testing shall be provided by the SI.

e. STQC/Other agencies appointed by RAILTEL / DRDM/ PSCDL shall perform the role of TPA. SI needs to engage with the TPA at the requirement formulation stage itself. This is important so that unnecessary re-work is avoided, and the audit is completed in time. The audit needs to be completed before Go-Live of different phases. SI needs to prepare and provide all requisite information/documents to third party auditor and ensure that there is no delay in overall schedule.

f. The cost of rectification of non-compliances shall be borne by the SI.

#### 14.1.6 Factory Testing

SI shall have to submit Factory Test Certificate for the below mentioned materials before the actual supply of the items.

i. Cable
ii. Pole
iii. Signal Aspects

Authorized representative from RAILTEL / DRDM/ PSCDL will visit the manufacturing plant of the product subject to present in India. Authorized representative will check the testing process.

#### 14.1.7 Final Acceptance Testing

The final acceptance shall cover 100% of the I Project, after successful testing by the RAILTEL / DRDM/ PSCDL, Police Department, other stakeholders/end user department or its PMU; a Final Acceptance Test Certificate (FAT) shall be issued by the RAILTEL/ DRDM/ PSCDL to the SI.

Prerequisite for Carrying out FAT activity:

i. Detailed test plan shall be developed by the SI and approved by RAILTEL / DRDM/ PSCDL. This shall be submitted by SI before FAT activity to be carried out.

ii. All documentation related to ICCC Project and relevant acceptance test document (Including IT Components, Non-IT Components etc.) should be completed & submitted before the final acceptance test to the RAILTEL / DRDM/ PSCDL.
iii. The training requirements as mentioned should be completed before the final acceptance test.
iv. Successful hosting of Application, NMS and MIS Software.
v. For both IT & Non-IT equipment's / software manuals / brochures / Data Sheets / CD / DVD / media for all the Puducherry Project supplied components.

The FAT shall include the following:

I. All hardware and software items must be installed at respective sites as per the specification.
II. Availability of all the defined services shall be verified.
III. The SI shall be required to demonstrate all the features / facilities / functionalities as mentioned in the RFP.
IV. The SI shall arrange the test equipment required for performance verification and will also provide documented test results.
V. The SI shall be responsible for the security audit of the established system to be carried out by a certified third party as agreed by RAILTEL / DRDM/ PSCDL.

Any delay by the SI in the Final Acceptance Testing shall render him liable to the imposition of appropriate Penalties. However, delays identified beyond the control of SI shall be considered appropriately and as per mutual agreement between RAILTEL / DRDM/ PSCDL and SI. In the event the SI is not able to complete the installation due to non-availability of bandwidth from the bandwidth service providers, the Supplier and RAILTEL / DRDM/ PSCDL may mutually agree to redefine the Network so the SI can complete installation and conduct the Final Acceptance Test within the specified time.

## 15 Annexure III: Project Milestones and Payment Schedules for Implementation

### Project Implementation and Timelines

**Payments will be paid to SI on awarding the contract on back-to-back basis on receipt of payments from client against the invoices submitted by SI.**

**The contract Management & Paying Authority shall be Corporate Office, RailTel Corporation of India, New Delhi**

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

T = Date of signing of Contract Agreement

**G= Go-Live Date**

The Payment schedule and milestones are divided into two phases:

i. Implementation phase

ii. Operations and maintenance phase

Based on findings of the Feasibility Study done by the SI, the SI may propose a change in the number of sites or individual units to be deployed in each phase as well as overall scope and a consequent change in phasing. PSCDL also retains the right to Suo-moto change the number of sites or individual units to be deployed for each scope item. The final decision on change in phasing and related change in payment schedules shall be at the discretion of PSCDL.

| Milestone | Payment Milestones for Implementation | Payment Schedule | Time Schedule | Deliverable |
|---|---|---|---|---|
| M1 | Contract / Work Order | NA | T | NA |
| M2 | Project Kickoff | NA | T + 7 days | NA |
| M3 | Site Survey | NA | T + 1 month | 1. Project Implementation Plan.<br>2. Site Survey report<br>3. Final BoQ<br>4. Inception Report |
| M4 | Solution design signoff | NA | T + 45 days | 1. Functional Requirement Specification document 2. System Requirement Specification document 3. Requirements Traceability Matrix 4. High Level Design documents 5. Low Level Design documents |

| | | | | |
|---|---|---|---|---|
| M5 | Supply of IT and Non-IT Infra and systems pertaining to all the Solution components. | 50%% of the Capex Cost on pro-rata Basis | T + 3 months | 1. Infra and Systems delivery report ( delivery challan).<br>2. Material inspection report signed by the Authority.<br>3. Tax Invoice<br>4. Packing list<br>5. QA/COQ<br>6. Inspection Certificate<br>7. Consignee receipt<br>8. Warranty Certificate of OEM<br>9. Insurance certificate<br>10. Certificate duly signed by firm certifying that equipment/materials being delivered are new and conformed to technical specification<br>11. Undertaking for fall clause |
| | | | | |
| M6 | Installation and Commissioning of<br>1. General Surveillance.<br>2. ITMS<br>3. Other Smart solution | 25%of the Capex Cost | T + 5 months | Installation and commissioning certificate duly signed by RailTel official, Customer and SI. |

| | | | | |
|---|---|---|---|---|
| | components<br>4. OFC Connectivity<br>5. ICCC<br>6. Any other CAPEX items. | | | |
| M8 | Completion of Integration of Smart devices and existing applications with ICCC and Go-Live | 25% of the Capex Cost | T + 6 months | 1. UAT report<br>2. Training Completion report<br>3. Go-live certificate. |
| M9 | Operations and maintenance | 100% of the Opex cost | 5 years from Go-Live | 100% of the Opex cost equally spread across quarterly payments in arrears from Go-Live . |

**Note:**

i. In cases of fire or any major accidents caused due to the negligence, omissions and commissions of the SI in any of the installations, the liability is on SI for his commissions and omissions in the interim and final ICCC, DC deployments and operations during the O&M phase of sixty months.

ii. It is fixed by a third party auditor on the part of the SI, the claims shall be a minimum of the loss fixed by any third party auditor including the loss of lives, data, equipment, etc. added cumulatively on dues from the SI and will be recovered from the SI.

iii. Single component / multiple components Go-Live shall be awarded on successful completion of the respective component(s) and integration of respective component with ICCC.

iv. In case of partial achievement of the project milestone, the payment shall be made proportionately.

v. SI is required to provide comprehensive O&M of 5 years from the date of Go-Live provided for multiple components / single component outlined in the RFP.

vi. All payments to the Implementation Vendor shall be made upon submission of invoices along with necessary approval certificates from the concerned Authority like PSCDL/DRDM.

vii. In case of Internet Bandwidth (ISP services), System Integrator need to submit the invoices from Internet Service Provider (ISP) in the name of Tender Inviting Authority.

**Mobilization Advance**

The Authority will, if requested by the CONTRACTOR, make mobilization advance payments subject to approval and receipt of advance from the client of 10(%) percent of the Awarded Contract Value to the CONTRACTOR to assist in defraying the initial expenses that will necessarily be incurred by the CONTRACTOR for mobilization and design. The payment of mobilization advance is subject to the approval & receipt of mobilization advance from the client. The Mobilization Advance will be given to the CONTRACTOR with Simple Interest of 10 % (Percent) per annum.

The Advance payment will be made in two equal instalments of 5% (five percent) of the contract price. Advance payment will be paid only after CONTRACTOR submitting unconditional and irrevocable Bank guarantee for an amount equivalent to 110 % (one Hundred and Ten percent) of each instalment.

The Authority's Representative shall issue an Interim Payment Certificate for the first instalment. The Authority will make payment of the First instalment of the mobilization advance only after the CONTRACTOR has fulfilled the following conditions:

a) Execution of the Form of Agreement by the parties hereto and submission of Performance Security bythe CONTRACTOR.

b) Mobilized the Project Manager for the Contract.

c) Established and staffed a functional design liaison office at Puducherry city.

After the first instalment of the advance payment has been utilized as per the approved Programme, and to the satisfaction of the Authority's Representative, the CONTRACTOR may then apply for the Second instalment.

The Authority will make payment of the Second installment after the CONTRACTOR has successfully fulfilled the following conditions:

a) Submitted the proposed Implementation Programme for approval by the Authority's Representative.

b) Submitted, for approval by the Authority's Representative, mobilization/ deployment schedules for:

i. CONTRACTOR's key personnel required for managing, executing and supervising the Works,

ii. CONTRACTOR's Plant, Machinery and Equipment required for executing the Works; and

iii. Procurement Schedule for materials to be incorporated into the Permanent Works.

c) Submitted a Cash Flow Forecast for approval by the Authority's Representative.

d) Submitted a list of proposed, suppliers and manufacturers, along with their credentials, for approval by the Authority's Representative.

e) Submitted details of funds mobilized by himself as per the Cash Flow Forecasts.

f) Actual deployment of: (i) such Personnel, (ii) Machinery and Equipment,

g) Established the fully furnished Site office.

h) Placed confirmed orders for supply of major items of material which is to be incorporated into the Permanent Works as per the approved procurement schedule.

i) Commenced construction work at the Site in accordance with the approved construction program.

Deduction of Mobilization Advance: Mobilization advance shall be deducted starting from Second Interim Payment certificate @ of 10 % (Percent) of the certified amount of Interim payment certificate and to be recovered fully prior to the time when 90 percent (90%) of the work is completed.

A bank Guarantee of 110 (%) percent against the Mobilization advance is to be submitted. The mobilization advances and interest on it shall be adjusted and recovered in the Interim Payment Certificates raised by the Contractor for the work completed as mentioned above. The bank Guarantee submitted against mobilization advance has to be valid till completion of the work. In case, the Contractor fails to mobilize necessary manpower, machinery, materials and any necessary procurement or purchase to start the preliminary work, the bank guarantee against mobilization advance may be forfeited and will lead to the termination of contract.

### 15.1 Quality Assurance

A thorough quality check is proposed for the Puducherry Project and its modules, as per standard Software Development Life Cycle (SDLC). SI is expected to lay down a robust Quality Assurance program for testing of the developed application for its functionality, performance and security before putting in production environment. The program must include an overall plan for testing and acceptance of system, in which specific methods and steps should be clearly indicated and approved by RAILTEL & PSCDL. SI is required to incorporate all suggestions / feedback provided after the elaborate testing of the system, within a predefined, mutually agreed timeline. SI must undertake the following:

i. Outline the methodology that will be used for testing the system.
ii. Define the various levels or types of testing that will be performed for system.
iii. Provide necessary checklist/documentation that will be required for testing the system.
iv. Describe any technique that will be used for testing the system.
v. Describe how the testing methodology will conform to the requirements of each of the functionalities and expected outcome.
vi. Indicate / demonstrate to RAILTEL & PSCDL that all applications installed in the system have

been tested.

## 16 Annexure V : Guidelines

Common guidelines regarding compliance of the system / equipment:

i. The functional requirements and technical specifications provided in the below sections and at other sections in this RFP are indicative and carry guiding rule. The SI is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards & best practices adopted in the industry. The SI is encouraged to design an Optimised solution which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical requirement in the RFP may be considered if it is required for meeting current & future requirements during the contract period. The SI is fully responsible for the specified outcome to be achieved.

ii. The specifications mentioned for various IT / Non-IT components are indicative requirements and should be treated for benchmarking purpose only. SIs are required to undertake their own requirement analysis and may propose higher specifications that are better suited to the requirements.

iii. In case of addition/update in number of license for the Integrated Command and Control Centre (ICCC) software and VMS licenses for Cameras, the SI is required to meet of technical specifications contained in the RFP and for the upward revisions and/or additions of licenses is required be made as part of change order and cost would be commensurate to the itemized rate approved at the LOI issuance.

iv. Any manufacturer and product name mentioned in the Tender should not be treated as a recommendation of the manufacturer / product.

v. None of the IT / Non-IT equipment's proposed by the SI should be End of Life product. It is essential that the technical proposal is accompanied by the OEM certificate in the format given in Volume I of this Tender, where-in the OEM will certify that the product is not end of life product & shall support for at least 6 years from the date of Bid Submission.

vi. All IT Components should support IPv4 and IPv6

vii. Technical Bid should be accompanied by OEM's product brochure / datasheet. SIs should provide complete make, model, part numbers and sub-part numbers for all equipment/software quoted, in the Technical Bid.

viii. SI should ensure that only one make and model is proposed for one component in Technical Bid for example all Traffic Surveillance cameras must belong to a single OEM and must be of the same model etc.

ix. SIs should ensure complete warranty and support for all equipment from OEMs. All the back-to back service agreements should be submitted during the contract whereas MAF for all the equipment from OEMs shall be shared along with the Technical Bid as per Format given in the RFP.

x. All equipment, parts should be original and new.

xi. The user interface of the system should be a user friendly Graphical User Interface (GUI).

xii. Critical core components of the system should not have any requirements to have proprietary platforms and should conform to open standards.

xiii. For custom made modules, industry standards and norms should be adhered to for coding during application development to make debugging and maintenance easier. Object oriented programming methodology must be followed to facilitate sharing, componentizing and multiple- 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 Police Department.

xiv. All the Clients Machines / Servers shall support static assigned IP addresses or shall obtain IP addresses from a DNS/DHCP server.

xv. The Successful SI should also propose the specifications of any additional servers / other hardware, if required for the system.

xvi. The indicative architecture of the system is given in this volume. The Successful SI must provide the architecture of the solution it is proposing.

xvii. The system servers and software applications will be hosted in Data Centers as specified in the Bid. It is important that the entire set of Data Center equipment are in safe custody and have access from only the authorized personnel and should be in line with the requirements & SLAs defined in the Tender.

xviii. The Servers provided should meet industry standard performance parameters (such as CPU Utilisation of 60 percent or less, disk utilisation of 75 percent or less). In case any non-standard computing environment is proposed (such as cloud), detail clarification needs to be provided in form of supporting documents, to confirm (a) how the sizing has been arrived at and (b) how SLAs would be met.

xix. SI is required to ensure that there is no choking point / bottleneck anywhere in the system (end- toend) and enforce performance and adherence to SLAs. SLA reports must be submitted as specified in the Bid without fail.

xx. All the hardware and software supplied should be from the reputed Original Equipment Manufacturers (OEMs). Department reserves the right to ask replacement of any hardware / software if it is not from a reputed brand and conforms to all the requirements specified in the tender documents.

xxi. Cameras, Network Video Recorder (NVR) 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.

xxii. SI shall place orders on various OEMs directly and not through any sub-contractor / partner. All licenses should be in the name of the RAILTEL & PSCDL

xxiii. Technical Solution and Architecture : All the components of the Technical Architecture which should comply with the published eGovernance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in and leading industry standards.

xxiv. Consider architecture design with respect to scalability, inter-operability , availability, manageability and comply with framework Smart City (K-15016/61/2016-SC-1, Government of India, and Ministry of Urban Development)

## 17 Annexure VI Security – General Guidelines

### 17.1 Security Framework

The Bidder shall develop Security Framework aimed at building a secure and resilient security space for citizens and stakeholders of Smart City. The Framework shall be designed to protect information and infrastructure; build capabilities to prevent and respond to attacks; and minimize damages through coordinated efforts of institutional structures, people, processes, and technology. Framework shall cover security architecture.

### 17.2 Security Policy

The policy shall address security of hardware and software, along with the connectivity between the field device and the respective application software. The bidder shall ensure to develop and implement Standard Operating Procedures for smooth Operations and Maintenance of IT infrastructure.

### 17.3 Security Governance

1. The Bidder shall conduct Risk Assessment and prepare Risk Treatment Plan for the IT applications and infrastructure deployed in smart city ecosystem.
2. The Bidder shall facilitate management reporting in form of dashboard covering Risk Assessment results along with risk treatment plan and timeline to the smart city management.
3. The Bidder shall implement all the controls as identified during the Risk assessment and treatment plan as per the agreed

### 17.4 Smart City IT Asset Management

1. The Bidder shall utilize automated asset management tools to prepare the information asset register (IAR) for all IT assets deployed in the Smart city. The IAR shall capture criticality, rating, classification, owner and custodian of the Asset.
2. The Bidder shall develop and implement an appropriate set of procedures for information labelling and handling in accordance with the classification scheme proposed in the security policy of smart city.

### 17.5 Physical & Environmental Security

4. The bidder shall implement and manage physical security of IT assets of smart city, which shall include, as a minimum: locks, alarms, surveillance equipment, sensors, access control systems (biometrics), etc. The bidder shall also design processes and procedures for same.
5. The Bidder shall ensure that all the equipment, information or software shall not be taken off-site without appropriate authorization.

### 17.6 Access Control

1. The Bidder shall ensure that users shall be provided single sign on functionality if required for the applications and solutions deployed in Smart City.
2. The smart city solution should support multiple authentication methods such as Username password, two factor authentication, digital certificate and biometric based authentication.
3. The solution should be capable of being deployed on mobile devices deployed for smart city
4. Solution should have the capability to define access based on time of day, day of week or by group or user defined access.
5. The smart city solution should have the functionality to provide authentication based on the role.

6. Remote access to all smart city IT users shall be securely managed.
7. The smart city solution should be able to deploy and configure the approved password policy and should provide the feature to configure the logs.
8. The smart city solution should have the option of blocking multiple sessions for the user.
9. All smart city applications should support role based access control to enforce separation of duties.
10. The application deployed in smart city should display the last login status (successful/unsuccessful, time) to the user and should not store authentication credentials on client computers after a session terminates
11. All smart city solution should be compliant with Indian IT Act, 2000 and Amended IT Act, 2008

### 17.7 Communications and Operations Management

1. Bidders must ensure that the IT systems in the smart city infrastructure are open, scalable and interoperable. The deployed systems must operate within 4 layers – Sensory layer, communication layer, data layer and application layer adhering to relevant security controls as mandated by the MoUD guidelines.
2. Bidders shall ensure that all the interfaces between IoT devices, field sensors, device applications and storage deployed in smart city are encrypted using appropriate protocols, algorithm and key pairs.
3. All transport link communication must be encrypted and sensitive data both in rest and transit is to be secured using encryption.
4. Bidders must ensure that all the changes made to the smart city infrastructure incl. of IoT field devices, sensors and related applications should be tracked and recorded in order to enable security monitoring of the infrastructure. The maintained logs should be systematically collated, enabling the access of critical information as per date, fortnight, month, quarter, year etc.
5. Bidders should ensure that separate environments are maintained for production, test and development for smart city infrastructure and solutions to reduce the risks of unauthorized access or changes.
6. Bidders must ensure that smart city IT systems are designed in such a way that only authenticated users have access to the smart city database. Also, the provision of access has to be routed only through designated applications.
7. Bidders must ensure that sensitive data is stored in the smart city database in an encrypted format thereby curtailing the database administrator from reading or modifying the stored sensitive data.

8. Bidders must ensure that the smart city architecture should include a VPN solution enabling designated users to access necessary applications and functions from remote applications.
9. Bidders must enable for the maintenance of an audit trail to record all the administrator, user level activities including the failed attempts thereby enabling a robust high level security monitoring of the smart city security infrastructure.
10. Bidders must ensure that the smart city components – Network elements, Operating system, Applications etc. are in sync and adhere to a singular master clock. Thereby ensuring an appropriate logging/ time stamping of incidents and bolstering smooth operation of the smart city.
11. Bidders must ensure that adequate security controls are deployed against the tampering of log information and unauthorized access to the smart city infrastructure such as the data center, IoT device control room etc.
12. Bidders must ensure that platforms hosted in the central data center support multi-tenancy with adequate authentication and role based access. This can be achieved by utilizing Authentication and privilege management technology thereby controlling the access of data as per user privileges.
13. Bidders must ensure that the smart city architecture accounts for latency issues for the flow of data between devices. Suitable protocols should be utilized to minimize data flow latency upon management of heterogeneous data.
14. Bidders must strictly make sure that the communication between IoT field devices and their respective management applications happens only over a data layer (digital platform). Thereby enabling this designated layer to be the one true source of data abstraction, normalization and correlation.
15. Bidders must ensure that the smart city IT infrastructure including the Wi-Fi network adheres to relevant and applicable security standards and protocols. Also, bidders must make sure that the Application Program Interfaces (APIs) are published and the IT systems run on standard protocols.
16. Bidders must ensure that the smart city architecture end-to-end has adequate security controls to enforce safety, privacy and integrity of confidential data. Necessary controls must be deployed to protect the integrity of data flowing into the control systems and other critical infrastructure.
17. Bidders must enable for wireless/ broadband architecture used in the smart city infrastructure to interface with other/citywide wireless networks thereby enabling interoperability.
18. Bidders must ensure that IoT field devices and sensory equipment operating within the smart city periphery connect only to authorize wireless networks. Secure Wi-Fi guidelines as prescribed by the Department of Telecom must be followed.

19. Bidders must make sure that the wireless layer of the smart city network is appropriately segmented, bifurcating the network into various trusted zones. Thereby segregating public and utility networks via VPN (Virtual private networks), ensuring that the traffic from internet users is not routed into sensor networks and vice versa.
20. Bidders must enable for the authentication of the sensory equipment during the provisioning of the sensors and connection into the smart city infrastructure.
21. Bidders must ensure that the data aggregators used for enabling the interoperability between field IoT devices and sensors functioning on different protocols incorporate appropriate authentication and encryption at the aggregator gateway when field devices are not capable of authenticating
    /encrypting critical information.
22. Bidders must ensure that the IoT field devices and sensory equipment deployed in smart city periphery must not have a physical interface for administration. System and Network monitoring should be only performed remotely thereby ensuring local cyber-attacks/ tampering of field devices is curtailed.
23. Bidders must ensure appropriate network segregation. The smart city data center must be systematically segmented into multiple zones. Each zone must have a dedicated functionality. IoT field devices and sensory equipment must be connected to a completely separate network isolated from public networks and other private networks.
24. Bidders must make sure that the internet facing segment of the data center must incorporate a DMZ (Demilitarized zone), where customer application servers would be located. Predefined ports must be assigned for enabling the communication between the customer application servers and utility application servers to facilitate the access/transfer of data.
25. Bidders must ensure that Smart city data centers are well equipped with adequate security controls to protect the confidentiality, integrity and accessibility of critical data. The center should consider including cyber security systems such as firewalls, Intrusion detection & Intrusion prevention systems, Web Application Firewalls, Behavioral analysis systems for anomaly detection, Correlation engine, Denial of Service prevention device, Advanced Persistent Threat notification mechanism, Federated identity, access management system etc.
26. Bidders must ensure that the proposed smart city architecture provides for:
    i Automatic and secure firmware updates
    ii Device logging and auditing capabilities
    iii Vendor self-certification for non-existence of backdoors, undocumented and hard codedaccounts.
    iv Bidders shall ensure that Data encryption at rest shall be implemented using

departmentsmanaged keys, which are not stored in the cloud.

### 17.8 Information Systems Acquisition, Development and Maintenance

1. The Bidder shall prepare the detailed technical security requirement as part of the 'Software Requirement Specification' document with secure coding guidelines for development of applications for smart city.
2. The Bidder shall incorporate validation checks into smart city applications to detect any corruption of information through processing errors or deliberate acts.
3. The Bidder shall obtain information about technical vulnerabilities of information systems being used in smart city, evaluate the exposure to such vulnerabilities, and take appropriate measures to address the associated risk.
4. The bidder shall implement maintenance and repair process of smart city IT assets in timely manner, with approved and controlled tools.

### 17.9 Business Continuity Planning and Disaster Recovery

1. The Bidder shall implement and operate Disaster Recovery site for the Smart city infrastructure and related IT & OT applications. IT & OT applications and processes should be supported from the disaster recovery site.

2. The Bidder shall define Business Continuity and Disaster Recovery plan and will perform the testing on a yearly basis

### 17.10 Information Security Audits

The bidder shall ensure Information security audits of the smart city infrastructure and related applications by a CERT-In empaneled vendor. VA/PT (Vulnerability assessment and Penetration Testing) activities, audits and application security testing must be carried out on once-a-year basis ensuring optimal operation and security of the smart city infrastructure and applications. Teams carrying out the audit exercise must be different from the implementation teams. Systematic actionable need to be derived post audits and necessary changes need to be made periodically.

### 17.11 Awareness Training

The bidder shall deploy appropriate resources to support periodic awareness training based on latest standards of ISMS in consultation with the Authorities. The trainings must focus on educating relevant employees (including privileged users, third party, senior management etc.) on necessary security practices and processes to be followed in order to maintain the Confidentiality, Integrity and

Availability of critical data.

### 17.12 Security Controls for Cloud Services

The security controls for creating and managing cloud services shall comply with the following guidelines. Empanelment of Cloud Service Offerings CSPs facilities/services shall be compliant with regulative directives and industry best practices. The SLA shall be based on the guidelines issued by Government Departments on contractual terms related to Cloud Services (MeitY guideline dated 31/03/17). The security controls should include the following:

1) The CSP should be empaneled by MeitY for providing cloud services. The CSPs facilities/services shall be certified to be compliant to the following standards: ISO 27001, ISO 27017, ISO 27018, ISO 20000- 9, ISO/IEC 20000-1 & PCI DSS.
2) The CSP/Service Provider shall comply or meet any security requirements applicable to CSPs/Service Providers published (or to be published) by MeitY or any standards body setup / recognized by Government of India from time to time and notified to the CSP/Service Providers by MeitY as a mandatory standard.
3) The CSP/Service Provider shall meet all the security requirements indicated in the IT Act 2000, the terms and conditions of the Provisional Empanelment of the Cloud Service Providers and shall comply with the audit criteria defined by STQC.
4) Incident Management shall be managed by CSP / third party.
5) Periodic secure code review shall be performed for cloud applications.
6) Data encryption at rest / transit depending on sensitivity of data shall be implemented using departments managed keys, which are not stored on the cloud.
7) The CSP will undertake to treat information passed on to them as classified. Such Information will not be communicated / published / advertised by the CSP to any person/organization without the express permission of the Department.
8) CSP shall inform all security breach incidents to Smart City management on real time.
9) CSP shall ensure data confidentiality and mention Sub-contractual risk shall be covered by CSP.
10) E-Discovery shall be included as clause in SLA with CSP. It is the process of locating, preserving, collecting, processing, reviewing, and producing Electronically Stored Information (ESI) in the context of or criminal cases/proceedings or investigation. Logging and reporting (e.g., audit trails of all access and the ability to report on key requirements/indicators) must be ensured.
11) The Law Enforcement Agency as mandated under any law for the time being in force may seek access to information stored on cloud as provided by the Service Provider. The onus shall be on the CSP to perform all due diligence before releasing any such information to any

such law enforcement agency.

12) CSP must ensure location of all data related to smart cities in India only.
13) The Cloud Service Provider's services offerings shall comply with the audit requirements defined under the terms and conditions of the Provisional Empanelment of the Cloud Service Providers (or STQC /MEITY guidelines. The Audit, Access and Reporting Requirements should be as per the terms and conditions of the Provisional Empanelment of the Cloud Service.
14) CSP's exit Management Plan shall include - Transition of Managed Services & Migration from the incumbent cloud service provider's environment to the new environment and shall follow all security clauses for smooth transition.
15) SLA with CSP shall cover performance management & dispute resolution escalation. Guidelines on Service Level Agreement issued by MeitY lists out the critical SLAs for cloud services.
16) Identification and problem resolution (e.g., helpline, call center, or ticketing system) mechanism must be defined.
17) Change-management process (e.g., changes such as updates or new services) must be defined.
18) Appropriate segregation of Virtual Private Cloud (VPC) security rules defined as part of firewall to restrict access, Role based access management, Logging and monitoring shall be ensured.
19) VPN gateway must be setup to ensure controlled access, appropriate security rules must be employed to encrypt outward data flow, IDS, IPS, API Gateways to be setup and ELB logs to be maintained for any activities and access and exceptions to carried out in the cloud setup, Database logs to be routed as part of the Logging VPC setup.
20) Digital Certificate shall be implemented for secure access.
21) Web Application Firewall must be provided, Host IPS must be setup on all the Web servers, Web servers must be configured as per the CIS hardening guidelines and baseline security requirements, logging and monitoring should be enabled.
22) Application access between hosted smart city applications shall be segregated, internal infrastructure and external traffic, Role based access must be defined, hardening of database instances as per the CIS baselines configuration guidelines in the cloud setup must be ensured, Logging and monitoring must be enabled.
23) For SLAs to be used to steer the behavior of a cloud services provider, imposition of financial penalties is to be incorporated.
24) Monitor Vendor Service level agreement for annual end-to-end service availability of 99.999 percent. The end to end service agreement should be in place for minimum period of six years form the date of operations of the systems.

## 18 Annexure VI – Smart City Guidelines

Universal Access IT Systems to empower differently-abled citizens to access ICT systems with ease

| Sl. | Parameters No. | Minimum Requirements |
|---|---|---|
| 1 | Text Alternatives | Provide text alternatives for any non-text content so that it can be changed into other forms people need, such as large print, braille, speech, symbols or simpler language. |
| 2 | Non-text Content | All images, form image buttons, and image map hot spots have appropriate, equivalent alternative text.<br>Images that do not convey content, are decorative, or contain content that is already conveyed in text are given null alt text (alt="") or implemented as CSS backgrounds. All linked images have descriptive alternative text. Equivalent alternatives to complex images are provided in context or on a separate (linked and/or referenced via longdesc) page. |
| 3 | Time-based Media | Provide alternatives for time-based media. |
| 4 | Audio Description or Media Alternative (Prerecorded) | A descriptive text transcript OR audio description audio track is provided for non-live, web-based video |
| 5 | Adaptable | Create content that can be presented in different ways (for example simpler layout) without losing information or structure. |
| 6 | Info and Relationships | Semantic markup is used to designate headings (<h1>), lists (<ul>, <ol>, and <dl>), emphasized or special text (, <code>, <abbr>, <blockquote>, for example), etc. Semantic markup is used appropriately.<br>Tables are used for tabular data. Where necessary, data cells are associated with their headers. Data table captions and summaries are used where appropriate.<br>Text labels are associated with form input elements. Related form elements are grouped with fieldset/legend. |
| 7 | Meaningful Sequence | The reading and navigation order (determined by code order) is logical and intuitive. |

| | | |
|---|---|---|
| 8 | Use of Color | Color is not used as the sole method of conveying content or distinguishing visual elements.<br>Color alone is not used to distinguish links from surrounding text unless the luminance contrast between the link and the surrounding text is at least 3:1 and an additional differentiation (e.g., it becomes underlined) is provided when the link is hovered over or receives focus. |
| 9 | Audio Control | A mechanism is provided to stop, pause, mute, or adjust volume for audio that automatically plays on a page for more than 3 seconds. |
| 10 | Resize text | The page is readable and functional when the text size is doubled. |
| 11 | Images of Text | If the same visual presentation can be made using text alone, an image is not used to present that text. |
| 12 | Keyboard Accessible | Make all functionality available from a keyboard. |
| 13 | Keyboard | All page functionality is available using the keyboard, unless the functionality cannot be accomplished in any known way using a keyboard (e.g., free hand drawing).<br>Page-specified shortcut keys and accesskeys (accesskey should typically be avoided) do not conflict with existing browser and screen reader shortcuts. |
| 14 | No Keyboard Trap | Keyboard focus is never locked or trapped at one particular page element.<br>The user can navigate to and from all navigable page elements using only a keyboard. |
| 15 | Pause, Stop, Hide | Automatically moving, blinking, or scrolling content that lasts longer than 5 seconds can be paused, stopped, or hidden by the user. Moving, blinking, or scrolling can be used to draw attention to or highlight content as long as it lasts less than 5 seconds.<br>Automatically updating content (e.g., automatically redirecting or refreshing a page, a news ticker, AJAX updated field, a notification alert, etc.) can be paused, stopped, or hidden by the user or the user can manually control the timing of the updates. |
| 16 | Seizures | Do not design content in a way that is known to cause seizures. |
| 17 | Three Flashes or Below Threshold | No page content flashes more than 3 times per second. |
| 18 | Navigable | Provide ways to help users navigate, find content, and determine where they are |

| | | |
|---|---|---|
| 19 | Bypass Blocks | A link is provided to skip navigation and other page elements that are repeated across web pages. If a page has a proper heading structure, this may be considered a sufficient technique instead of a "Skip to main content" link. Note that navigating by headings is not yet supported in all browsers. If a page uses frames and the frames are appropriately titled, this is a sufficient technique for bypassing individual frames. |
| 20 | Page Titled | The web page has a descriptive and informative page title. |
| 21 | Focus Order | The navigation order of links, form elements, etc. is logical and intuitive. |
| 22 | Headings and Labels | Page headings and labels for form and interactive controls are informative. Avoid duplicating heading (e.g., "More Details") or label text (e.g., "First Name") unless the structure provides adequate differentiation between them. |
| 23 | Focus Visible | It is visually apparent which page element has the current keyboard focus (i.e., as you tab through the page, you can see where you are). |
| 24 | Readable | Make text content readable and understandable |
| 25 | Language of Page | The language of the page is identified using the HTML lang attribute |
| 26 | Language of Parts | The language of page content that is in a different language is identified using the lang attribute. |
| 27 | Predictable | Make Web pages appear and operate in predictable ways. |
| 28 | On Input | When a user inputs information or interacts with a control, it does not result in a substantial change to the page, the spawning of a pop-up window, an |
| | | additional change of keyboard focus, or any other change that could confuse or disorient the user unless the user is informed of the change ahead of time. |
| 29 | Compatible | Maximize compatibility with current and future user agents, including assistive technologies. |
| 30 | Parsing | Significant HTML/XHTML validation/parsing errors are avoided. In content implemented using markup languages, elements have complete start and end tags, elements are nested according to their specifications, elements do not contain duplicate attributes, and any IDs are unique, except where the specifications allow these features. |

| | | |
|---|---|---|
| 31 | Name, Role, Value | Markup is used in a way that facilitates accessibility. This includes following the HTML/XHTML specifications and using forms, form labels, frame titles, etc. appropriately.<br>For all user interface components, the name and role can be programmatically determined; states, properties, and values that can be set by the user can be programmatically set; and notification of changes to these items is available to user agents, including assistive technologies. |
| 32 | Audio-only and Videoonly (Pre-recorded) | A descriptive text transcript (including all relevant visual and auditory clues and indicators) is provided for non-live, web-based audio (audio podcasts, MP3 files, etc.) A text or audio description is provided for non-live, web-based video-only (e.g., video that has no audio track). |
| 33 | Captions (Prerecorded) | Synchronized captions are provided for non-live, web-based video (YouTube videos, etc.) |
| 34 | Captions (Live) | Synchronized captions are provided for all live multimedia that contains audio (audio-only broadcasts, web casts, video conferences, Flash animations, etc.) |
| 35 | Audio Description (Prerecorded) | Audio descriptions are provided for all video content<br>NOTE: Only required if the video conveys content visually that is not available in the default audio track. |
| 36 | Sensory Characteristics | Instructions do not rely upon shape, size, or visual location (e.g., "Click the square icon to continue" or "Instructions are in the right-hand column"). Instructions do not rely upon sound (e.g., "A beeping sound indicates you may continue."). |
| 37 | Distinguishable | Make it easier for users to see and hear content including separating foreground from background. |
| 38 | Contrast (Minimum) | Text and images of text have a contrast ratio of at least 4.5:1. Large text - at least 18 point (typically 24px) or 14 point (typically 18.66px) bold has a contrast ratio of at least 3:1. |
| 39 | Enough Time | Provide users enough time to read and use content. |
| 40 | Timing Adjustable | If a page or application has a time limit, the user is given options to turn off, adjust, or extend that time limit. This is not a requirement for real-time events (e.g., an auction), where the time limit is absolutely required, or if the time limit is longer than 20 hours. |

| | | |
|---|---|---|
| 41 | Link Purpose (In Context) | The purpose of each link (or form image button or image map hotspot) can be determined from the link text alone, or from the link text and its context (e.g., surrounding paragraph, list item, table cell, or table headers). Links (or form image buttons) with the same text that go to different locations are readily distinguishable. |
| 42 | Multiple Ways | Multiple ways are available to find other web pages on the site - at least two of: a list of related pages, table of contents, site map, site search, or list of all available web pages. |
| 43 | On Focus | When a page element receives focus, it does not result in a substantial change to the page, the spawning of a pop-up window, an additional change of keyboard focus, or any other change that could confuse or disorient the user. |
| 44 | Consistent Navigation | Navigation links that are repeated on web pages do not change order when navigating through the site. |
| 45 | Consistent Identification | Elements that have the same functionality across multiple web pages are consistently identified. For example, a search box at the top of the site should always be labeled the same way. |
| 46 | Input Assistance | Help users avoid and correct mistakes. |
| 47 | Error Identification | Required form elements or form elements that require a specific format, value, or length provide this information within the element's label. If utilized, form validation errors are presented in an efficient, intuitive, and accessible manner. The error is clearly identified, quick access to the problematic element is provided, and user is allowed to easily fix the error and resubmit the form. |
| 48 | Labels or Instructions | Sufficient labels, cues, and instructions for required interactive elements are provided via instructions, examples, properly positioned form labels, and/or fieldsets/legends. |
| 49 | Error Suggestion | If an input error is detected (via client-side or server-side validation), provide suggestions for fixing the input in a timely and accessible manner. |
| 50 | Error Prevention (Legal, Financial, Data) | If the user can change or delete legal, financial, or test data, the changes/deletions can be reversed, verified, or confirmed. |
| 51 | Visual Captcha | Alternative mode of authentication should be offered to in order to be authenticated |
| 52 | Mandatory use of Unicode for regional language | Unicode facilitates assistive technology to access content. |