PUDUCHERRY SMART CITY DEVELOPMENT LIMITED

REQUEST FOR PROPOSAL FOR SELECTION OF SYSTEM INTEGRATOR 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

RFP NO: 2

DATED: 01.06.2023

Table of Contents

1 Disclaimer 6

2 Definitions and Acronyms 7

3 Overview 9

3.1 Introduction 9

3.2 Vision 9

3.3 Project Background 9

3.4 Objective of the Project and RFP 10

3.4.1 Objective of the Project 10

3.4.2 Objective of the RFP 11

4 Project broad scope 13

5 Project Scope of Work 23

5.1 Assessment, Site Survey and Project Plan 23

5.2 Documents/ Drawings Submission after Award of Contract 24

5.2.1 Stage 1: Design engineering 24

5.2.2 Stage 2: Project execution 24

5.2.3 Stage 3: Post commissioning 25

5.3 Finalization of Detailed Technical Architecture 25

5.4 Site Clearance Obligations and Other Relevant Permissions 28

5.4.1 Survey And Commencement of Works 28

5.4.2 Existing Traffic Signal system 28

5.4.3 Electrical Works and Power Supply 28

5.5 Miscellaneous: 28

5.6 Design and Implementation of Integrated Command & Control Center System 29

5.7 Design, Supply, Installation & Commissioning of the Field Equipment 30

5.8 City Surveillance System – (CCTV Camera) 30

5.9 Integrated Traffic Management System (ITMS) 32

5.10 Lightning-Proof Measures 35

5.11 Earthing System 36

5.12 Junction Box / Outdoor Cabinet, Poles and Cantilever 36

5.13 Power & UPS - for Field Locations 38

5.14 Civil and Electrical Works 38

5.15 Cabling Infrastructure 39

5.16 Responsibility Matrix - Overall 39

5.17 Project Deliverables 42

5.18 Project Timelines – Phase wise 44

5.19 Project Timelines – Component wise 46
5.20 Project Defect Liability Period (DLP) / Warrantee of Product & Services 47
6. Functional Requirement and Technical Specifications 48
Details of Key Modules 48
6.1 Integrated Command and Control Centre 48
6.2 On Premise Data Centre (DC) 76
6.2.1. 42U Rack with All Accessories: 76
6.2.2 Core Router: 77
6.2.3. Firewall + IPS 78
6.2.4. Server Specification 82
6.2.5. Storage Specification 82
6.2.6. Hypervisor 83
6.2.7. Core Switch 84
6.2.8. TOR Switch & WAN Aggregation switch: 86
6.2.9. Access Switch -8 Port – POE 88
6.2.10. Access Switch-24 Port –POE 89
6.2.11 Wireless LAN Controller: 91
6.2.12. Indoor Access Points: 92
6.2.13 AAA Server: 94
6.2.14 Centralized-Anti Virus Solution For ICCC 95
6.2.15 Video wall and Video wall Controller 96
6.2.16 Lan Networking For ICCC 104
6.2.17 Centralized Help Desk 105
6.2.18 IP Phones 105
6.2.19 Three Monitoring Workstations: 107
6.2.20 Data Center & ICCC: Non-IT Components 109
6.2.21 Intranet router at DC: 109
6.2.22 Backbone Router 111
6.3 Cloud Services to deploy all smart solutions 126
6.4 Intelligent Traffic Management System 136
6.4.1 Key Issues 136
6.4.2 Indicative Key Outcomes and KPIs 136
6.4.3 Key components 137
6.4.4 Automatic Number Plate Recognition (ANPR) 137
6.4.5 Red Light Violation Detection (RLVD) 139
6.4.6 Speed Violation Detection (SVD) 139

6.4.7 Traffic Analytics 140
6.4.8 Adaptive Traffic Control System (ATCS) 141
6.4.9 Reports 143
6.4.10 Graphical User Interface 144
6.4.11 Video Management & Operator Functions 145
6.4.12 Entry Exit Point Management: 151
6.4.13 Corridor Management: 155
6.4.14 Variable Message Display 156
6.4.15 Specification for Speed Violation Camera: 158
6.4.16 Instant Speed Violation Detection: 160
6.4.17 Average Speed Violation Detection: 161
6.4.18 Wrong Side Driving Violation 161
6.4.19 Adaptive Traffic Control System 161
6.4.20 Automatic E Challan System: 185
6.5 Enterprise Management System (EMS) 188
6.6 Citizen Engagement System : Creation of Online and Mobile Applications 193
6.7 Smart Poles 201
6.7.1 Smart Pole Specification 201
6.7.2 Digital Bill Board 202
6.7.3 Environmental Sensors 203
6.7.4 Emergency Call Box: 211
6.7.5 IoT Gateway Specification 212
6.7.6 Public Address System 213
6.7.7 City Public Wi-Fi 215
6.8 Geographical Information System 217
6.9 Flood Sensors & Alert System 217
6.10 City Surveillance System 220
6.10.1 Video Management System: 223
6.10.2 City Surveillance fixed Camera Specifications 243
6.10.3 City Surveillance PTZ Camera Specifications 246
6.11 Smart Kiosks 248
6.12 Local Processing Units (LPU): 252
6.13 External IR Illuminator (Optional) 252
6.14 Network Connectivity - OFC 253
7 Approach and methodology to be adopted for implementation: 254
8 Lifecycle of implementation of ICT intervention: 256

9 Detailed Technical and Non-Technical Manpower: 257
10 Use cases to be deployed / integrated: 258
10.1 Digital Assistant Application 258
11 Training, Audit and Change Management Plan: 260
12 Proposed Governance Model: 261
13 Exit Management Under Contract Completion: 261
14 Detailed work Phases and considerations 263
14.1.1 Phase 1(Implementation Phase) 263
14.1.2 Phase-2 (Operations and Maintenance) 268
14.1.3 Project Management and Governance 268
14.1.4 Change Management & Control 270
14.1.5 Testing and Acceptance Criteria 272
14.1.6 Factory Testing 273
14.1.7 Final Acceptance Testing 273
15 Annexure III: Project Milestones and Payment Schedules for Implementation 274
15.1 Quality Assurance 277
16 Annexure V : Guidelines 278
17 Annexure VI Security – General Guidelines 280
17.1 Security Framework 280
17.2 Security Policy 280
17.3 Security Governance 281
17.4 Smart City IT Asset Management 281
17.5 Physical & Environmental Security 281
17.6 Access Control 281
17.7 Communications and Operations Management 282
17.8 Information Systems Acquisition, Development and Maintenance 284
17.9 Business Continuity Planning and Disaster Recovery 284
17.10 nformation Security Audits 285
17.11 Awareness Training 285
17.12 Security Controls for Cloud Services 285
18 Annexure VI – Smart City Guidelines 287

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	Meaning
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
Authority	RailTel Corporation of India Limited (RailTel) & DRDM / PSCDL
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

Terms	Meaning
KPI	Key Performance Indicator
LOA	Letter of Acceptance or Letter of Award
LAN	Local Area Network
LoI	Letter of Intent
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

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 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."**

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 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. • 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. • Live alerts in case of an event/ incident. • Help to identify, apprehend and prosecute offenders. • 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. • Better Management of Security breaches based on alerts received from system. • Provide assistance to emergency services and fast turn-around time.
Effective Monitoring	• Address detection of hot listing vehicles. • Assist in management and policing of large-scale events (political, religious etc.). • Aid to investigation by Police Department by integration of analytic tools. • Providing evidence for criminal and civil action in the courts.
Improved Traffic Management	• Address the manual Traffic Signaling in the city. • Optimizing the traffic movement with help of Adaptive Traffic Signal Control
Improved Management	• Help in maintaining Law & Order situations. • 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 Smart Cities

i. Operations and maintenance of DC & DR facility.
ii. Annual technical support for all hardware and software components for the O & M period
iii. Overall maintenance of the DC & DR facility and continuity of operations as per Service 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 reference to all related work, milestones and their progress during the implementation phase.
b) Formats for all above mentioned reports and their dissemination mechanism shall be discussed and finalized along with project plan. The Authorities on mutual agreement may change the formats, periodicity and dissemination mechanism for such reports.
c) Periodic meetings shall be held between the representatives of the Authorities and SI once in every 15 days during the implementation phase to discuss the progress of implementation. After the implementation phase is over, 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 of work are part of such meetings.
e) All the goods, services and manpower to be provided / deployed by SI under the Contract and the manner and speed of execution and maintenance of the work and services are to be conducted in a manner to the satisfaction of 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, SI shall 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 the right 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 in accordance with the standards committed to or required by the Authorities and SI undertakes to cooperate with and provide to the Authorities any other agency appointed by the Authorities, all Documents and other details as may be required by them for this purpose. Such audit shall not include SI's books of accounts.
h) Should the rate of progress of the works or any part of them at any time fall behind the stipulated time for completion or is found to be too slow to ensure completion of the works by the stipulated time, or is in deviation to Tender requirements/ standards, the Authorities' representative shall so notify SI in writing.
i) SI shall reply to the written notice giving details of the measures they propose to 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 be entitled to any additional payment for taking such steps. If at any time it should appear to the Authorities representative that the actual progress of work does not conform to the approved plan SI shall produce at the request of the Authorities representative a revised plan showing the modification to the approved plan necessary to ensure completion of the works within the time for completion or steps initiated to ensure compliance to the stipulated requirements.
j) The submission seeking approval by the Authorities of such plan shall not relieve 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 be taken care by SI. SI shall prepare and distribute Service level performance reports 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 should cover following aspects. The SI shall first carry out a detailed survey to identify & finalize the 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.

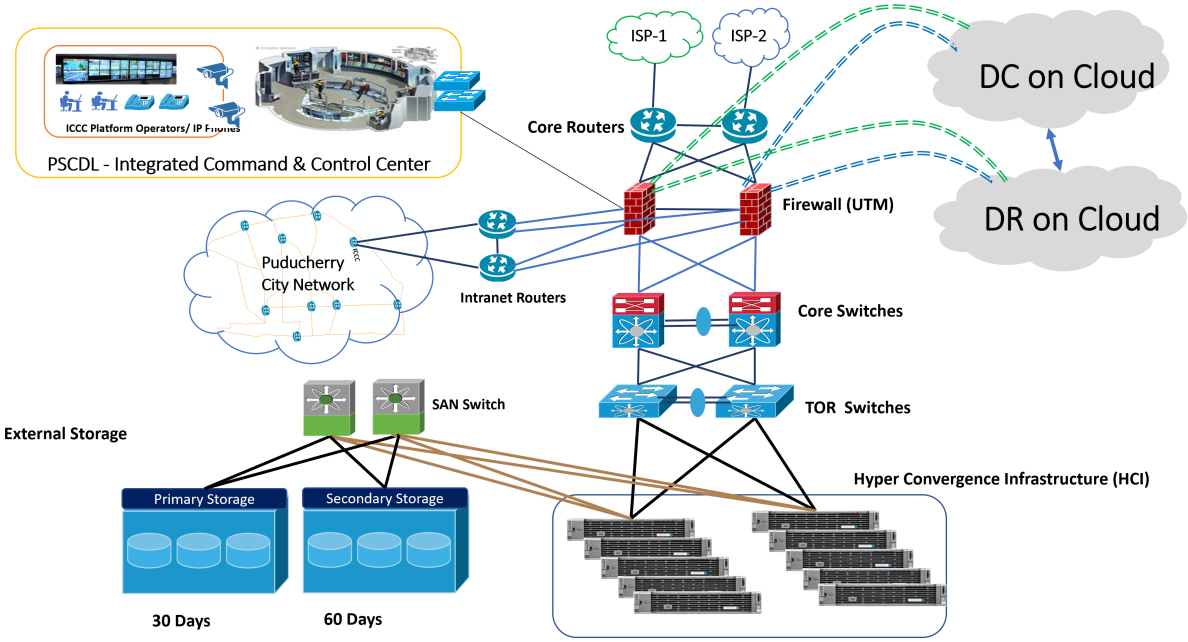
f) Installation manuals

5.2.3 Stage 3: Post commissioning

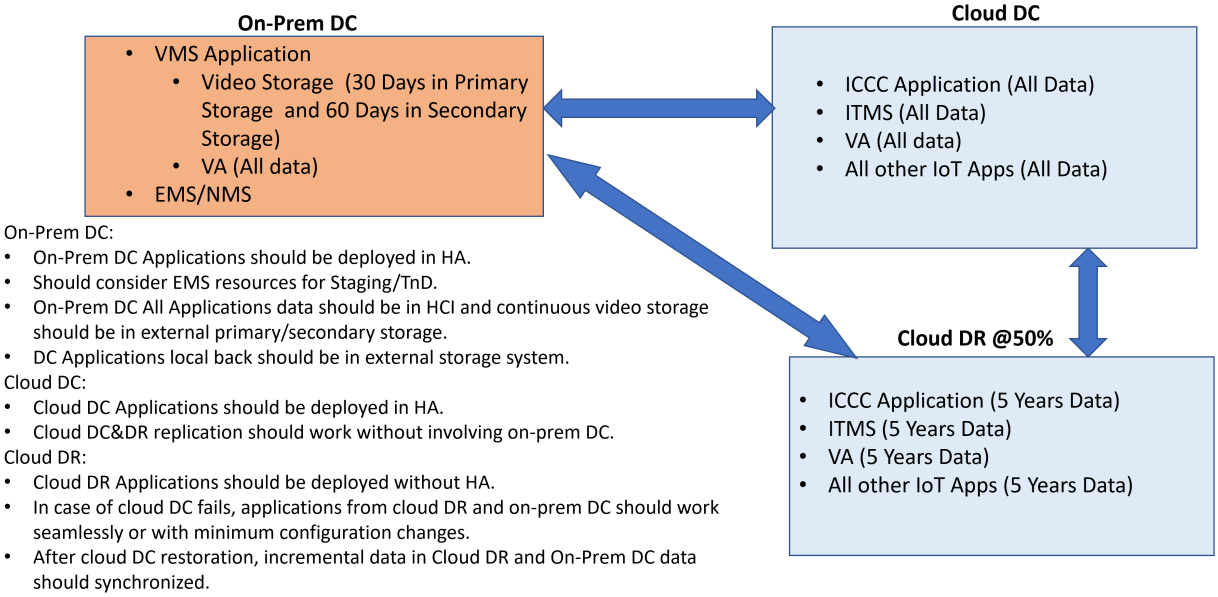
a) As-built drawings
b) Training manuals and schedules.
c) Operation and maintenance manuals.
d) Spares list (recommended spares, commissioning spares and operation spares)

5.3 Finalization of Detailed Technical Architecture

Puducherry Architecture (On-Prem DC, Cloud DC&DR)



Applications Architecture

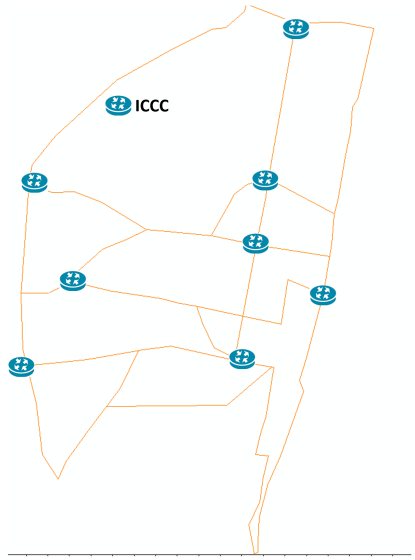


On-Prem DC:
- On-Prem DC Applications should be deployed in HA.
- Should consider EMS resources for Staging/TnD.
- On-Prem DC All Applications data should be in HCI and continuous video storage should be in external primary/secondary storage.
- DC Applications local back should be in external storage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

Cloud DC:
- Cloud DC Applications should be deployed in HA.
- Cloud DC&DR replication should work without involving on-prem DC.

Cloud DR:
- Cloud DR Applications should be deployed without HA.
- In case of cloud DC fails, applications from cloud DR and on-prem DC should work seamlessly or with minimum configuration changes.
- After cloud 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 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.

d) **Manageability -** Ease of configuration, ongoing health monitoring, and failure detection are vital to the goals of scalability, availability, and security and must be able to match the growth of the environment. Network should be auto/manual configurable for various future requirements for the ease of maintenance / debugging.

e) **Interoperability -** The system should have capability to take feed from cameras installed by private / Govt. at public places, digitize (if required) & compress (if required) this feed & store as per requirements.

f) **Open Standards -** Systems should use open standards and protocols to the extent possible

g) **Single Sign On**- The application should enable single-sign-on so that any user once authenticated and authorized by system is not required to be re-authorized for completing any of the services in the same session. For employees of the department concerned, the browser-based application accessed on the intranet, through single-sign-on mechanism, will provide access to all the services of the departments concerned (based on their roles and responsibilities), Help module, basic and advanced reporting etc. Similarly, for external users (citizens, etc), based on their profile and registration, the system shall enable single-sign on facility to apply for various services, make payments, submit queries /complaints and check.

h) **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.

i) **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:

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 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.
3. SI shall design and develop the Smart City System as per the Functional and System requirement 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 & Water Pipelines, OFC Network of other Operators, Trees, existing installations, etc. The Authorities shall be fully informed of the results of the survey and the amount and extent of the demolition and site clearance shall then be agreed with the 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. willbe dismantled and replaced with the new systems which are 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 challan of 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 of the required power, etc. SI shall provide & manage all necessary paper work to 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 as cameras and other field equipment. All mounting devices for installation of CCTV cameras suchas 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, stainlesssteel bands, screws and other accessories.

c) All the equipment, software and workmanship that form a part of the service are 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 proofand in case the equipment's get damaged /stolen for reasons whatsoever, it shall repair/replace the same in the specified time as per SLAs at no extra cost to the Authority. All such costs shall be factored in the comprehensive insurance of fieldequipment 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 its designated agency.

g) In addition to above, the SI shall be fully responsible for all maintenance activities for theperiod 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 without any 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 commercials or 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 other location 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 be provided 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 required field 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 damage and 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 safety norms.

5.8.21. Appropriate branding or color coding (Police/Authority Branding) of poles and junction boxes, 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 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.

5.8.23. For more details on technical and functional specifications of Surveillance Cameras, SI should 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 the following, 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 the following, 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 the following, but is not limited to:

a) The SI shall install the ANPR Cameras at every entry & exit points of the city on major 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 the RFPs, 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, 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 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 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.
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, all wiring connections to the traffic signal controllers and to the camera platforms shall be installed by the SI. The SI shall supply all 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 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 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.
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 RLVD Cameras, SI should 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 and event 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 platforms shall be installed by the SI. The SI shall supply all 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

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 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.

5.10 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 from the frame of the component ring and will be connected via several earth electrodes. The cable arm will be earthen through the cable glands. The entire applicable IT infrastructure i.e. field locations/traffic junctions or command centre shall have adequate earthing. Further, earthing should be done as per Local state national 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 rust proof. 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 to earth 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 not be 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 to be 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 field sensors like the cameras, traffic sensors, traffic light aspects, active network components, controller and UPS at all field locations, as per the specifications given in the RFP.

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

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. Boxes shall 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 mind the 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 air circulation filters that shall not require maintenance and shall allow free circulation of air inside the enclosures to prevent overheating as well as the build-up and effects of humidity and heat, without permitting the entry of elements that might endanger system operation.

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 for installation by the SI. However, SI will be responsible for obtaining all the necessary permissions etc. The details of traffic junctions/locations are provided in 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 the cameras and ensure that the pole / mast implementation is vibration resistant. Arrangements for bird scare spikes on top of camera shall be made to prevent birds from sitting on top of camera box.

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 that there 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 equipment could 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 be designed keeping in mind the normal flow of vehicular traffic and pedestrian movement 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 during implementation 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 at each 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 housing in corrosion resistant cabinets.

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

vi. SI shall provide UPS for efficient heat dissipation without air conditioning. It shall be 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 all the field components of the system including:

a) Preparation of concrete foundation for MS-Poles & cantilevers
b) Laying of GI Pipes (B Class) complete with GI fitting

c) Hard soil deep digging and backfilling after cabling
d) Soft soil deep digging and backfilling after cabling
e) Chambers with metal cover at every junction box, pole and at road crossings
f) Concrete foundation from the Ground for outdoor racks

ii. SI shall provide electricity to the cameras through the aggregation point. Since this component has dependency on approval from local authorities, it is recommended that SI plans this requirement well in advance & submits the application 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 components of 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, with minimum 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 name of Authority.

viii. SI shall house the electricity meters inside the power cabinet as mentioned in the 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 basis to 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 Specificationdocument
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 InstallationReport
17	Physical Infrastructure setup	Training Completion report
18	Procurement of all IT & Non-IT equipment's	Application deployment andconfiguration 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 (ifany)	
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 CitySolutions	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-ITinfrastructure 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 andException 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(Implemen-tation 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 in phase 1 thereof up to the maximum value of 10% on the amount to be released in phase 1. 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.
ProgressReports	Monthly Progress Reports during the implementation on period and during the O&M period	By 5th of each succeedingmonth	After 5th of succeeding month, a penalty of Rs. 1 lakh per day with a capping of 15 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 warranty from OEMand 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 below sections. 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. All specified parameters mentioned in the scope/technical requirement in the RFP may be considered for meeting current & future requirements during the contract period. The SI is fully responsible for the specified outcome to be achieved 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 clearly mentioning 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 support and services.
x. Product serial numbers of all IT active components should be available in the OEM online 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:
xiii. Both Bidder and OEM should submit following certificate along with the bid document:

1. 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.
2. 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 requisite alerts and standard operating procedures (SOPs) in terms of responding to incidents. The platform should support and be open for community development requirement and will be extended 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 monitoring of 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 objective of this DPR 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. 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. 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. 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 360° situational awareness for operations	1. It should enable effective management of City Operations through a Integrated Command and Control Center Application System. 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 management Application system so that City Workforce across all departments can be integrated and equipped with Mobile App to efficiently run their day to day activities. 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. 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.

The ICCC OEM should be in existence in India since last 5 years. The OEM should have at least the following certificates: ISO 9001, 27001, and CMM I Level 3.

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 a.	
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 System	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		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 Normalisation 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	API Management System	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		The platform should enable contextual information and correlation across domains and verticals (Multiple vendor and Multi-sensor in future	
31		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	Manage and Scale API Traffic	API Management System should support API composition, protocol and data transformation	
42		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 possessintegrated 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	Control Access and Enforce Security	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		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 & automated decisions	
100		Should provide an environment for designing, developing, and deploying 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 systems based 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	IoT Security	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		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		Standard Authentication	
164		Custom Authentication	
165		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 Manageme nt	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	Configurati on 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	Centralized Logging & Monitoring Platform	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		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 per second, 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	Provisioning & Service Management	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		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			
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 provide parameters based on the selected Algorithm	
228		Geo ML: Users can select ML Algorithms especially built for Geospatial 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		Smart parking system	
244		Intelligent Traffic Management System - Adaptive Traffic Control System (ATCS), Red Light Violation Detection (RLVD) and	

		Automatic number-plate recognition(ANPR), Automatic Traffic Counter and Classifier (ATCC) & Speed Violation Detection (SVD)	
245		City Surveillance system - CCTV/PTZ camera with video analytics capabilities	
246		Environment management system - Environmental sensors	
247		Variable Message Board (VMD),	
248		E governance - Citizen Engagement System - Citizen Services application – Open Data Collaboration Platform	
249		Storm Water level Monitoring system	
250		Smart Street Lighting system - Smart Street light controllers (CCMS)	
251		GIS platform integrated with Command-and-Control Center	
252		Smart Poles with Emergency Call Box, Public Announcement system, Smart Street lighting, digital billboard, public Wi Fi, etc.	
253		Information Kiosk	
254		OFC network.	
255		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 all the alarms and provides an easy-to-use GUI interface (web & client server)	
258		help manage: alarms, map-based visualization of the city assets and events, execute SOPs and coordinate the operations;	
259		provide 360-degree situational awareness and insights across urban 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		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		provide the details about each alarm received from the various sub-systems integrated.	
265		provide the operator details regarding the source of the alarm, type of alarm, generated time, priority, and elapsed time to take appropriate action.	
266		provide advanced map & video visualization for situation awareness.	
267		provide an easy use GUI that is simple to operate.	
268		operator to view various types of alerts in a single place and validate 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 Visualization	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.	
277		Selection of cameras can be based on the following:	
		Map based selection	
		Jurisdiction/ camera selection from the camera list alert the details 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 in at least 3 smart cities in India /Global. All these implementations should be successfully operational for least 3 years with Integration to minimum 10 different sub systems /applications. Document Proof: OEM Shall submit P.O and Completion Certificate/ Installation Notes/UAT Certificates from SI as documentary proof. ICCC Platform OEM should have ISO 9001:2015 & ISO 27001:2013.	

Key Integration Requirement

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.

S.No	Parameter	Minimum Description
		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

S.No	Parameter	Minimum Description
		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 and 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. Advisory no 22 of cyber security framework guidelines recommended by MoHUA shall be considered.
8	Future Applications	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: Finalization of Detailed Technical Architecture.

(a) Storage of all outdoor camera feeds at on premise Data Centre primary storage for first 30 days.
(b) Storage of all outdoor cameras feeds on secondary storage for further 60 days .
(c) Historical and Other Data like VA Alerts and Violations data should be Stored upto 5 years at on-prem and cloud.
(d) Data gathered from all sensors to be stored in Cloud from 1st day till 5 years.

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. 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.	
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: a. 1M IPv4 FIB routes and 64K IPv6 FIB routes. b. 32 VRF/L3VPN and 200 L2VPN. c. HQoS and minimum 2K Queues. d. 1K number of MPLS Labels (Provider Router). e. 6PE /6VPE, MPLS label-Switching router (LSR & LER) functionality. f. 4K VLANs.	
11	Shall support following class of service features: a) Classification, policing, marking, shaping, filtering b) Manage congestion using a weighted random early detection (WRED) algorithm c) Ingress policing d) egress shaping e) strict queuing , WFQ 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 a) 802.3ah/802.1ag/TWAMP b) LLDP	
13	IPv6 Features a) IPv6 Ping b) IPv6 trace route c) OSPF v3 d) IS-IS	

14	Multicast Feature: It shall support following: a) It shall support IGMP snooping v2/v3 b) The router shall support PIM Sparse Mode, RFC 4601 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. 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 50 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 2nd Gen processors	
		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 the make**	
2.		**Model : The solution will be provided by the SI along with the model**	
3.	Solution/ Type	1) IP Based/iSCSI/FC/NFS/CIFS 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 5 configuration). Storage Capacity after RAID to be provided with 20% additional capacity for future useto be provided. 2) RAID solution offered must protect against double disc failure. 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) 4) To store all types of data (Data, Voice, Images, Video, etc) 5) Proposed Storage System should be scalable (vertically/horizontally)	
5.	Hardware Platform	1) Rack mounted form-factor 2) Modular design to support controllers and disk drives expansion	
6.	Controllers	1) At least 2 Controllers in active/active mode 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): i) Priority Queue, ii) Ingress policer, 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): i) Priority Queue, ii) Ingress policer, 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	
41	Core Switch and TOR switch should be from same OEM. Hardware /Software should have 5-year warranty	

6.2.9. Access Switch -8 Port – POE

S.No	Specification	Compliance (Yes / No)
	Make :	
	Model :	
1	Should have minimum 8 GE ports. Should have dual power supply with hot swappable.	
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 Operating Temperature range 0°C to 50 °C	
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

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 Operating Temperature range 0°C to 50 °C	
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, rackmountable with 2 x 10G (or better) Ethernet interface.	
4	The proposed WLC should support both centralized as well as distributed traffic forward- ing 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 chang- ing environmental conditions and signal coverage adjustments. It should also adjust ra- dio channel automatically.	
10	Should support dynamic bandwidth selection among 20Mhz, 40 MHz, and 80Mhz chan- nels.	
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. 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 repairing noncompliant machines in a quarantine area 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 endpoint is 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-Anti Virus 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 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) 2x Input (HDMI2.0) 2x LAN 2x USB 1x Output (DP1.2)	
21	Power Supply	100 – 240 VAC, 50-60Hz; Power supply: Remote 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 be provided	
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 be of 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 Power supply	
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 at any time with a simple mouse click or schedule/timer based.	
19	Software	The software should be able display multip sources anywhere on video wall in any siz Key features of Video Wall manageme Software •Central configuration database •Browser based user interface •Auto-detection of network sources •Online configuration of sources, displays and system variables	
20	Software	Video Wall Control Software shall allow commands on wall level or cube level or a selection of cubes: • Switching the entire display wall on or	

No	Parameters	Minimum Technical Requirements	Compliance (Yes /No)
	Make:		
	Model:		
		off. • 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. • 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. 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 time Can 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. 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: 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 the SI. The SI would need to undertake the provisioning of LAN cabling between end user till 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 to best 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" style wraps to provide proper support and management of cables. No plastic tie wraps may be 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 all the floors and wiring closets.
- The distance between any I/O point and the corresponding switch should not be more than 90 meters. The place for installing the racks & network equipment will be the responsibility 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 Network Equipment's.
- Dedicated raceways / cable-trays should be used for laying LAN.
- Additional cabling requirements on an on-going basis shall also need to be catered to.
- 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 and closing 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 incident resolution time for priority / non- priority incidents.
- Helpdesk should be an ITIL certified tool from certified Authority like Pink Verify for Incident, 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 Monitoring Systems so that the Help Desk Operators can to associate alarms with Service Desk tickets

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 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: • 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 . • Should have ISO 11064, ISO 14001 (environment), OHSAS 18001, HFE and ISO 9241 or similar certifications • 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 • 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. • Safety of User & ICCC: Safety is a high concern area therefore panelling and Plank ceiling must be standard one to withstand vibrations. • 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. • 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. • Sound transmission class (STC) value should be as per site conditions. • 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: a. 64K IPv4 FIB routes and 16K IPv6 FIB routes. b. 32 VRF/L3VPN and 200 L2VPN. c. HQoS and minimum 2K Queues. d. 1K number of MPLS Labels (Provider Router). e. 6PE /6VPE, MPLS label-Switching router (LSR & LER) functionality. f. 4K VLANs.	
11	Shall support following class of service features: a) Classification, policing, marking, shaping, filtering b) Manage congestion using a weighted random early detection (WRED) algorithm c) Ingress policing d) egress shaping e) strict queuing , WFQ 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 a) 802.3ah/802.1ag/TWAMP b) LLDP	
13	IPv6 Features a) IPv6 Ping b) IPv6 trace route c) OSPF v3 d) IS-IS	
14	Multicast Feature: It shall support following: a) It shall support IGMP snooping v2/v3 b) The router shall support PIM Sparse Mode, RFC 4601 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. 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: a. 32K IPv4 FIB routes and 8K IPv6 FIB routes. b. 32 VRF/L3VPN and 200 L2VPN. c. HQoS and minimum 2K Queues. d. 1K number of MPLS Labels (Provider Router). e. 6PE /6VPE, MPLS label-Switching router (LSR & LER) functionality. f. 4K VLANs.	
11	Shall support following class of service features: a) Classification, policing, marking, shaping, filtering b) Manage congestion using a weighted random early detection (WRED) algorithm c) Ingress policing d) egress shaping e) strict queuing , WFQ 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 a) 802.3ah/802.1ag/TWAMP b) LLDP	
13	IPv6 Features a) IPv6 Ping b) IPv6 trace route c) OSPF v3 d) IS-IS	
14	Multicast Feature: It shall support following: a) It shall support IGMP snooping v2/v3 b) The router shall support PIM Sparse Mode, RFC 4601 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. Warranty –Hardware/ Software License should be for 5 years.	

Civil and Architectural Work

Sl. No	Minimum Specifications	Compliance (Yes / No)
	a. Designer Acoustic Metal False ceiling with Plank 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. c. The proposed ceiling tiles shall be as per industrial grade standards . 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. e. The Ceiling system must ensure restriction of hazardous substance in any of the materials. f. The Non uniform gaps between the designer Metal ceiling / Grid type Snap Fit Ceiling shall be covered with Calcium Silicate Ceiling. 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. 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. 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	

Sl. No	Minimum Specifications	Compliance (Yes / No)
	structure shall allow easy assembly of Hinged Shutters, Slat wall, Gland Plate, Monitor arms in extremely rigid manner. j. **Table-top:** - The material of the working surface should be of industrial grade. 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. l. Slat Wall shall be made of industrial grade material . 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 . n. **Shutters & Side Legs:** - Front, back shutters shall be industrial grade material . Side leg shall be of the same finish. 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. 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. 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. r. Sound transmission class (STC) value as per site conditions. s. Standard design feature of Load bearing capacity of panelling - panelling structure shall have sufficient load carrying capacity . 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. u. Industrial grade feature of Modular wall panelling tile having secure locking arrangement for equidistant mounting. 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. x. The Panel should be as per industrial grade. 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. • Shall have end circuit to detect open circuit fault.

Raised Floor

Sl. No	Minimum Specification	Compliance (Yes / No)
1	System: • Access floor system to be installed at finished floor height as per site conditions. • 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. 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. • 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. • Conduit runs shall be so arranged that the cables connected to separate main circuits shall be enclosed in separate conduits, and that all lead and return wire of each circuit shall be run to the same circuit. • All conduits shall be smooth in bore, true in size and all ends where conduits are cut shall be carefully made true and all sharp edges trimmed. All joints between lengths of conduit or between conduit and fittings boxes shall be pushed firmly together and glued properly. • Cables shall not be drawn into conduits until the conduit system is erected, firmly fixed and cleaned out. Not more than two right angle bends or the equivalent shall be permitted between draw and junction boxes • Conduit concealed in the ceiling slab shall run parallel to walls and beams and conduit concealed in the walls shall run vertical or horizontal. • The chase in the wall required in the recessed conduit system shall be neatly made and shall be of angle dimensions to permit the conduit to be fixed in the manner desired.	

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. • 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. • Where, single phase circuits are supplied from a three phase and a neutral distribution board, no conduit shall contain wiring fed from more than one phase in any one room in the premises, where all or part of the electrical load consists of lights, fans and/or other single phase current consuming devices, all shall be connected to the same phase of the supply. • Circuits fed from distinct sources of supply or from different distribution boards or M.C.B.s shall not be bunched in one conduit. In large areas and other situations where the load is divided between two or three phases, no two single-phase switches connected to difference phase shall be mounted within two meters of each other. • All splicing shall be done by means of terminal blocks or connectors and no twisting connection between conductors shall be allowed. • Metal clad sockets shall be of die cast non-corroding zinc alloy and deeply recessed contact tubes. Visible scraping type earth terminal shall be provided. Socket shall have push on protective cap. • All power sockets shall be piano type with 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. • 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. • 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. • All metallic objects on the premises that are likely to be energized by electric currents should be effectively grounded. • The connection to the earth or the electrode system should have sufficient low resistance in the range of 0 to 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. • Recommended levels for equipment grounding conductors with very low impedance level. • There should be enough space between data and power cabling and there should not be any cross wiring of the two, in order to avoid any interference, or corruption of data. • The earth connections shall be properly made. A small copper loop to bridge the top cover of the transformer and the tank shall be provided to avoid earth fault current passing through fastened bolts, when there is a lighting surge, high voltage surge or failure of bushings. • A complete copper mesh earthing grid needs to be installed for the server farm area, every rack need to be connected to this earthing grid. A separate earthing pit need to be in place for this copper mesh. • Provide separate Earthing pits for Servers, UPS & Generators as per the standards.	

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. • 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. • Each section of the rising mains shall be provided with suitable wall straps so that same can be mounted on the wall. • Whenever the rising mains pass through the floor they shall be provided with a built-in fire proof barrier so that this barrier restricts the spread of fire through the rising mains from one section to the other adjacent section. • Neoprene rubber gaskets shall be provided between the covers and channel to satisfy the operating conditions imposed by temperature weathering, durability etc. • Necessary 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. • 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 • Compressor – As per site condition • Refrigerant – As per site condition • Power Supply – Three Phase, 380-415 V, 50 Hz • Air Flow Rate – minimum 19 cu m / min • Noise Level - < 50 dB • Operation – Remote Control	

Fire Alarm System

Sl. No	Minimum Specification	Compliance (Yes / No)
1	• **System Description** ➢ The Fire alarm system should be installed as per latest NFPA 72 guidelines. ➢ 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. • **Smoke detectors** – Smoke detectors shall be of the optical or ionization type. ➢ Heat detectors ➢ Heat detectors shall be of the fixed temperature (58° C) or rate of temperature rise type with a fixed temperature operating point. ➢ Detector bases shall fit onto an industry standard conduit box. • **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: • Controlled Entries to defined access points. • Controlled exits from defined access points. • Controlled entries and exits for visitors.	

	• Configurable system for user defined access policy for each access point. • Record, report and archive each and every activity (permission granted and / or rejected) for each access point. • User defined reporting and log formats. • Fail safe operation in case of no-power condition and abnormal condition such as fire, theft, intrusion, loss of access control, etc. • Day, Date, Time and duration based access rights should be user configurable for each access point and for each user. • One user can have different policy / access rights for different access points 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. • The ceiling speakers shall have wide, controlled constant directivity dispersions for optimum coverage. • The ceiling speakers shall have in-built amplifiers or shall be supported by an external amplifier. • The ceiling speakers shall have a conical coverage pattern. • The ceiling speakers shall be in a colour to match the ceiling and surrounding interior design. • Full audio coverage within the command centre room and video room should be made. • The Ceiling Speakers shall automatically adjust the output audio level based on ambient noise. • 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: 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 Engine shall be complete with following accessories • In-line fuel pump with mechanical governor • Optimised turbocharger • Stainless steel exhaust flexible coupling • Silencer • Radiator • Coolant inhibitor • Plate-type lube oil cooler • Dry-type, heavy duty, replaceable paper element air cleaner with restriction indicator • Flywheel housing and flywheel to suit single bearing alternator • Electrical starter motor • Battery charging alternator • First fill lube oil	
2	ALTERNATOR SPECIFICATIONS: 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. • Self-excited, self-regulated • Class 'H' insulation • Salient pole revolving field • Single bearing • Digital automatic voltage regulator (part of PCC 1301)	
3	BASE FRAME: Sturdy, fabricated, welded construction, channel iron base frame for mounting above Engine & Alternator.	
4	FUEL TANK: 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: Set of 2 nos., 12V, Dry Lead acid automotive batteries.	
6	MANUAL CONTROL PANEL: 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: • 1250A, 4 Pole Contactor for ALTERNATOR with Thermal O/L relay • BACK-UP PROTECTION: • HRC fuse for short circuit protection.	
8	MICROPROCESSOR BASED AMF MODULE INCORPORATING: Functions:	

	• Supply Failure Timer • Restoration Timer • Impulse automatic engine start / stop logic • Mains / Generator Voltage & Frequency sensing Controller with the following features: Water Temperature/ Lube Oil Pressure / engine speed Voltage / Ampere / Frequency / kVA o Running-hour counter No. of starts • Fault Indication (LED Type) Over /Under Speed Fails to Start Low Oil pressure High Engine Temperature Under / over voltage Over current • Combined Meter for kW / Power Factor / KVA • Electronic kWH Meter (Counter Display) • Current Transformers	
9	Relay: • Earth Fault Relay (Electronic type) • Reverse Power Relay	
10	Indications (LED): • DG ON, Load on DG • Mains ON, Load on Mains, Battery Charger ON	
11	Push Buttons (AMF MODULE BY PASS MODE): • Generator Contactor CLOSE / TRIP • Mains Contactor CLOSE / TRIP (If Provided) • Fault ACCEPT / RESET	
12	BATTERY CHARGER: • SMPS Based Unit with inbuilt Auto / Manual & Float /Boost Facility • DC Voltmeter & Ammeter (Separate) • 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	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 nos for 3Ph Unitary UPS & min. 10000 nos for Modular UPS (for ICCC/DC)	
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: 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 is proposed 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,

a) Should be at least 500 KM from Primary Data Centre and
b) Should not be in same River Flood plain and

The proposed data center must be 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 and these SLAs should be declared in public portal of CSP.
d) The CSP should provide marketplace with certified applications which can be deployed on cloud. The CSP should also provide capability for administrators to create private marketplace with images from the public marketplace.
e) The CSP should provide all variants of cloud service as per MeiTY guidelines.
   - Infrastructure as a Service (IaaS),
   - Platform as a Service (PaaS)
   - Software as a Service (SaaS)

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 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.	
6	Certified marketplace for purchase of third party solutions.	
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 selectable from a marketplace hosted by the CSP without intervention from CSP.	
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	Native CSP provided Media services and CDN for media streaming and large file transfer between department/organization and CSP	
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: • Layer 3 and Layer 4 Firewall • Layer 7 Firewall (WAF) • SIEM & SOAR (CSP / CSP marketplace) • Vulnerability Scanner • Endpoint Security (Attack Surface Management) • Backup Tools • Disaster Recovery Tools	
14	The CSP should have minimum following experiences. • Providing the Public Cloud Services (PaaS, SaaS) in India	

15	CSP should support both BYOL (Bring your own license) BYOL is eligible to run everywhere, and with a Pay as you go option. The OS offered should come with continuous updates and upgrades anytime.	
16	Monitoring services for cloud resources hosted in the data centre and support for customized report generation.	
17	The CSP should support per hour, per month and options for long term (such as 1 yr. & 3 yr.) reservation of compute VMs and DB as a service for MYSQL, PostGreSQL and Microsoft SQL servers.	
18	The CSP should provide options for dynamic pricing as well as fix unit pricing of all the resources proposed	
19	CSP should have accreditations relevant to security, availability, confidentiality, processing integrity, and/or privacy Trust Services principles such as SOC 1, SOC 2, SOC 3.	
20	Data Centers should be compliant to MeitY recommended security guidelines.	
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	
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 – • Optimized for generic applications and provides a balance of compute, memory, and network resources. • Optimized for memory intensive applications. • Optimized for compute intensive applications. • 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 • Cloud provider should offer persistent block level storage volumes for use with compute instances. • Cloud provider should offer higher block storage volumes as required • Cloud service should support solid state drive (SSD) backed storage media that offer millisecond latencies. • 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. • Cloud service should support encryption of data on volumes, disk I/O, and snapshots using industry standard AES-256 cryptographic algorithm. • Cloud service should support encryption using customer managed keys. • Cloud service should support point-in-time snapshots. These snapshots should be incremental in nature. • 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. • 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. • Cloud service should support a baseline IOPS/GB and maintain it consistently at scale • 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 publicly disclosed.	

90	Object Storage • Cloud provider should offer secure, durable, highly scalable object storage for storing and retrieving any amount of data from the web. • Cloud provider should support an extremely low-cost storage for archival. The CSP should automatically tier the data. • Cloud service should support encryption for data at rest using 256-bit Advanced Encryption Standard (AES-256) encryption to encrypt your data. • 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. • Cloud service should support encryption using a Key • 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. • 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. • Cloud service should be able to send notifications when certain events happen at the object level (addition/deletion). • 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). • Cloud Service should support versioning, where multiple versions of an object can be kept in one location. Versioning protects against unintended overwrites and deletions. • Cloud service should support flexible access-control policies to manage permissions for objects. • 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. • 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. • Cloud service should support a lower cost option for noncritical, reproducible data at lower levels of redundancy. • 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. • Cloud service should support read-after-write consistency for PUT operations for new objects. • 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. • Cloud provider should support moving large amounts of data into the cloud by bypassing the internet. • Cloud provider should support replicating data to DR site and should provide read-only access to the replicated data.	
91	File Storage • Cloud provider should offer a simple scalable file storage service to use with compute instances in the cloud. • Cloud service should offer SSD backed storage media to provide the throughput, IOPS, and low latency needed for a broad range of workloads. • Cloud service should support petabyte-scale file systems and allow thousands of concurrent NFS connections. • Cloud service should support consistent low latency performance and should support scalable IOPS and throughput performance. • Cloud service should support thousands of instances so that many users can access and share a common data source. • Cloud service should automatically scale up or down as files are added or removed without disrupting applications. • Cloud service should be highly durable - file system object (i.e. directory, file, and link) should be redundantly stored across multiple data centers. • 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 as per 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 in real-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 camera view 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 the license 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 are stolen 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. The system should allow the user to import the vehicle license plate data in the hot lists stored in 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 such case. The system should also have the functionality to send the alert via email and SMS to designated 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 stop line (irrespective whether the signal is GREEN or RED) in form of Video popup at the Monitor and/or SMS on Cell phones.

l) The system should have the functionality to trace the movement of a vehicle of interest on GIS 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 for easy inspection of the license plate number. The system should keep audit trail of any license 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 feed from the traffic signal controller or by video analytics by recording the evidence snap showing 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 mark and encryption as per the techno-legal requirements.

V. The system should synchronize the evidence camera, license plate recognition camera and store the record in database with License plate image, image of the vehicle, and at least five snaps showing clearly that the vehicle is crossing the red light / stop line while the signal is RED. This event should be corroborated with the video clip archived in the VMS system 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 using the 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 time for the signal light status change.

6.4.6 Speed Violation Detection (SVD)

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

i. 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 should be able to differentiate between a helmet and various other conditions such as the bald head, 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 name etc.

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 switching has taken place. The report shall show the cycle sequence and cycle timings for the cycle in a day.
- Mode switching report – The report shall give details of the mode switching taken place on a day.
- Event Report - The report shall show events generated by the controller with date and time of event.

- 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 mode is 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 intersections in a corridor for every cycle executed for the corridor and the average corridor saturation for a day

- Corridor Cycle Time Report – The report shall show the Corridor cycle time, Intersection cycle time, Mode of operation and degree of saturation of all the intersections in a corridor for every cycle for a day

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 coding on site map whether an intersection under the ATCS is online or off. On double clicking the intersection a link shall be activated for the traffic flow display for the intersection.
- Traffic Flow Display – This online display shall indicate the current traffic flow with animated arrows, mode of operation, stage number being executed and elapsed stage time.
- Saturation Snapshot – This display shall show the current saturation levels of all intersections in a corridor.
- Reports Printing/ Viewing – This link shall allow selection, viewing and printing of different reports available under ATCS
- Time-Space Diagram – The time-space diagram shall display the current stages being executed at every intersection in a corridor with immediate previous history.
- Junctions shall be plotted proportional to their distance on Y-axis and time elapsed for the stage in seconds on X-axis.
- Junction names shall be identified with each plot.
- 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: