Model RFP 2.0

Selection of Master System Integrator (MSI)

For Implementation of

Integrated Command and Control Center

(ICCC)/ ICT Projects

in {CITY_NAME}

Section-1 Volume II: Scope of Work

Core Infrastructure

RFP Ref/Tender No.:

Date:

RFP/Tender invited by: [SPV_Full_NAME]

Disclaimer

[The Authority may customize as per city's requirement]

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

This RFP is neither an agreement nor an offer or invitation to any party. The purpose of this document is to provide the Bidders or any other person with information to assist the formulation of their Techno-commercial offers ("**Bid**"). This RFP includes statements, which reflect various assumptions and assessments which may be arrived at by Authority in relation to the project scope. This RFP does not purport to contain all the information which each Bidder may require. This RFP may not be appropriate for all persons, and it is not possible for the Chief Executive Officer, Authority 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. Hence, each Bidder must therefore conduct their own independent analysis of the information contained in the RFP and to seek its own professional advice from appropriate sources.

Information provided in this RFP to the Bidder is on a wide range of matters, some of which may depend upon the interpretation of the 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. Authority accepts no responsibility for the accuracy or otherwise for any interpretation of opinion on law expressed herein.

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

This RFP does not imply that Authority is bound to select a Bidder or to appoint the Selected Bidder (as defined hereinafter), for Implementation and Authority reserves the right to reject all or any of the Bidders or Bids without assigning any reason thereof.

Table of Contents

Glossary

Terms	Meaning
ANPR	Automatic Number Plate Recognition
AP	Access Point
ATCS	Adaptive Traffic Control System
AVLS	Automated Vehicle Locator System
BOM	Bill of Material
BQS	Bus Queue Shelters
CCHS	Central Clearing House solution
CCTV	Closed Circuit Television
CCC	Command and Control Center
CONOPS	Concept of Operations
COP	Common Operating Platform
CSP	Cloud Service Provider
DBA	Database Administrator
DC	Data Center
DNS	Domain Name Server
DR	Disaster Recovery
DRC	Disaster Recovery Center
EMD	Earnest Money Deposit
EMS	Enterprise Management System
ETA	Estimated Time of Arrival
ETD	Estimated Time of Departure
ETM	Electronic Ticketing Machine
E-Procurement Portal	Means electronic tendering system of Authority
FMS	Facility Management Services
FRS	Functional Requirement Specifications
GIS	Geographical Information Systems
GPRS	General Packet Radio Service
GPS	Global Positioning System

GSM	Global System for Mobile Communication
GUI	Graphical User Interface
HDPE	High-Density Polyethylene
HO	Head Office
IaaS	Infrastructure as a Service
ICCC	Integrated Command and Control Center
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IMS	Infrastructure Management System
IOE	Internet of Everything
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITMS	Intelligent Traffic Management System
LAN	Local Area Network
LOI	Letter of Intent
LOA	Letter of Award
KPI	Key Performance Indicator
MCC	Mobile Command Center
MeitY	Ministry of Electronics & Information Technology
MLCP	Multi-Level Car Parking
MoHUA	Ministry of Housing & Urban Affairs
MoU	Memorandum of Understanding
MPLS	Multi-Protocol Label Switching
MSI	Master System Integrator
MTBF	Mean Time Between Failure
MTTR	Mean Time to Repair
NFC	Near Field Communication
NIC	National Informatics Centre

ONVIF	Open Network Video Interface Forum
O&M	Operation and Maintenance
OEM	Original Equipment Manufacturer
OFC	Optical Fiber Cable
OGC	Open Geospatial Consortium
OS	Operating System
OTP	One Time Password
OWASP	Open Web Application Security Project
PA System	Public Address System
PaaS	Platform as a Service
PDU	Power Distribution Unit
PIS	Public Information System
PKI	Public Key Infrastructure
PMC	Project Management Consultant
PoE	Power over Ethernet
PoP	Point of Presence
PTZ	Pan Tilt Zoom
QR Code	Quick Response Code
RF	Radio Frequency
RFID	Radio Frequency Identification
RFP	Request for Proposal
RLVD	Red Light Violation Detection
RoW	Right of Way
RTO	Recovery Time Objective
RPO	Recovery Point Objective
SaaS	Software as a Service
SCADA	Supervisory control and data acquisition
SCM	Smart Cities Mission
SLA	Service Level Agreement
SMPS	Switched Mode Power Supply
SMS	Short Message Service

SNMP	Simple Network Management Protocol
SOP	Standard Operating Procedure
SOS	Save Our Souls. SOS is International Morse code distress signal
SRS	System Requirement Study
TPA	Third Party Auditor
TRAI	Telecom Regulatory Authority of India
TRS	Technical Requirement Specifications
TSP	Telecom Service Provider
UAT	User Acceptance Testing
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
VA	Video Analytics
VM	Virtual Machine
VMD	Variable Message Display
VCA	Video Content Analysis
VLAN	Virtual Local Area Network
VM	Virtual Machine
VMS	Video Management Software/System
WAN	Wide Area Network
{MUNICIPAL_SHORT_NAME}	{MUNICIPAL_FULL_NAME}
{SPV_FULL_NAME}	Authority
{SPV_SHORT_NAME}	Authority
{CITY_NAME}	City Name

Section-1 Core Infrastructure

1. Introduction

1.1 Introduction to {CITY_NAME} Smart City Project

[<< Authority to provide details of the Project here >>]

1.2 City Objectives

[Authority to refer Guidance document available at …… while developing various section of the RFP]

The Authority has envisaged implementation of an Integrated Command & Control Center (ICCC) and Digital infrastructure in the city.

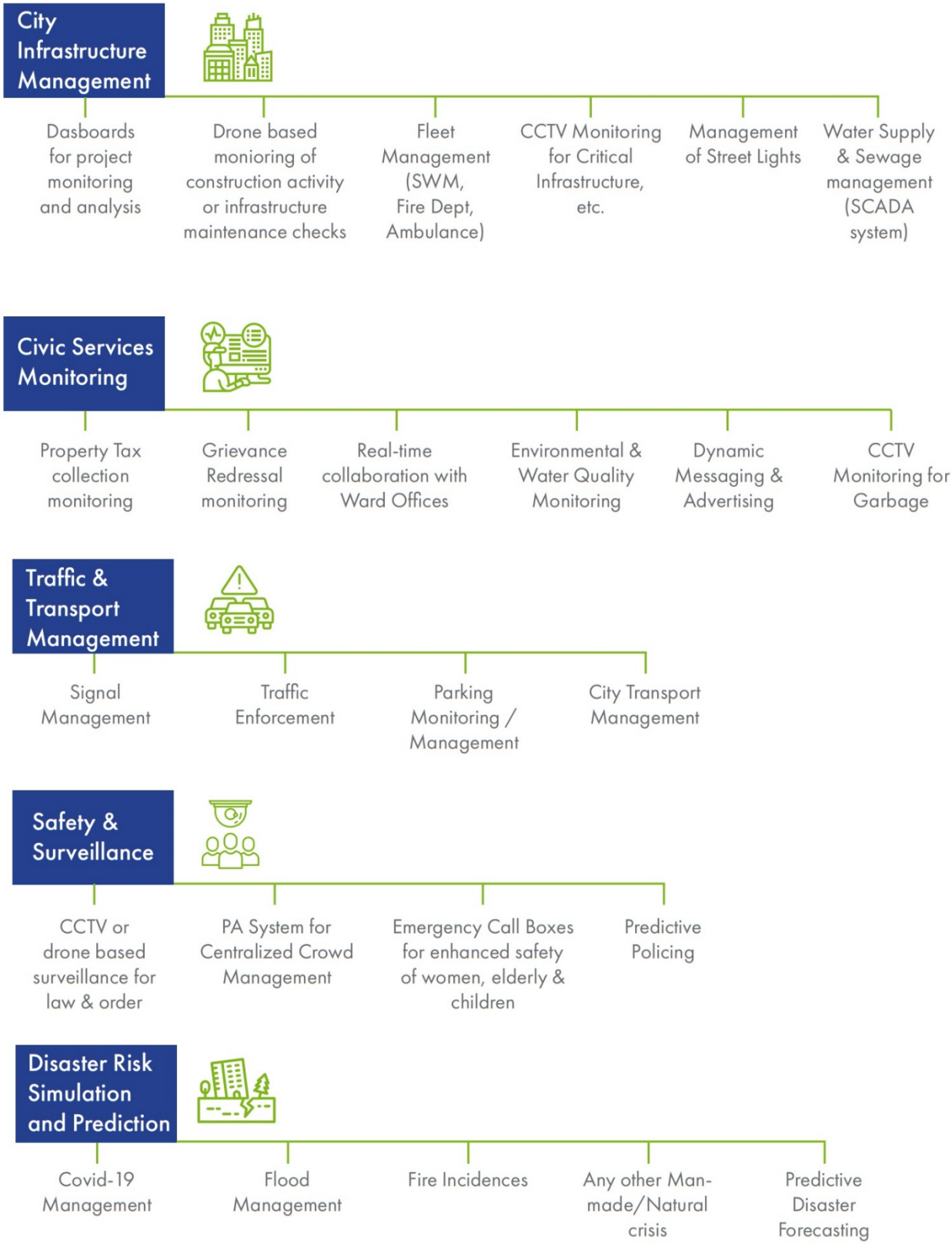
Through this initiative, the Authority plans to utilize information technology to build a well-informed, connected, smart and intelligent system of systems to help in providing an efficient and effective citizen service.

ICCC is envisaged as a nervous system of the city which shall enable collation of information and collaborative engagement among city stakeholders, thus helping in the analysis of data for quicker decision-making.

Intelligent operations capability shall ensure data visualization and analysis, real-time collaboration that can help city stakeholders prepare for exigencies, coordinate and manage response efforts, thereby enhancing the ongoing efficiency of city operations. Furthermore, the ICCC shall help in anticipating the challenges and minimizing the impact of disruptions.

The key objective of this project is to establish a collaborative framework where input from different functional departments such as Transport, Water, Solid Waste Management, Fire, Police, Traffic, e-governance etc. can be assimilated and analyzed on a single platform for building an effective decision support system.

Indicative municipal and non-municipal services that can be supported well by ICCC are depicted in the infographic as below.


City Infrastructure Management
Dasboards for project monitoring and analysis
Drone based monioring of construction activity or infrastructure maintenance checks
Fleet Management (SWM, Fire Dept, Ambulance)
CCTV Monitoring for Critical Infrastructure, etc.
Management of Street Lights
Water Supply & Sewage management (SCADA system)
Civic Services Monitoring
Property Tax collection monitoring
Grievance Redressal monitoring
Real-time collaboration with Ward Offices
Environmental & Water Quality Monitoring
Dynamic Messaging & Advertising
CCTV Monitoring for Garbage
Traffic & Transport Management
Signal Management
Traffic Enforcement
Parking Monitoring / Management
City Transport Management
Safety & Surveillance
CCTV or drone based surveillance for law & order
PA System for Centralized Crowd Management
Emergency Call Boxes for enhanced safety of women, elderly & children
Predictive Policing
Disaster Risk Simulation and Prediction
Covid-19 Management
Flood Management
Fire Incidences
Any other Man-made/Natural crisis
Predictive Disaster Forecasting

1.3 Envisaged Benefits for the city

Following benefits are the envisaged though ICCC,

a. **Enable real-time monitoring** of various facets of management of {CITY_NAME} Smart City i.e., Security, Traffic, e-governance services, City Utilities and many more.

b. **Increased Traffic Efficiency**: Reduction in stoppage time, optimized cycle times of intersection to regulate and maintain free flow of traffic to enhance the efficiency of the road & transport infrastructure. Traffic intersections designed for differently abled should help in improving the quality of life and convenience for people with disability.

c. **Increased Travel Speed:** Optimized signal timings shall result in improved road network performance, enabling higher travel speed. It shall be possible to plan traffic diversions and traffic re-routing for a particular public event and avoid road congestion and minimize inconvenience to the citizens.

d. **Increase Operational Efficiency:** City Authorities intend to spend more time on public facing functions. Thus, ICCC solutions should help in reducing repetitive paperwork/records & making the back-office as well as city operations management functions more efficient.

e. **Safety Improvement:** The real-time safety management, traffic monitoring and intelligent traffic control can help prevent accidents and also respond to potentially dangerous situations in advance.

f. **Higher Productivity:** Achieving improvement in the productivity, logistics and other economic activities by obtaining precise real-time information on transport due to the availability of data on traffic flow in key areas of the city.

g. **Solid waste management:** Addressing the challenges through monitoring mechanisms, instant communication, data-based decisions and automation to bring efficiency and cost effectiveness across the SWM life cycle, convenience to the citizens and cleaner, healthier environment.

h. **Real Time Information & Response:** The real-time information at the ICCC shall help in taking necessary actions and execute the required responses such as sending an emergency vehicle to the spot, arranging alternate routes to VIP convoys, diverting the traffic to different routes etc. It shall be possible to track a particular event using the cameras installed at the traffic junction.

i. **Creating awareness and educating the public:** Through VMD boards, awareness of current traffic situations, road traffic rules and safe driving precautions shall be imparted to road users.

j. **Enforcement:** Continued monitoring of traffic flow at junctions shall reduce the traffic related offences like- Red Light violation and Stop line violations, resulting in effective enforcement of traffic regulations.

k. **Reduction in Pollution:** Optimized traffic flow shall lead to less congestion which shall have a direct impact on the carbon emitted by the vehicles. This shall help improve the air quality of the city and help meet the sustainable goals.

l. **Security and public Safety:** Live Surveillance through a network of CCTV Cameras shall help to identify, apprehend and prosecute offenders and provide live alerts in case of events and incidents.

m. **Effective & Preventive Policing:** The technological interventions proposed for traffic regulation enforcement and CCTV coverage shall enable quick tapping of issues in the form of data and maps such as crime mapping, blind spots identification, hotspots identification, peak hour traffic volume count, average travel time along corridors/ network, among others. This shall enable the law enforcement to reduce crime, do preventive policing and prevent loss of life and property.

n. **Optimize parking and reduce Congestion and Emissions:** Smart parking enables better and real time monitoring and managing of available parking spaces, and guides parking seekers to a parking facility in an informed manner, resulting in reduction of emission of CO^2 and other pollutants. Thus, it creates a better livable environment.

o. **Provide capability to respond** in a unified manner to situations on ground (both day-to-day and in case of emergencies) by creating a birds-eye-view for the relevant stakeholders within the city.

p. **Provide and manage touch points** from all concerned stakeholders during the lifecycle of various incidents.

q. **Define and manage the Key Performance Indicators** (KPIs) for various systems deployed.

r. Provide capability to conduct analysis for continuous improvement of city operations.

s. Better management of utilities and quantification of services.

t. Disaster Management and Emergency Response System.

u. Asset Management for improved allocation of city resources, thereby enhancing the efficiency of the management system.

v. Fraud detection and prevention

w. Provide and manage system for transit management

x. Enhanced Citizen and Government engagement: E-Government services delivered to citizens faster

y. Generate Alerts over different modes of communication related to core systems deployed

z. Availability of city services, anytime, anywhere and on any device

[City to add/modify as per envisaged benefits expected from proposed Smart solutions in their RFP]

1.4 Project objective

Authority is intending to select a **Master System Integrator (MSI)** for setting up an Integrated Command and Control center along with following components **(*Indicative*)** to achieve the {CITY_NAME} smart city's objectives:

- Component 1: Solid Waste Management
- Component 2: City Surveillance
- Component 3: Smart Mobility
    - Smart Traffic management
    - Smart Parking management
    - Intelligent Public Transportation management
- Component 4: Smart Streetlight management
- Component 5: Environmental Monitoring
- Component 6: Smart Governance and Citizen Services
- [Add more/modify]

In order to achieve the convergence with other city level projects, the Integration with existing/proposed ICT systems as below are also envisaged:

a. Water/sewerage SCADA & Smart Meters
b. Electrical SCADA and Smart Meters
c. e-Medicine/Health
d. e-Education
e. City Mobile App and Portal
f. Public Bike Sharing System
g. City payment Card
h. Fire management
i. Dial 100/112
j. Dial !08
k. [Add more/modify]

The above components shall be supported by:

- ICCC Application and Analytics
- Respective Line Department level Command and Control Centers
- Viewing centers at identified strategic locations
- Data Centre and Disaster Recovery Centre
- Cloud based services
- City Communication Network
- Use Cases and SOPs

2. Scope of work and Payment Schedule

2.1 Overview

The MSI shall deploy the team (based out of {CITY_NAME} proposed for the project upon signing of agreement and ensure that a Project Inception Report is submitted to Authority within …… [days] of signing of the agreement, covering following aspects:

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

The MSI shall conduct a comprehensive As-Is study of as existing infrastructure, systems and associated processes in the city in line with project requirement.

The below ILLUSTRATIVE EXAMPLE explains various aspects to be considered during AS-IS study.

[<<The existing infrastructure study of traffic junctions/intersections to be done during various time periods of day including peak and non-peak hours to establish the key performance indicators (KPI) for the ITMS System. The following minimum parameters should be captured during the ITMS study:

- Volumes of vehicles moving in the road network within the area identified for ITMS implementation
- Vehicle type distribution
- Directional distribution
- Physical and visual characteristics of the area
- Travel times, delays between different points of the network
- Additional dependencies with respect to the available infrastructure and geometry at the junctions
- Any other relevant data which the MSI anticipates shall assist in establishing the benchmarks for the project

The MSI shall be responsible to propose transition strategy for dismantling of existing traffic signals, and setting up of new signals and field components, wherever applicable. The proposed strategy should clearly provide approach and plan for implementing the new signals and field components while ensuring minimum disturbance to the road traffic and shall use appropriate static signage designating the work in progress status.

The report shall also include the expected measurable improvements against each KPI as well as use cases to be implemented under ITMS, once the ICCC is commissioned. The benchmarking data should also be developed to track current situation and desired state.>>]

Similar detailed study to be undertaken for other smart component of the project and report to be submitted to the Authority. The MSI shall study the existing business processes, functionalities, existing ICT systems and applications.

Additionally, the MSI should provide detailed TO-BE designs specifying the following, at the minimum:

- High Level Design (for all components installed) for Application architecture, Logical and physical database design, Data dictionary and data definitions, ER diagrams and other data modelling documents and Physical infrastructure design for devices on the field.
- Application component design including component deployment views, control flows, etc.
- Low Level Design (including but not limited to) for all components installed Application flows and logic including pseudo code, GUI design (screen design, navigation, etc.), Database architecture, including defining data structure, data dictionary as per standards laid-down by Government of India/ Government of (State)
- KPI design for the Video wall to visualize important events on real time basis.

2.1.1 Key activities under the scope of the MSI:

- CONOPS design finalization and sign off with Authority
- Project Planning, Procurement, and execution.
- AS-IS and TO-BE Assessment, Survey and Gap analysis for components under the scope.
- Development of use cases and Standard operating procedures (SoPs)
- Site Preparation including required civil work and site clearances.
- Solution design, development, implementation, customization, testing of entire system.
- Deployment of use cases.
- Training- general awareness, Use cases, SoP management, governance, ICCC operation, System maintenance.
- Business Process Reengineering and KPIs for the selected applications/ services
- STQC Certification and system audit
- UAT & Go-live
- Capacity Building
- Operation & Maintenance (O&M) for 05 Years from phase-wise Go-live date
- Security audit and compliance

2.1.2 The bidder shall be responsible to carry out detailed survey prior to submission of the bids in order to familiarize with infrastructure requirement, electrical power, network bandwidth requirement, operational & administrative challenges etc.

2.1.3 The bidder shall furnish the survey report (The template to be specified by the Authority) along with their realistic assessment of AS-IS situation and assumptions (if any) for the desired output, as part of their technical bid.

2.1.4 Field equipment installed through this Project would become an important public asset. During the agreement period, the MSI shall be required to repair / replace any equipment if stolen / damaged / faulty

2.1.5 Convergence: Authority has already initiated many projects, which have state of the art infrastructure at field locations deployed under them. The ICCC Infrastructure should be made scalable for future convergence needs. The Authority has envisaged to create a state-of-the-art infrastructure and services for the citizens of {CITY_NAME}.

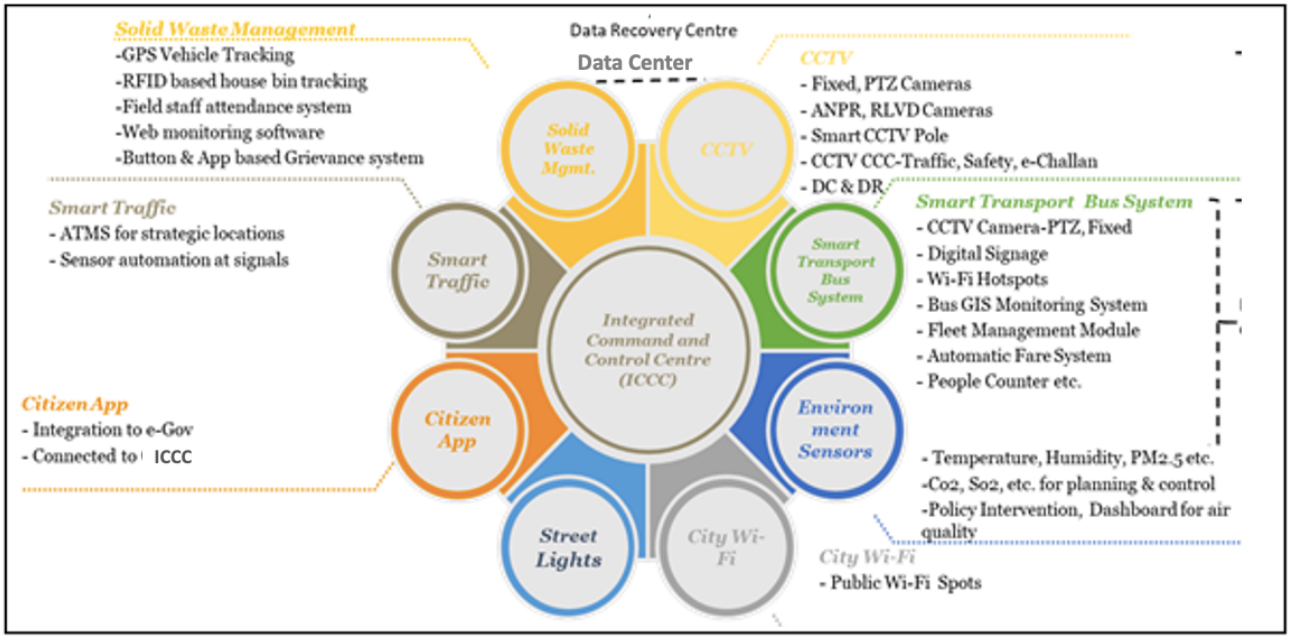
Hence it is imperative that all infrastructure created under the project shall be leveraged for maximum utilization. Therefore, the bidder is required to ensure that such infrastructure shall allow for accommodation of equipment that is being procured under other city projects (e.g. equipment like junction boxes and poles deployed under the ICCC project at the field locations shall be utilized to accommodate field equipment created under the other projects of Authority. The procedure for utilization of the infrastructure shall be mutually agreed between the Authority and MSI.)

The MSI shall note that the activities defined within scope of work mentioned are indicative and may not be exhaustive depending on the respective city specific requirement later provided by them.

MSI is expected to perform independent analysis of any additional work that may be required to be carried out to fulfil the requirements as mentioned in the RFP and factor the same in their techno-commercial bid response.

2.2 Diagrammatic representation for ICCC

(** Illustrative only)



2.3 Responsibility Matrix (Indicative)

R/A = Responsible/Accountable

C = Consulted

I = Informed

#	Key Activities	MSI	Municipal Corporation	Smart City SPV	Other Departments	PMC	Existing ICT Vendors of Authority
1	Project Kick Off	R/A	C	C	I	C	I
2	Deployment of manpower	R/A	C	C	I	C	I
3	Assess the requirement of IT and Non-IT Infrastructure	R/A	C	C	C	C	C
4	Involving and facilitating with departments for business process assessment	I		R	A	R	
5	Providing As-Is information		R/A	R/A			

6	Assessment of Business processes	R/A	C	C	C	C	I
6	Acceptance of changes and ownership of business process post assessment	I		R	A	R	
8	Assessment of Software/ Application requirements	R/A	C	C	C	C	I
9	Assess the Integration requirement	R/A	C	C	C	C	C
10	Assess the connectivity requirement all locations (Field level+ ICCC/DC/DR site)	R/A	C	C	C	C	I
11	Providing relevant data sets for identified use cases			R	A		
12	Assessment of available city data sets	R/A	C	R	I	C	I
13	Preparation and finalization of use cases	R/A		R	R	C	I
14	Assessment of training requirement	C	C	R	A	C	I
15	Develop the Concept of Operations (CONOPS)	R/A	C	R	R	C	I
16	Formulation of Solution Architecture	R/A	C	C	C	C	I
17	Preparation of Detailed Drawing	R/A	C	C	C	C	I
18	Preparation of detailed Design of ICCC Solution	R/A	C	C	C	C	I
19	Development of test cases (Unit, System Integration and User Acceptance)	R/A	C	R	R	R	R
20	Preparation of phase wise bill of material	R/A	C	C	C	C	I
21	Approval of material for procurement	C		R/A		C	
22	SoP preparation	R	C	A	A	C	I
23	Material Procurement including software licenses	R/A	C	C	I	C	I

24	Physical Infrastructure setup	R/A	C	C	I	C	I
25	IT and Non-IT Infrastructure Installation	R/A	C	C	I	C	I
26	Development, Testing and Production environment setup	R/A	C	C	I	C	I
27	Software Application customization (if any)	R/A	C	C	I	C	I
28	Development of Bespoke Solution (if any)	R/A	C	C	I	C	I
29	Implementation, testing of Solutions and urban services	R/A	C	C	I	C	I
30	Integration of GIS and other sub-systems in ICCC	R/A	C	C	C	C	I
31	Providing data for migration in the specified format	C		R	A	C	C
32	Data Migration	R/A	C	C	I	C	I
33	Training contents preparation	R/A					
34	Integration with city level/Third party services/application (if any)	R/A	C	C	I	C	R/A
35	SoP and KPI implementation	R/A	C	C	C	C	I
36	User Acceptance Testing	R/A	C	C	I	C	I
37	Helpdesk setup	R/A	C	C	I	C	I
38	Preparation of manual/ documents for system installation, system operation, User guide, SoPs	R/A	C	C	I	C	I
39	Role based training(s) on the Smart Solutions	R/A	C	C	I	C	I
40	Go Live	R	C	R/A	I	C	I
41	Operation and Maintenance of IT, Non-IT infrastructure and Applications	R/A	C	C	I	C	I
42	SLA and Performance Monitoring	R/A	C	R	R	C	I

43	Logging, tracking and resolution of issues.	R/A	C	C	I	C	I
45	Application enhancement	R/A	C	C	I	C	I
46	Patch & Version Updates/upgrades	R/A	C	C	I	C	I
47	Future Integration with other services/infrastructure	R/A	C	C	I	C	I
48	Business process re-engineering	R/A	C	C	C	C	I
49	Use-cases enhancements	R/A	C	C	C	C	I
Note: 1. Authority shall extend required support to prospective bidders to familiarize with city environment during pre-bid stage to help in bringing clarity of above Roles and responsibilities 2. Authority may modify the above matrix as per project requirements, which shall be adhered to, by all the stakeholders as mentioned above.							

The MSI shall ensure that all identified and approved use-cases are implemented along with Standard Operating Procedures (SoPs) to measure city performance against key outcomes that they bring to various city stakeholders.

An indicative list of use cases is mentioned in Section 12 (Domain Use Cases). These use cases shall be key acceptance criteria during UAT. For this purpose, the bidder needs to factor costs associated with use case implementation into their pricing and ensure that domain use cases are ready before UAT phase. Finalization of use cases shall be done in design phase in coordination with the Authority.

The solution proposed by bidder should provide an option to integrate existing deployed solution by the city and needs to provide scalability option to implement new use cases as and when new smart systems are deployed in the city.

The MSI shall provide supporting documents in the technical bid justifying the approach & design of offered solution. The technical marking is specified in the evaluation criteria mentioned in the volume 1 of the RFP document.

2.4 Project Deliverable, Milestones and Timelines

T = date of signing of agreement

#	Milestone	Deliverables	Timelines (in months)
Phase 0			T+ 3 months
1.	Project Initiation	○ Project Team deployment, Detailed Survey Report including infrastructure AS-IS and TO-BE	T+3 months

		assessment, phase wise location distribution ○ Site Assessment Report ○ Detailed Project deployment plan including Operations management, Contract management, Risk management, Information Security and Business Continuity ○ High Level Design, Low level design, Use cases finalization ○ Design of CONOPS for utilities to be configured as per Project deployment plan. ○ Set up Project Management Platform and portal to push project design and technical documents.	
Phase 1			T+6 months
2. Delivery of Urban Services-1 (US-1): Part -1			
	Supply, installation, commissioning, training & operationalization of (US-1) at [50%] of [total no. of identified locations], along with field level smart components at these locations	○ Material Delivery, inspection reports (component-wise) ○ Installation and testing ○ Use case deployment ○ Urban Service Go-live ○ Integration with other systems ○ Handover of Software Licenses ○ Training Completion Certificate ○ Acceptance/Go-Live Certificate from Authority ○ [Add/Modify]	T+6 months
3. Delivery of Urban Service-2 (US-2): Part -1			
	Supply, installation, commissioning, training & operationalization of (US-2) at [50%] of [total no. of identified locations], along with field level smart components at these locations	○ Material Delivery, inspection reports (component - wise) ○ Installation and testing ○ Use case deployment ○ Urban Service Go-live ○ Integration with other systems ○ Handover of Software Licenses ○ Training Completion Certificate	T+6 months

		○ Acceptance /Go Live Certificate from Authority ○ [Add/Modify]	
4. Delivery of Urban Service- n (US-n): Part -1			
	Supply, installation, commissioning, training & operationalization of (US-n) at [50%] of [total no. of identified locations], along with field level smart components at these locations	○ Material Delivery, inspection reports (component - wise) ○ Installation and testing ○ Use case deployment ○ Urban Service Go-live ○ Integration with other systems ○ Handover of Software Licenses ○ Training Completion Certificate ○ Acceptance /Go Live Certificate from Authority ○ [Add/Modify]	T+6months
5. City Network Backbone (Capex/Opex): Part -1			
	Supply, installation, commissioning, training & operationalization of city network at identified locations where urban services to start	○ Material Delivery, inspection reports (component-wise) ○ Installation and testing and commissioning ○ Integration with other systems ○ Training Completion Certificate ○ Acceptance /Go Live Certificate from Authority ○ [Add/Modify]	T+6months
6. ICCC, DC, DR and Viewing centers: Part -1			
	Design, supply, installation, commissioning, and operationalization of DC, DR and ICCC, viewing centers, including interior civil work.	○ Material Delivery, inspection reports (component - wise) ○ Installation and testing and commissioning ○ ICCC Go-live ○ Integration with other systems/applications ○ Handover of Software Licenses ○ Training Completion Certificate ○ Acceptance/Go-Live Certificate from Authority	T+6 months

		○ [Add/Modify]	
Phase 2			T+9months
7. Delivery of Urban Services-1 (US-1)- Part 2			
	Supply, installation, commissioning, training & operationalization of balance work of Phase -1 of (US-1)	○ Material Delivery, inspection reports (component - wise) ○ Installation and testing ○ Use case deployment ○ Urban Service Go-live ○ Integration with other systems ○ Handover of Software Licenses ○ Training Completion Certificate ○ Acceptance /Go Live Certificate from Authority ○ [Add/Modify]	T+9 months
8. Delivery of Urban Service-2 (US-2)- Part 2			
	Supply, installation, commissioning, training & operationalization of balance work of Phase -1 of (US-2)	○ Material Delivery, inspection reports (component - wise) ○ Installation and testing ○ Use case deployment ○ Urban Service Go-live ○ Integration with other systems ○ Handover of Software Licenses ○ Training Completion Certificate ○ Acceptance /Go Live Certificate from Authority ○ [Add/Modify]	T+9 months
9. Delivery of Urban Service- n (US-n)- Part 2			
	Supply, installation, commissioning, training & operationalization of balance work of Phase -1 of (US-n)	○ Material Delivery, inspection reports (component - wise) ○ Installation and testing ○ Use case deployment ○ Urban Service Go-live ○ Integration with other systems ○ Handover of Software Licenses ○ Training Completion Certificate	T+9 months

		○ Acceptance /Go Live Certificate from Authority ○ [Add/Modify]	
10. City Network Backbone- Part 2			
	Supply, installation, commissioning, training & operationalization of city network at identified locations where urban services to start.	○ Material Delivery, inspection reports (component - wise) ○ Installation and testing ○ Use case deployment ○ Urban Service Go-live ○ Integration with other systems ○ Handover of Software Licenses ○ Training Completion Certificate ○ Acceptance /Go Live Certificate from Authority ○ [Add/Modify]	T+9 months
11. Additions/ enhancement- ICCC, DC, DR and Viewing centers- Part 2			
	Design, supply, installation, commissioning, and operationalization of additional services, DC and DR, IT/Non-IT infrastructure enhancement, other viewing centers etc,.	○ Material Delivery, inspection reports (component - wise) ○ Installation and testing ○ Use case deployment ○ Urban Service Go-live ○ Integration with other systems ○ Handover of Software Licenses ○ Training Completion Certificate ○ Acceptance /Go Live Certificate from Authority ○ [Add/Modify]	T+9 months
Note: 1. Authority may decide to increase OR decrease no. of phase-wise go-live (such as phase-3 & above) as per city specific requirements. 2. For those urban services not planned in Phase-1, the city can adopt similar approach (for subsequent phases) in regard to project deliverables and milestones as applied above for Phase-1 and 2. 3. CONOPS should be ready before finalizing the roll out plan. [The Timeline specified above are Indicative. the Authority may align as per specific requirements]			
12. Operation and Maintenance phase (O&M)		Monthly SLA Compliance Report	60 months from the date of

		Phase wise Go-Live acceptance by the Authority.

2.5 Deemed Acceptance

The Authority shall provide acceptance for go-live of each milestone within 60 working days from the date of completion of the UAT for that milestone. The Authority shall provide the following to the MSI:

- Stakeholders/Approvers involved in deliverable, project output
- Deliverable details and its impact/strategic outcome
- Deliverable Timeline calendar with alerts to all Stakeholders/Approver
- Sign off timeline calendar with alerts to all Stakeholders/Approvers

In case the Authority fails to respond and provide feedback on above stated submission, the deliverables shall be DEEMED ACCEPTED.

Post the elapse of the 60 days' approval period, the MSI shall not be asked to rework on the said project outputs/outcomes. However, in case the Authority confirms to the MSI with an alternative date, then that date would hold valid for the deemed acceptance. Such revisions shall be limited to 2 (two).

Any subsequent rework post acceptance/deemed acceptance would form the subject of a formal "Change Control/ Change Request", which has been detailed in Article 55- Change Control Note (CCN) of Volume III.

2.6 Payment Schedule

T1- Phase 1 Go-Live

T2- Phase 2 Go-Live

[More phases may be added by the authority]

Payments to MSI, after successful completion of the target milestones, shall be made as under:

#	Scope of Work	Timelines	Payment
1.	Phase-0	T + 3 Months	…% as Mobilization Advance (Note 1)
2.	Phase-1 Operationalization & acceptance of Go Live	T1= T + 6 Months	**On Delivery of material and acceptance by authority** ○ 35% of actual value of Material as required for phase -1 **On acceptance of go-live** a) Supply items

			○ 50% of actual value of Material supplied for DC, DR, ICCC infrastructure and applications cost of phase-1 ○ 50% of actual value of Material supplied for Urban Service-1,2…n of phase-1 ○ 50% of actual value of Material supplied for city backbone network cost for Urban Service-1,2…n of phase-1 b) Implementation Services ○ 85% of actual value of Implementation service (including development, installation, testing, commissioning, training) of phase-1
3.	Phase-1 Operations & Maintenance (O&M)	T1+ 60 Months	Equal quarterly installments of the total O&M cost.
4.	Phase-2 Operationalization & acceptance of Go Live	T2 = T + 9 Months	**On Delivery of material and acceptance by authority** ○ 35% of actual value of Material supplied and accepted by authority as required for phase -2 **On acceptance of go-live** a) Supply Items Balance payment of Phase-1 ○ 65% of actual value of Material supplied for DC, DR, ICCC infrastructure and applications cost of phase-2 ○ 65% of actual value of Material supplied for Urban Service-1,2…n of phase-2 ○ 65% of actual value of Material supplied for city backbone network cost for Urban Service-1,2...n of phase-2 b) Implementation Services ○ Balance payment of phase-1 (Implementation services) ○ 100% of actual value of Implementation service (including Development, installation, testing, commissioning, training) of phase-2
5.	Phase-2 Operations & Maintenance (O&M)	T2+ 60 Months	Equal quarterly installments of the total O&M cost.

[Note:

1. Mobilization advance to be adjusted against subsequent payments, starting from Phase-1.

2. For those urban services not planned in Phase-1, the city can adopt similar pattern as applied above for Phase-1 and 2.

3. The city to ensure that the Price bid format is aligned accordingly.]

- The bill of material proposed by the MSI shall be approved by Authority. The template is provided in Annexure A.2.14, A.2.14, and Annexure A.3.3 of Vol I. The exact quantity and requirement shall be proposed as part of the technical bid by the bidder.
- All payments to MSI shall be made upon submission of invoices along with necessary approval certificates from concerned Authorities.
- The request for payment shall be made to Authority in writing, accompanied by invoices describing the services performed, and by the required documents submitted pursuant to general conditions of the contract and upon fulfilment of all the obligations stipulated in the agreement.
- Due payments shall be made promptly by Authority generally within sixty (60) days after submission of an invoice for payment by MSI. The Taxes, as applicable, shall be deducted / paid, as per prevalent rules.
- The currency or currencies in which payments shall be made to the MSI shall be Indian Rupees (INR) only. All remittance charges shall be borne by the MSI.
- In case of disputed items, the disputed amount shall be withheld and shall be paid only after settlement of the dispute.
- Any penalties/liquidated damages, as applicable, for delay and non-performance, as mentioned in this RFP document, shall be deducted from the due payments of the respective milestones.

3. ICCC System Architecture

3.1 Introduction

The bidder shall design the ICCC solution incorporating guiding principles, foundational design aspects for the functionalities/ components as mentioned below, which are further detailed out in this RFP - volume II.

- ICCC Application & Analytics
- Use cases, KPIs and SOPs
- Data Management
- Geographical Information System (GIS)
- IoT Platform
- Cybersecurity
- DC-DR/ Cloud Infrastructure
- City Communication Network
- ICCC Physical Build Infrastructure
- Smart Components
- Urban Solutions

The MSI shall submit a detailed Technical solution, including CONOPS, logical architecture, data architecture, integration architecture, network architecture, security architecture and deployment architecture. MSI shall describe how each of the functionalities/ components shall work in their overall solution. MSI shall also detail the platforms and tools they propose to implement for achieving the standardization requirements as listed in the sections that follow along with compliances (wherever applicable).

Common Principles/ Gudielines regarding compliance of IT systems/equipments shall also be captured along with Perpetual licenses, Software licensing, IPv4 and IPV6 compliances, etc.

The MSI is requested to refer 'section 3.4 Reference architecture' for standardization requirements.

3.2 Guiding Principles

MSI shall design the solution while taking into consideration the following guiding principles:

3.2.1 Scalability

Important technical components of the architecture must support scalability to provide continuous growth to meet the growing demand of the city. The architecture should be scalable (cater to increasing load of internal and external users and their transactions) and capable of delivering high performance at all times. The solution should support vertical and horizontal scalability so that depending on changing requirements from time to time, the solution may be scaled upwards. There must not be any system-imposed restrictions on the upward scalability of data center IT components such as compute infrastructure such as Application & Web Servers, Database Servers, data storage

infrastructure, bandwidth, application software, number of cameras, or other smart city components required in this RFP. The data center infrastructure shall be capable of serving the growing concurrent users' requirement which would be increasing as the city grows.

3.2.2 Availability

The architecture components should provide redundancy and should be resilient to technology sabotage. It should be ensured that there are no single points of failures in the key solution components, including core/data center components. To take care of remote failures, the systems should be configured to mask and recover with minimum outage. The MSI shall make the provision for high availability for all the services of the system.

3.2.3 Security

The architecture should adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc. MSI should make provisions for security of field equipment as well as protection of the software system from hackers and other threats. Bidder's solution shall adhere to the model framework of cyber security (K- 15016/61/2016-SC-1, Government of India, and Ministry of Urban Development) and also section 9 of this RFP, while designing the solution, the ICCC system shall be highly secure as it is intended to handle sensitive data relating to the city and its residents. The Authority would carry out the security audit of the entire system upon handover and also at regular intervals during O&M period.

3.2.4 Manageability

Ease of configuration, ongoing health monitoring, and failure detection are vital to the goals of ICCC project. The system should be auto/manual configurable for various future requirements for the ease of maintenance / debugging.

3.2.5 Interoperability

The system should have interoperable capability with other ICT Systems.

3.2.6 Open Standards

Systems should be built on open standards and protocols. Keeping in view the evolving needs of interoperability considering that solution shall become the focal point of delivery of services and may also involve cross-functionality with the project systems of other departments The MSI shall ensure that the ICCC application developed is easily integrated with the existing applications using open APIs. The software code should not build a dependency on any proprietary software. The standards should at the minimum comply with the published national standards such as BIS standards for smart cities, e-governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time). Systems implemented by the MSI shall adhere to the Unified Digital infrastructure (UDI) properties defined in IS 18000 and the data principles defined in Table 1 of IS 18002.

3.2.7 Universal Access IT Systems

The solution designed should ensure Universal Access to IT systems to empower citizens of {CITY_NAME} city with disabilities, to access various systems/components envisaged and future systems for integrations with ease. The bidders should refer to Annexure XXXXX for minimum requirements for Universal Access to IT Systems.

3.2.8 Single-Sign On

The application should enable single-sign-on so that any user once authenticated and authorized by the 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 a single sign-on mechanism, shall provide access to all the services of the departments concerned (based on role based access policy), Help module, basic and advanced reporting etc. Similarly, for external users (citizens, etc.), based on their profile and registration, the system shall enable single sign-on facility to apply for various services, make payments, submit queries/complaints and check status of their applications/queries.

3.2.9 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) including e-sign. In particular, 3 factor authentications (login id & password, biometric and digital signature) shall be implemented by the MSI for officials/employees involved in processing citizen services.

3.2.10 GIS Integration

MSI shall undertake detailed assessment for integration of all components (e.g., e- Governance, Surveillance System etc.) with the Geographical Information System (GIS). MSI is required to carry out the seamless integration of ICCC with GIS to ensure ease of use of GIS in the dashboards in ICCC. If this requires a field survey, it needs to be done by MSI/**{AUTHORITY},** If such data is already available with the city, it shall facilitate the same. MSI shall check the availability of such data and its suitability for the project. MSI is required to update GIS maps from time to time. Please refer Section 6 for detailed GIS requirement.

3.2.11 Application Architecture

The software applications designed and developed must follow best practice and industry standards and shall be based on approved requirements. In order to achieve 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 ICCC Applications should integrate with key initiative of State, namely Portal Services, Citizen Contact Center, and Certifying authority, etc.

The systems should at least comply with the published BIS smart city standards, eGovernance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time) and https://bis.gov.in/. System implemented in the city shall adhere to the

Unified Digital infrastructure (UDI) properties defined in IS 18000 and the data principles defined in Table 1 of IS 18002

All IT products and services used by MSI must necessarily incorporate the principle of Universal Design and global accessibility standards as approved by MeitY. In absence of any such MeitY approved standards, MSI should adhere to global accessibility standards as reference (e.g. EN 301 549).

All information portals and websites developed by MSI for information dissemination must necessarily be in accessible formats, adhering to the provisions of the WCAG 2.0, Web Access Guidelines. The IT systems should be built, with an aim, to provide maximum accessibility and usability to its users irrespective of device in use, technology or ability.

3.3 Key Design Considerations for ICCC application

Bidders should keep in mind the following design considerations during the implementation stage of ICCC application;

ICCC to be designed as a system-of-systems	Various sub-systems should talk to the ICCC, thereby providing common operating picture on city operations to ICCC supervisors and Smart City/ULB leadership - in normal circumstances as well as during emergency or crisis
Focus to be on outcomes	ICCC implementation to be driven by use cases to deliver specific outcomes for various departments and stakeholders of the city. Various prevalent deployment models (IaaS, PaaS, SaaS) while designing and deploying the use cases may be adopted while subscribing to Cloud to suite the functional, scalability and performance requirements. Refer Sec 12 of this Volume 2 for indicative use cases that can be implemented through the ICCC. The ICCC Maturity Assessment Framework (IMAF) may also be additionally referred for the same. [<< Authority to provide the weblink>>]
Scalable and Interoperable Architecture	IT usage within cities is going to increase in years to come and thus productive use of ICCC is expected to improve only with the passage of time. Scalable architecture can support integration of additional sub-systems in future, without additional/substantial investment of time & money
Adhere to open standards & IndEA Framework	ICCC platform should follow open standards and use Open APIs. It should also adhere to the IndEA framework released by MeitY, Govt. of India
Robust IT Security Systems & Policies	ICCC is expected to become the brain and nervous system for city operations, with access to a lot of valuable data & systems. It is thus, essential that a robust IT Security system be designed & implemented to safeguard the data & systems from internal/external threats

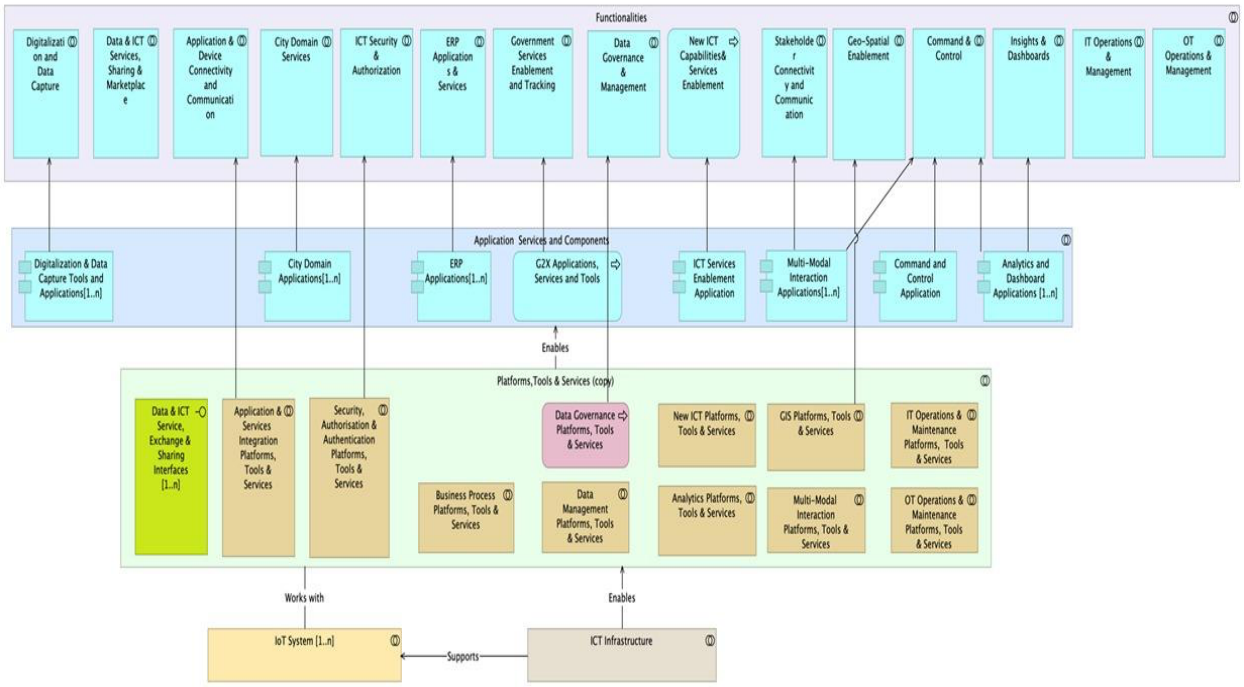
Address data privacy concerns	ICCC shall have access to various data sets - video, audio & text data, both through field level systems such as CCTV cameras, sensors or through social media or grievances received. It's essential to have right access controls and usage guidelines to address privacy concerns
Compliance with PPP-MII provisions	DPIIT has notified orders to promote manufacturing and procurement of locally manufactured products and services under the Make in India initiative. Bidders are required to comply with the same.

The following section provides more detailed solution architectural requirements.

3.4 Reference Architecture for ICCC

The solution architecture for ICCC shall have broad set of components/layers as indicate below. It may be noted that some of the layers/components might already exist in the city and the MSI should leverage these as best as possible (at city level) to reduce the cost.

Detailed description of each layer is given below.



3.4.1 Component Layers

a) Compute-Data Center /cloud Layer

The compute-data center layer shall house centralized computing and storage resources needed to store, process and analyze the digital data required to derive actionable information. This layer includes general purpose compute servers, specialized GPU clusters, non-volatile storage clusters, data center network equipment and system software for Operations & Service management and Security & Trust management. Please refer Section 9.2 in IS 18000:2020 ICT Reference Architecture

(ICT RA) for details (attached at Annexure…….). This layer should have redundancy and disaster recovery capabilities.

The MSI can have following options: a) Cloud solution, b) On-premises solution, c) Hybrid on-premises and cloud solution. The detailed considerations for these are described in the DC-DR/ Cloud Infrastructure section of this RFP. The MSI should also identify the preferred or recommended model being proposed to Authority, its advantages/disadvantages and why that shall be a good fit for Authority.

The layer should be sized to meet the compute throughput (Transactions(s)) and bandwidth (MB(s)) requirements as derived from the application and use cases mentioned elsewhere in the document.

The MSI should propose a methodology for scaling up of the performance metrics as the needs of the city grow by a factor of 10x.

b) Communication Layer

- The secured communication layer shall serve to provide connectivity to gather data from sensors including video cameras and other field devices and communicate messages to display devices, actuators and other field devices.
- It shall support all smart urban solutions (sensors. displays, Wi-Fi services etc.) at given locations as required by the use cases and application detailed elsewhere in the document.
- The MSI may suggest the required throughput, latency and availability to meet the use cases and application needs mentioned elsewhere in the document.
- The MSI should propose a methodology for scaling up of the performance metrics as the needs of the city grow by a factor of 10x. Such a scale up should be possible via seamless addition of new endpoints and appropriate provisioning of network resources.
- The MSI Shall detail out two main components of the communication layer:
    - A Wide Area Network to bring data from across the area of interest to the compute-data center
    - A field network to interconnect all the field devices to their respective gateways to eventually get connected into the applications in the compute-data center layer. (Note that either or both of the above might not be needed to be developed, if alternative communication infrastructure is already available)
    - A standards-based field device and network management framework should be adopted and demonstrated by the MSI.
    - Provisioning of network connectivity/bandwidth shall be done by the MSI as part of their scope, subject to TRAI regulation.
    - MSI shall also provide detailed bandwidth calculations with appropriate justifications in their bid. Indicative bandwidth Calculations for various components as envisaged in the scope may be provided

- MSI shall design the network in such a way that there are no interdependencies amongst the various components. Refer to the "City Communication Requirements" section.

Following standards as provided in Annex may also be referred -

- IS 18010 (Part 1): 2020 Unified Digital Infrastructure - Unified Last Mile Communication Protocols Stack Part 1 Reference Architecture (UDI - ULMCPS – RA)
- IS 18010 (Part 5/Sec 1): 2020 Unified Digital Infrastructure - Unified Last Mile Communication Protocols Stack Part 5 Network Access Layer (IEEE 802.15.4)
- IS/IEEE 802.15.4 LITD/28 Low-rate wireless networks

c) Sensors, Actuators and IoT Layer

- The Sensors, Actuators and IoT layer shall help the city administration to gather information or capture information from the field devices like solid waste management system, intelligent traffic signals, cameras, Wi-Fi, enforcement sensors, etc.
- The exact sensors, actuators and their numbers and physical deployment locations, as well as data rates, bandwidths and latencies, shall be driven by the applications and use cases scenarios described elsewhere in the document.
- The MSI should indicate/explain the plan/capability of their solution for scaling by up to 10x to meet the future requirements of the city.
- The solution should be based on standards based IoT architecture (as per IS18004: UDI IoT System Reference Architecture).
- The MSI may use a 3rd party IoT system to provide the IoT data.
- The IoT System implemented in the city shall adhere to the Unified Digital infrastructure (UDI) properties defined in IS 18000 and the data principles defined in Table 1 of IS 18002
- The data to/from the IoT system (i.e. from the devices) (whether by the IoT solution of the bidder or a 3rd party IoT system) should be available as per the standards based, data exchange framework (IS18003-1 and 18003-2)
- The MSI should explain the security architecture, tamper detection schemes if any and non-repudiation of the data from the field devices. The security architecture should be as per appropriate international standards, 8.14 of IS18000 and Indian Government guidelines
- The MSI should indicate the expected key performance indicators like data rate, latency and availability.
- The MSI should explain the life cycle management of the field devices, including the periodic maintenance of such devices. The IoT management should be as per Chapter 8.11 of IS18000.

d) Platform Tools & Services Layer

This is a key software layer that converts the ICCC system into a platform that shall allow it to be extended in the future with new functionalities and capabilities. Various prevalent cloud deployment

models (IaaS, PaaS, SaaS) may be adopted to suite the functional, scalability and performance requirements.

The components of this layer are:

- **Data Management Platform, Tools & Services:** This is the data layer for the solution and is described in brief in 8.12 and 9.4.2 of IS18000 and in detail in IS18002.
- **Data Governance Platform, Tools & Services:** This pertains to management, policies, quality, privacy etc., for the data and is covered in 8.12 and 9.4.3 of IS18000 and in IS18002.
- **Analytics Platforms Tools & Services:** This pertains to analysis of data to extract actionable insights and is detailed in 9.4.4 of IS 18000 and in IS 18002.
- **Application and Services Integration Platform, Tools & Services:** This pertains to integration of applications running within the ICCC as well as from external departments. These shall also allow legacy applications systems to get integrated into the ICCC. This is further detailed in 9.4.1 of IS18000.
- **GIS Platforms Tools & Services:** Geo-Spatial enablement shall be achieved by this layer and is described in detail in 8.15 & 9.4.5 of IS18000 and in IS 18008.
- **Multimodal Interactions Platforms, Tools & Services:** This shall enable interactions with all stakeholders via diverse modalities of text, email, messaging, social media, video, voice etc. This is detailed in 9.4.6 of IS18000.
- **IT Operations & Management Platforms, Tools & Services:** This shall enable management of the ICT Systems in ICCC using standards-based interfaces and tools. The functionalities are detailed in 9.4.7 & 8.10 of IS 18000.
- **Business Process Platforms Tools & Services:** Allows creation and automation of Standard Operating Procedures using standards like BPMN etc. (see 9.4.8 of IS 18000)
- **Security, Authorization & Authentication Platforms, Tools and Services:** Collection of tools and processes to implement cyber-security. (see 9.4.9 & 8.14 of IS 18000)
- **IoT Operations & Management Platforms, Tools & Services:** This shall allow management of operational assets like field devices etc. (see 8.11 of IS18000 and IS 18004)
- **Data & ICT Services Exchange and Sharing Interfaces:** (8.8 & 9.4.11 of IS18000). Data exchange shall be as per IS18002-1-1 and 18002-1-2. Service integration shall be achieved via integration tools like enterprise service bus, message brokers and/or API gateways (8.13, 9.4.1 of IS18000). The integration should be responsible for data exchange to and from other systems developed by the government (such as police department, traffic department, street lights department, water department, irrigation department, transport organizations within {CITY_NAME}) and non-government agencies.
- **New ICT Services Platform, Tools & Services:** (8.9 & 9.4.12 of IS18000). The ICCC platform should not remain static with only the initial set of applications and services, but rather should allow onboarding and provisioning of new applications as well as decommissioning of old, unnecessary applications. It shall help the platform to evolve/grow with time with the

applications added and integrated as and when they are developed at Authority. The MSI should indicate how such capability may be achieved.

- MSI shall describe how each of the above listed functionalities shall be met in their solution and what platforms and tools they propose to implement for achieving the objectives.

e) Security Layer

Information and Infrastructure Security plays a very critical role in protecting the smart city physical assets such as field IoT devices, IT infrastructure and logical assets such as field data and citizen data. ICT security covers all layers such as Infrastructure, Data, Integration, Services and Applications.

The detailed functional requirements of the security layer are as per Section 8.14 of the IS18000 and covers

- Application security,
- Data security
- API security
- Security Emergency Management
- IP Protection and data loss prevention.

MSI shall describe how end-to-end security is achieved in their solution and what platforms and tools they propose to implement for achieving the objectives. Bidder's solution shall adhere to the model framework of cyber security (K- 15016/61/2016-SC-1, Government of India, and Ministry of Urban Development) and further guideline as per section… of this document, while designing the solution.

f) Application Services & Component Layer

This layer of the ICCC system shall be driven by the actual use cases and applications desired by the City, which is covered under the use cases section of this document. It shall broadly consist of the following components. [The specifics shall be as per the city application needs].

- **City Domain Applications:** These shall be the core applications in various verticals as detailed under Smart Urban solutions section 2 of RFP volume II. These shall be integrated into the ICCC systems (in terms of exchanging data, alerts, etc.), leading to generation of new insights and dashboards, especially across different vertical silos. This is detailed in 8.3 & 9.5.3 of IS18000.
- **ERP applications:** These shall deliver ERP functionalities for the City Administration as detailed in 8.5, 9.5.4 & Annex D of IS18000 and in detail in IS 18006-1
- **G2X Application Services & Tools:** Covers the necessary E-Governance Services and applications as well as the ability to track them. See 8.4 & 9.5.5 of IS18000 and in detail in IS 18006-1.
- **Command & Control Applications:** Allows oversight, decision support and management of city's operations (8.2 & 9.5.7 of IS18000)
- **Analytics & Dashboard Applications:** Analytics applications shall use the analytics tools of the ICCC platforms to perform data analysis to provide trends & predictions. These should be visualized in various forms. These shall enable citizens and administrators alike to get a

holistic view of city conditions. These could be seen on displays inside ICCC as viewed over a web browser or available in form of a mobile application (8.1 & 9.5.8 of IS18000). Moreover, the tools of this layer shall also provide predictive functionalities for predicting events and alerting the stakeholders through insights and dashboards for appropriate action.

- **ICT Services Enablement Application:** These applications shall allow lifecycle management of existing applications as well as allow onboarding and provisioning of new applications (8.9 & 9.5.6 of IS18000)
- **Multi-Modal Interaction Applications:** These applications shall enable interactions between various stakeholders via multiple channels and modalities (8.6 & 9.5.2 of IS18000)
- **Digitalization & Data Capture tools and applications:** These applications shall allow for scanning, curating and managing documents (in case of data which is not in digital form). For digital data, it shall consist of forms (to gather data from people), as well as data from social media sources, chatbots, message boards etc. (see 8.7 & 9.5.1 of IS18000)

4. ICCC application and Analytics

4.1 Overview

ICCC as a platform through its different layers and components shall act as a Decision Support System (DSS) for city administration to respond to real-time events by consuming data feeds from different data sources and by processing information out of data sets.

Core objectives to be attained through a well-designed ICCC application are listed below:

- Monitoring and management of various city infrastructure/utilities like water, streetlights, solid waste management, roads development, etc.
- Continuous analysis of data, preparation of dashboards for effective decision making by department heads, city leadership, creating simulations
- Increasing the situational awareness within city by providing insights using data across urban functions
- Faster response to the incidents, crisis situations; enhancing disaster resilience
- Enhancing collaboration across multiple departments within and outside urban local bodies and other government bodies
- Enhanced communication across different stakeholders in the city, including citizens, in day-to-day matters as well as during crisis situations
- Real time urban planning

4.2 Functional Requirements

ICCC platform may be offered as a cloud and edge based architecture. ICCC platform can include integration framework for:

- End device (Field) through IoT platform
- Service level integration
- GIS based dashboard for monitoring
- ICCC platform should be ready with e-governance and citizen centric application so that inter deployability is taken care of on day one.
- Blockchain shall be an important technology in providing citizen services. ICCC platform may have provision (Optional) for block chain platform integrated with e-sign capabilities to offer the following capabilities
    - Blockchain framework for recording transactions ensuring trust worthiness
    - Temper evident storage of e-signed documents and enabling traceability

Following Use cases may be considered on Blockchain are:

- Land Records, Property Tax
- Vaccination
- Contracts and agreements

- Financial Transactions

The ICCC application shall have following functionalities:

#	Functional Area	Function requirement
1	ICCC Platform	The ICCC platform should be shall be robust, secure and scalable, complied to the industry open standards and should have provisions for fault tolerance & High Availability. It should provide uniform, coherent, user-friendly and standardized interface for "day to day Operations", "Common Operating Picture" and situational awareness. A standard operating environment (SOE) framework should be followed defining KRAs and KPI's of all involved in the ICCC operations including Inventory management, Emergency response operations. It should be configured to manage operations on a 360 degree basis (e.g. In case of occurrence of an incidence, a thorough analysis and investigation should be possible and remedial actions should be triggered/implemented to resolve the issue as per defined timeline/SoP/SLA including escalation to relevant stakeholders. It should Provide secure API lifecycle, monitoring mechanism for available APIs. It should Provide different tier of user categorization, authentication, authorization, and services based on the subscriptions. It should Provide role-based access view to applications. The platform shall also be able to bring in other city data (from other departments/public/private systems) as i-frames in ICCC dashboard.
2	Software Licenses	There should not be a restriction on Software Application, Database licenses based on the hardware infrastructure.
3	Users and roles	The platform shall have provision to assign one or more role (including more or more locations) for operators to perform tasks at the assigned locations only.
4	Self-Check/ Authentication	The platform should be protected by multiple levels of user authentication to cover against any malware attack/misuse. The platform should be further protected against malicious codes and cyber-attacks. User Authentication should be protected by two level of authentication at Domain level and at

		Module access. Integration with LDAP should be either built-in or integrable. User passwords should be encrypted.
6	Asset Management	The city should maintain complete inventory of critical assets. Asset could be defined as source code, documents, binaries, configuration data, scripts, supplier agreements, SW Licenses. ICCC platform should be able to do asset control with an integrated view of all field assets (such as sensors/devices etc.) accessible and managed through a console application. The platform should provide an asset management functionality to ascertain the location, asset information, date of installation, AMC and support details, etc. both for IT /Non-IT systems throughout the life cycle of the project. The information should be catalogued and modelled as per city needs. Based on the availability and error trends, the platform should be able to produce required report for all important assets. It should have the capability to generate report detailing all maintenance and other works carried out on any asset over any specified period of time.
7	GIS Support	The platform shall integrate with GIS and map information and be able to dynamically update information on the GIS maps to show status of resources and to trigger pre-defined SoPs. The ICCC platform should have the ability to demonstrate and use GIS for spatial analytics specific use cases as per their requirements. e.g. ability to analyse civic utilities like fire hydrants across the city on a city map, or display the ability to analyse city slum pockets on city map.
8	Data Acquisition & Integration	The data acquisition engine aggregates static and real-time data feeds from different sensors/IoT devices like cameras, metering devices, telematics devices, applications, as well as feeds from sources like enterprise systems, government databases, etc. Integration with Sensors/Sensor Applications- Ability to collect and aggregate data in real-time generated from field sensors/edge infrastructure like bin sensors, water sensors, environment sensors, access sensors and actuator sensors. ETL Capability (Extract, Transform, Load)- Ability of ICCC platform to consume raw data feeds from different data sources and ability to prepare information for downstream use.

		Integration with Video Feeds- Ability to consume video feeds generated from various applications capturing videos like surveillance, parking, traffic etc. Integration with Data Feeds and Publishing Data Feeds- Ability to consume real-time data feeds from various systems/applications using APIs. This includes, for example, data on air and water quality, ambient luminosity, disasters, traffic, solid waste, etc. This enables other functional layers of ICCC to aggregate, process and consume the data for deriving information. Platform should be able to integrate with any type of sensor platform being used for the smart services irrespective of the technology used. Agnostics to sensor technologies such as ZigBee, LoRA, GPRS, Wi-Fi, BLE, Bluetooth, IPv4/IPv6, etc. The Platform should be able to handle high data volume, handle a high events rate (up to ……. events per sec) processing with low latency. Platform should be able to correlate and handle multiple data streams, while providing Realtime logic, analysis and routing applied to incoming data streams and aggregating data over time.
9	Data Normalization	It is envisaged that the city shall implement multiple use cases over a period of time. The potential example of use cases are Smart Traffic, Solid waste Management, Smart Parking, Smart Lighting, Water Metering, CCTV, Public Transport, Public Wi-Fi and other integrations as per defined scope. The platform should be able to normalize the data coming from multiple devices of same type such as Different lighting / environment sensor from different OEMs and provide secure access to the data using APIs. The city shall be using various device/equipment for smart services which may generate data in their own format. The ICCC Platform should be able to define its data model for each smart service like waste, lighting, transport, etc. and map data from different device vendors to the common data model. It should enable define a standard data model for each of the urban services domains (i.e. Parking, lighting, etc.). Data from IoT platforms must be exposed to application eco system using secure APIs.

		Platform should be able to correlate and handle multiple data streams, while providing Realtime logic, analysis and routing applied to incoming data streams and aggregating data over time.
10	Data & Event Correlation	The data correlation and analytics engine analyses information to show trends, patterns and insights, in visualized forms that guide towards prompt decisions. It comprises components for extraction and transformation of data from different systems, data sources and data formats. For e.g., health records are captured from Integrated Hospital Management System, traffic information is captured from Adaptive Traffic Management System and the ambulance can be tracked using Vehicle Tracking System in different formats. ICCC Data Aggregation and Analysis Engine can process the information to allow users to use information from different systems as per requirements. This engine has data aggregation, normalization and data models with the following capabilities: o Collect and integrate sensor/IoT devices and other data from multiple sources o Normalize the aggregated data to a common data model to make comparisons more meaningful so that city administration can construct working digital models of their communities o Expose APIs through which application developers and vendors can plug in to the city management infrastructure and provide public service capabilities. The application developers/vendors can use the platform APIs and build applications on top of platform consuming the data model exposed as part of these APIs. This engine enables ICCC to derive intelligence from the information collected from Data Acquisition and Visualization Engine.
11	Data Management & Analytics	The platform shall be able to predict and integrate with Smart City solutions helping in driving Operational policies creation. Data Analytics components are used to perform data churning to derive intelligence from different datasets across the domain. This intelligence can then be used for exception handling and visualization in different scenarios through various analysis using ICCC components or third-party tools/applications, such as:

		a) Predictive Analytics: Ability to make predictions about future events using historical data. b) Diagnostic Analytics: Ability to do the root cause analysis using data slicing, data aggregation, data mining, data discovery and correlation techniques c) Prescriptive Analytics: Ability to find best course of action for a given variable situation/scenarios d) Sentiment Analytics: Ability to provide sentiment analytics of configured key words/accounts through internet crawling using ICCC platform. Ability to categorize key issues/topics/words in real-time on social e) Video Analytics: Ability to automatically analyze video to detect and determine temporal and spatial events f) Descriptive Analytics: Ability to view insights using past data for given data set.
12	Operations/ Process Control	ICCC platform should be able to aid in improved coordination for different city operations including management & control of multiple stakeholders. For example, in case of hazardous chemical gas leakage situation, metrological dept. along with health dept. can collaborate with ICCC. central helpdesk to extend support to at-risk citizens as well as field staff. ICCC platform should manage the life cycle of incidents and related entities via pre-defined workflows which cut across multiple systems via the interfacing modules. ICCC should be able to provide field force control on real-time to manage civic operations. For example, workflow for operational field alerts and escalations should be triggered without human intervention. Standard Operating Procedures (SOPs) must be adhered to, in case of any incident. ICCC should manage the SoPs lifecycle configured in ICCC platform. ICCC should have provision to provide access or restrict access to user group for any facility or applications in real time. Ability to control the access to field assets through ICCC platform.

13	Communication Capabilities	The Communication Engine shall house the action oriented SOPs, incident response dispatches and management systems (rules engines, diagnostics systems, control systems, messaging system, events handling system), and reporting/dashboard system to provide actionable information to city administrators and citizens. It should be flexible to accept inputs from various downstream applications and sensors as and when they get introduced in the city. It shall be responsible for managing: a) Communication with Stakeholders o Automated messaging to citizens for regular updates through Social Media/WhatsApp/ SMS o Automated Messaging to the all the concerned stakeholders and respective departments with real time update. o Training & Awareness campaigns by authorities involving citizens at large o Use VMDs, PA System to update people and avoid any scenarios of rumors. o Communicate with various NGOs to come and help for any incident (like food donation, volunteering) o Communicate the property details to the departments and to the other emergency services for providing help b) Device Control (asset, access and authorization): ICCC should be able to control devices/sensors access rights or system privileges based on defined SOPs & role-based access mechanism o Remote configuration & control o Event Processing o Device Diagnosis c) User Interface and Visualization o Reports o Dashboard o Scorecard o Simulation d) Complex Real-time Event Handling

		e) Service Management o Control Bus o API Management o Services Management: ICCC platform should have the ability to configure based on configured o SLAs for various services & applications. For e.g. garbage collection SLA, water quality, network operations SLA etc. o Policy Management
14	Business Rule Management	The Business Rules Engine helps correlate the information, configure Standard Operating Procedures (SOPs), manage external and internal triggers, policy implementation, and handling of complex events. This engine enables ICCC to handle the events to make real-time decisions as per the configured protocol. a) Defining and configuring an event b) Defining and configuring external/internal trigger c) Defining and configuring event response d) Defining and configuring responsibility matrix e) Defining and configuring incidents and change requests f) Defining and configuring user access and authorization g) Defining and configuring access policy of field assets The Platform should provide a "standard operating environment" to help in culmination of multiple SOPs. The platform should be integrated with business process monitoring tool. There shall be a provision to define various SOPs such as alert category specific SOPs, Accident specific SOPs, Solid waste specific, Street light specific, water distribution specific, etc. It should have facility to define more than one SOP for the selected alert category/ location. There shall be a provision to define multiple tasks under a single SOP. The platform should be able to select an appropriate SOP automatically based on predefined policies/ workflow.

		Actions taken as part of SOP should be logged in audit trail with date & time stamp and operator comments. There should be no restriction on number of configurable and customizable SoPs through User friendly GUI interface. The users shall be able to edit the SOP such as adding, modifying, or deleting the activities as per assigned role.
15	Situational Awareness	The platform should be able to combine data from various sources and present it as different views tailored to different operator's needs providing Common Operational Picture. It should comprise of a comprehensive view of the incident or a group of related incidents as on a specific date and time which should include but not be limited to the following: o Tasks assignment and their status o Agencies involved o Resources deployed o Incident status across relevant parameters of the incident o Timeline view of the situation o Suggested actions from the system with their status
16	Incident Response	The platform should provide complete view of sensors, applications, systems, video streams and alarms in an easy-to use and intuitive GIS-enabled graphical interface with a powerful workflow and business logic engine. The platform should define and prioritize critical events and trigger necessary actions. There should be defined rules for any given event or events with SLAs. Real time tracking of authorized and unauthorized activities should be available. It should facilitate setting the priority of the event and enable triggering the incidents automatically. It should support for sudden critical events and linkage to standard operating procedures automatically without human intervention. It should support for multiple incidents with both segregated and/or overlapping management and response teams. It should enable associating response procedures to incident types. The associated procedures should be available for selection to operators upon manual incident creation.

		The Incident response system should be optimised to serve emergency response in call taking, incident positioning, incident assessment, response determination, dispatching as well as various other needs of the city services. System should have a strong incident assessment framework including a set of questions and their consequences. These assessments should be defined and maintained by the in the system. The operator should execute the incident assessment by following the questions to gather relevant information about the incident.
17	Emergency Response	The platform should be capable of managing emergencies and SoPs should be triggered automatically (and manually if necessary) as per defined work flow. The platform should have both provisions. The emergency services should be tracked and monitored at various levels. It shall have the capability to create response models defined specifically for specific areas and times. The platform should be able to recognise the similarity of the incidents based on the incident location and task class when the incident that the operator is handling starts to appear similar to an active incident. If the similar incidents are growing in no., operator should be able to alarm an epidemic or disaster. The operator should be able to merge the two or more incidents together. In case there seems to be an epidemic or a disaster, the pre-nominated city official should be immediately alerted, before sounding any epidemic or disaster alarms. The required and protective best practices should be immediately put into action.
18	Root cause Analysis (RCA)	The platform should be able to Isolate and pinpoint the problem area before it impacts the operations & business continuity while suppressing the unwanted events. The platform should be able to track down to the root cause of incidents and provide capacity Analysis to proactively Identify the need for upgradations/ realignment of the city assets and functions. ICCC should have provisions for data analytics and a dashboard to carry out various capacity analysis.
19	Post Incident Requirement	The platform should have an incident recording mechanism that includes all the activities such as voice, Location, alarm triggers etc., including the operator activities for analysis.

		It should have an event reconstruction functionality to give a complete overview of the synchronous events in the timeframe. It should provide a facility to export all the event scenario as a playable media file. It should support sorting and filtering the list of incidents.
20	Dashboard & Reporting	The platform should provide a real-time Dashboard and Reporting services for City operations and administration. The Dashboard & Reports shall support tweaking on-the-fly for situational changes and helping in projecting the realistic data from sources. Platform should have capability to provide access to real time data and historical data from various connected devices for reporting and analytics. Incident Reports (Periodic Reports, Maintenance Reports, Statistical Reports)- It shall include an incident summary, all the tasks associated with the incident, sensor related activities, relevant snapshots, and maps.
21	Export Formats	System shall allow export the analysis into min following formats: XML/JSON Excel, PDF, CSV.

4.3 ICCC Application integration with other city systems

{CITY_NAME} landscape shall have multiple applications (XX+ sub systems) running on variety of platforms. Some of these applications shall publish messages and others shall consume the messages. To establish seamless integration between these applications with ICCC, Authority wishes to have a service based integration layer, built using ESB.

ESB also provides **Business activity monitoring** module for tracking key performance indicators (KPI) in interfaces. These can include performance parameters like completion time and business data which shall be monitored by bidder as part of operational KPIs.

List of systems to be integrated (cities to add/delete/update basis actual technological & functional component):

#	List of Sub-systems	Integration Point	Input Data Format	Dashboard at ICCC
1	Video Management Software	IMS & ICCC	API/ SDK	Yes
2	Video Analytics	VMS & ESB	API/ SDK	Yes
3	Disaster Management System + Incident Management System	ESB	API/ SDK	Yes
4	ANPR/RLVD Software	ICCC	API/ SDK	Yes

5	Facial Recognition Software	VMS	API/ SDK	Yes
6	Enterprise Management Software	ESB	API/ SDK	No
7	Public Address Software	ICCC	API/ SDK	Yes
8	Variable Message Display System	ICCC	API/ SDK	Yes
9	GIS Map data / Engine	ESB	API/ SDK	Yes
10	Wi-Fi Management Software	ESB	API/ SDK	Yes
11	Smart Lighting Software	ESB	API/ SDK	Yes
12	Adaptive Traffic Control System Application	ESB	API/ SDK	Yes
13	VTS, Fleet Management & PIS	ESB	API/ SDK	Yes
14	Solid Waste Management Software	ESB	API/ SDK	Yes
15	Parking Management	ESB	API/ SDK	Yes
16	Environmental Sensor Software	ESB	API/ SDK	Yes
17	2 – way Mobile Application	ICCC	API/ SDK	No
18	Video Wall Application	ICCC	API/ SDK	Yes
19	EPABX	ICCC	API/ SDK	Yes
20	Mobile Van Surveillance	ICCC	API/ SDK	Yes
21	Vending Kiosks/Dedicated Hawker zones	ESB	API/ SDK	Yes
22	Smart Poles	ESB	API/ SDK	Yes
23	24x7 drinking Water supply SCADA	ESB	API/ SDK	Yes
24	Sewerage SCADA	ESB	API/ SDK	Yes
25	Storm water Drainage SCADA	ESB	API/ SDK	Yes
26	Smart Metering	ESB	API/ SDK	Yes
27	Solar Roof Top	ESB	API/ SDK	Yes
28	Public Bike Sharing	ESB	API/ SDK	Yes
29	E-RICKSHAW	ESB	API/ SDK	Yes

30	Public Toilets + Community Toilets	ESB	API/ SDK	Yes
31	Social Media Integration	ESB	API/ SDK	Yes
32	VAHAN	ICCC	API/ SDK	Yes
33	SARATHI	ICCC	API/ SDK	Yes
34	e-Challan Integration	ICCC	API/ SDK	Yes
35	DIAL 100	ICCC	API/ SDK	Yes
36	e-Governance Portal	ESB	API/ SDK	Yes
37	Enterprise Service Bus	ICCC	API/ SDK	Yes

Below is the current list of projects that shall be integrated to ICCC:

[Authority to add/delete/update basis actual technological & functional component]

#	List of projects for ICCC Integrations
1	Integration with Disaster Management System
2	Integration with Smart Governance Portal
3	Integration with Smart Sensors (Environmental Sensors)
4	Integration with Traffic Management
5	Integration with CCTV Surveillance
6	Integration with Smart Poles
7	Integration with ICT based SWM
8	Integration with Smart GPS based Buses and Bus stops
9	Integration with 24x7 drinking Water supply
10	Integration with Sewerage
11	Integration with Storm Water Drainage
12	Integration with Smart Metering
13	Integration with Public Bike Sharing
14	Integration with Transportation (Smart Bus Stops cluster with amenities)
15	Integration with MLCP + Retail outlet
16	Integration with E-RICKSHAW
17	Integration with Vending Kiosks/ Dedicated Hawker zones
18	Integration with Public Toilets + Community Toilets

19	Social Media Integration
20	Dial 100 /112 Integration
21	Integration with CCTNS
22	Integration with VAHAN
23	Integration with SARATHI
24	e-Challan Integration
25	Integration with Smart Street Light System
26	Integration with Existing Live Services**

4.4 Infrastructure Management System (IMS)

The Authority has planned to implement an integrated city operation management tool, which should be able to manage both IT and NON-IT infrastructure. The tool should be able to manage both IT/Telecom Network (including bandwidth usage) as well as electrical power network i

The system should provide functionality for Fault Management, Performance Management, Configuration Management, fault ticketing, asset management, Incident/ Problem, SLA management, Change Management etc.

The System should have the capability to nomenclate all installed equipments/software/etc., including field level equipments.

The end equipment outages should be constantly monitored and required dispatches should get alerts and timelines to fix/repair/replace the end equipment and report back. The NTP (Network time protocol) clock should be synchronized.

4.5 Helpdesk-cum-Support Centre

Authority plans to set up a Helpdesk-cum-Support Centre, with provision of appropriate manpower to coordinate and manage city operations, complaint redressal etc. This Helpdesk will be central to the administration for different departments of the authority, so that citizens reaching out to the individual department's websites/ mobile apps will be directed to this central helpdesk for further help.

The objective is to bring citizens closer to the authority and help them support/ solve their issues in a timely fashion. This will aid in providing most of the citizen services via digital means, for efficient and effective service delivery to citizens.

The Citizen Help Desk & Support center should have following indicative functionalities:

- An Integrated Helpdesk-cum-Support Centre, to enable citizens to communicate with the Authority via multiple communication channels. The common communication channels must include voice, video, email, SMS, chat and social media interfaces.
- The request should be categorized in various types like Grievance, Information, Feedback survey, follow-up, etc.

- To reduce citizen's efforts by automating important regular tasks via digitization so that people do not have to travel physically for basic information and other related work.
- Availability of common services including basic queries, form submission, complaint registration etc. to the citizens via IVR (Voice & Mobile) and/or Chatbot.
- Recording of the communication between Citizen and Authorities
- Survey and emergency notification solutions to measure citizen's happiness.
- Log and track all service/compliant tickets raised either by voice call, email, SMS, web requests through portal, in-person requests, etc.
- The ICCC operator shall have the ability to contact the backend Field Response team over Voice, Email and Chat.
- It should have the ability to bring multiple stake holders on to a common voice conference call as a standard operating procedure in response to event
- It should be integrated with Citizen Mobile App through which the citizen can make request for various city services. The APIs must be available for carrying out this integration
- The Citizen Mobile app should have an integrated functionality to initiate chat and email.
- The Citizen should have ability to share the live video of an incident with the ICCC Operator

Detailed operational guideline documents shall be prepared by MSI during the design & implementation phase which shall specify detailed responsibilities of the deployed manpower resources, their SOPs and do's & don'ts.

4.6 City Mobile App

The MSI shall develop a city mobile app envisaged as a single unified digital platform between the Government and citizens for any kind of citizen related service, notification and collaboration to:

- Improve delivery of services to citizens, businesses and employees
- Engage citizens in the process of governance through interaction
- Empower citizens through access to knowledge and information
- Make the working of the government more efficient and effective

The **city Mobile app** is thus set to achieve the purpose of truly empowering the Citizens with a 'One Stop Solution' as well as to ensure maximum citizen engagement and transparency in the activities of the Authority and the local government bodies.

The City App shall meet the following objectives:

1. To provide a Grievance Redressal (GR) tool where public grievances can be filed through any mode – electronic or manual; the tool should enable resolution of the pain points and problems in efficient and time-bound manner.
2. To enable seamless delivery of identified 'citizen-centric services' on the envisaged platform for the citizens.

3. To seek and take opinions from citizens through feedbacks, polls, surveys, questionnaires etc. about policy matters and any other governmental topics of high interest and benefit to people.
4. To provide a 'Discussion Forum/Platform' for citizens to provide voluntary self-initiated opinions and feedback on topics that interest the community as a whole.

Integration of citizen services

The envisaged platform will serve as an aggregator platform which should integrate with various types of citizen centric services available in the city like G2C, B2C, emergency services as identified by the department along with necessary payment gateways, identity authentication through Aadhar. The number and name of the services to be integrated will be finalized by the Authority.

Indicative List of Services

Department	Services
Municipal Services /Urban Development department	• Property Registration • Land Survey / Property Survey • Encumbrance Certificate / Certified Copies • Birth, marriage, death Registration and issuance of certificate • Building permission • Application and renewal for various licenses, including trade, building, labour, food, health, etc. • Khata Registration / Khata Bifurcation / Khata Transfer • Property Tax Payment • Application of RTI • Skill development trainings • Higher education and vocational training facilities' information • Hospitals & Clinics Search • Information on vaccination for epidemic diseases • Information on benefits entitlement in terms of subsidies for citizens • Details of govt. trusts and funds, allowances for disabilities, backward castes etc. • Dynamic city dashboard • Smart parking information; informing citizens of parking area availability ward-wise on a real-time basis

	• Information on Wi-Fi hotspot locations across the city • Application for market stalls, generation of online certificate • [add/modify]
Water supply and sewerage Department	• Request for new connection • Payment of bills • Name / Ownership transfer
PWD, Education, Planning, SWM, Revenue & Land Records, Health and Family Welfare, Transport Departments (Add /modify)	• Repairing of Potholes on Road / open drains etc. • Traffic Challan Payment • Towed Vehicle search • Public Bike Sharing • Vehicle Search • Bus Routes / Timetable • Metro Rail Routes / Timetable • Rail / Flight / Taxi Details • Ambulance / Fire Ambulance Services • Nearest Public Toilets / Request for cleaning the toilets • Request for picking garbage • Services for removal and adoption of stray animals • Location/Map services of all the buildings and structures in the city E.g. heritage buildings, schools, administrative buildings, public service offices, wards, Citizen Facilitation Centres etc.
Electrical Department	• Request for power connection • Payment of bills • Name /ownership transfer • New User Registration
Urban Development Authority	• [add/modify]
Miscellaneous	• Any new startup/initiative services like Kabadiwala, Books Donation/Library etc. • Contact Administration • Emergency / SOS / Report Accident Services • Contact details of nearest Police Stations / Fire Stations etc. • Alternate route plans, in case of natural disasters • Heat maps of all disaster-prone/ disaster affected areas

	• Weather forecast of the city • [add/modify]

5. Data Management

5.1 Data Management

Data is a valuable asset in any smart city. Data in a city is generated in a variety of applications, operating across a host of departments and organizations working towards a common goal of building and running city infrastructure to better serve the citizens. However, this multiplicity of data owners often causes problems related to accuracy, consistency, and accessibility of right data at the right time. There is a need to bring together a large amount of data in cities, including energy, transport, ERP, water, crowdsourced data, etc., and provide a holistic view of the information with the aim of improvement and development of innovative smart city services across following data streams.

- **Demand-side stream** which can give better understanding of specific properties and characteristics of urban processes, e.g., buildings services, government-to-citizens services, and provide solutions for improvement.
- **Supply-side stream** to monitor incidents and crisis situations and the respective responses and solutions with the aim of drawing conclusions and recommendations.
- **Analytical stream** to identify data patterns and correlations in order to derive predictions for urban innovation, provide impact assessment, and demonstrate the challenges and opportunities in urban development.
- **Standardization stream** to bring the city data in line with the national and international standards like IS 18002:2021, ISO 8000 etc.

Most of the cities are unable to utilize the data captured from deployed sensors & enterprise systems to generate actionable insights due to data silos, data quality and data interpretability issues. While IoT deployments are enabling cities to capture relevant data about the cities, environment and citizens, it is not enough to think of smart cities as an IoT only solution.

To overcome these issues, Authority intends to have robust Data Management capabilities that puts in place a mechanism to not only share the data amongst different departments but also a set of tools and technology to better use this data for decision making. Integrated data plays a vital role in understanding the problem in the right context and providing a solution which is in the interest of administration as well as citizens.

All data generated through this project, shall belong to Authority and should adhere to following data principles to ensure its usability and usage on a longer run. The bidder shall include and implement these as part of Data Architecture for all city data under scope:

ID	Data Principle	Description
P1	Accuracy	City Data stored shall be as correct as possible for an object, whereby the object must have the right values and must be represented in a consistent and unambiguous form in alignment with known frameworks such as OWL and RDF when possible and appropriate.

P2	Completeness	City data shall reflect what is recorded based on a standard schema that defines completeness. Metadata that defines and explains the raw data should be included with explanations and formulas for how data was derived and calculated.
P3	Timeliness	City data shall be available in a timely fashion. They shall be made available as quickly as they are collected and processed, based on data priority defined according to the time sensitiveness of utility and value.
P4	Privacy	Except Open data, direct access to all other data shall be prohibited.
P5	Confidentiality	Data should be disseminated data only to authenticated and authorised stakeholders (both internal and external) through applicable data fiduciaries. Use of APIs to be mandated where data access is permitted.
P6	Machine Readable	City data should be stored in widely used file formats that easily support machine readability, interpretation and processing. Files should be accompanied by documentation related to the format and how to use it in relation to the data.
P7	Non-Redundancy	City data should be acquired, stored in a timely manner, and made available for multiple / generic purpose reuse to avoid data duplication, and promote data consistency and quality.
P8	Permanence	City data released for online consumption should be available in archives and in perpetuity as defined in the policy for the type of data. Deletion of city data should be as per city data policy.
P9	Consistency	City data should be consistent across different systems. Data written to the storage must be valid according to all defined rules, including constraints, cascades, triggers, and any combination thereof. When data is aggregated from multiple sources there shall be consistency in measurement of variables throughout the datasets.
P10	Non Repudiation	Data shall include source information like the owner, device which generated the data and also store the hash values of computed on the original data to cater to non-repudiation.

Following additional principles need to be applied only to Open data in the city:

ID	Data Principle	Description
OP1	Non-Discriminatory	Access to Smart City Open data by the public should not contain any barriers to use. Any person should be able to access open data published at any time without having to identify him/herself or provide justification for gaining access.
OP2	Non-Proprietary	Smart city open data should provide for freely available alternative formats to allow the public to avoid costs for consuming data in specific formats. Removing this cost makes data available to a wider pool of potential users.

5.2 Functional capabilities

The city intends to implement a robust Data Management framework that puts in place a mechanism to not only share the data amongst different departments but also a set of tools and technology to better use this data for decision making.

This section describes the Data Management capabilities of the Data that Authority needs to implement using appropriate tools and solutions by the bidder to ensure compliance of Smart City data to principles defined in Sec 7.1 as well as to ensure data is useful for usage on a longer run.

Data Governance: Bidders shall ensure that Authority data policies and standards are adhered to as needed to account for {CITY_NAME}, including but not limited to:

- **Data privacy policy:** describing the Authority's obligations towards the privacy rights of its service users
- **Data retention / archival policy:** describing how long data should be kept and the conditions for data archival or retirement
- **Open data policy:** describing when and how the agency should publish its data for public use
- **Data classification standards:** describing the criteria for categorizing data into different access levels depending on need-to-know basis and the risks associated with getting the data into the wrong hands
- **Domain-specific data standards:** describing domain-specific controls for collecting, organizing and managing data

Data Architecture: Data architecture pertains to Processes, systems and setup required to store, access, move and organize data. The data architecture helps define the steps to collect, integrate, enhance, store, and deliver data to decision makers (Authority CEO, Municipal commissioner, department heads, etc.). Other than data principles listed in table on sec 5.1, Bidder needs to identify the data needs of the city (regardless of the structure), and design and maintain the master blueprints to guide data integration, control data assets, and align data investments with business strategy. Data architecture should capture the following at minimum:

- Data movement and transformation automation through data driven workflows.
- Facilitation and optimization for future Big Data architecture decision making.
- Creation of Data Models that capture business requirements and present them in a structured way.

Data architecture should be effectively designed (e.g. ingestion, data storage, cleansing) to handle the variety, volumes and velocity of big data, allowing it to be easily understood and retrieved by different users.

- Data management capabilities should be designed to manage structured and unstructured datasets.
- Distributed database file system technologies (DDFS) to host and manage the information coming from large volumes of unstructured data.

- Big data streaming technologies to handle high frequency of incoming data that needs to be collected, aggregated, and processed in batch and real-time.
- Common data models that would be deployed to prevent unnecessary data transformation and overcome application semantic differences. As such, data exchanges would use the schemas that codify canonical data models.

Data quality: Data quality is the ability of data to satisfy the stated business, system, and technical requirements of the Smart city. Bidder needs to implement the following functionalities:

- Data Cleansing: Maintenance of data to fit defined Smart City Data Standard for enhanced interoperability and decision making.
- Data Profiling: Systematic analysis of data to gather actionable and measurable information about its quality.
- Data Traceability: Tracking of the lifecycle of data to determine and demonstrate all changes and access to the data.
- Data Compliance: Ongoing processes to ensure adherence of data to both enterprise business rules, and, especially, to legal and regulatory requirements.
- Data Monitoring: Routine checking and validation of data against quality control rules to ensure quality and format consistency.

Master Data management: Bidder needs to create a centralized database of data entities used by multiple application across a city. Examples of master data in a city could be addresses (property, buildings, road names, locality names, etc.), Assets (Fixed asset like real estate, plant & machinery or movable asset like vehicles), Citizens (or customers), and many more.

Metadata Management: Bidder needs to enable metadata management for all city data under scope. Metadata describes what each data element recorded means and this meaning remains consistent across applications. Metadata can be categorized as technical metadata or business/operational metadata.

Data Processing: This pertains to ingestion of IoT or other data sources in real-time or batches. Batching can be done to ingest data through execution of a series of programs without manual intervention on a scheduled basis. Streaming is presentation of ingested data that is being received continuously to analytics engines and dashboards. This gives real time view of all city assets to the various stakeholders. The data processing shall, at minimum, be capable of the following:

- Data Ingestion:
    - Filter, aggregate, summarize and / or transform data from structured sources
    - Enable scalable storage
    - Integrate Master and Reference Data
    - Handle historical data in bulk
    - Handle incremental data, e.g. data synchronization
    - Apply soft and or hard deletions of data

- Auditing:
    - Track historical changes of data
    - Enable logging of services, users and requests for data
- Ontology (semantics) definition:
    - Create data schemas/ catalogues that are understandable by both humans and machines
    - Capturing and storing data about data or Metadata
    - Creation of data models
    - Allow for easy search of data schemas based on keywords, tags and various contextual information

Data Transformation: Bidder needs to enable Data transformation which includes a certain set of activities like conversion of data from one format to another, enrich data by merging data from multiple sources, perform aggregation function i.e., create summary of data (example could be creating a total revenue earned from a citizen across multiple services offered by city), or cleanse data of null values.

Data warehouse: Data warehouse capability pertains to Storage and consolidation of data from multiple sources in a relational store for querying. A data warehouse is different from database in a lot of ways including how it stores the data, the purpose of the stored data, the duration of the data stored, as well as the format in which the data is stored**.** Bidder also needs to closely govern the creation, storage, maintenance and usage of Smart City data by ensuring, at minimum, the following data principles listed above in sec 7.1 are adhered to across agencies for storage and retention:

- Creation:
    - Datasets are available when needed.
    - Datasets used are understandable and clear.
    - Datasets are accessible to all members of the intended audience to conduct day to day business activities.
    - Datasets created are trusted, accurate and as complete as possible
- Storage & Retention:
    - Data stored is stored securely
    - Data and document retention shall be retained as long as agencies deem their current usefulness and historical relevance
    - Data shall be maintained in current storage per their economic useful life
    - Data retention must satisfy any current data retention policy
- Usage and Maintenance:
    - Usage of data stored and retrieved should be consistent for the purpose for which the data is intended

- Data retrieval requests and fulfillment should be reviewed and monitored for adherence to current security policies and standards.

- Retirement:
    - All data nearing end-of-life shall be first retired to a secure offline or near-line storage repository for cleansing
    - Disassociate metadata from the data to remove identification
    - Set up a plan to temporarily remove data for retirement to test impact

Data Integration & interoperability: Data Integration and interoperability are both enablers of data exchange between two or more systems. Bidder needs to implement a middleware that translates the data from one system into something that the other system can understand to achieve the following objectives:

- Translation of internal service and data formats for external platform compatibility and consumption.
- Translation of internal protocols for external platform compatibility and consumption (e.g. SOAP to REST).

Data Exchange: Bidder needs to enable Data Exchange which pertains to sharing ingested and analyzed City data via Open Data sets, Data APIs, Dashboards, as well as Sandbox for working on open data sets with various stakeholders based on city data policy.

- Open Data Management: Management and accessibility of open datasets in useable formats and enablement of query generation on these datasets.
- Data Visualization: Manipulation and placement of data in a visual context such as infographics, dials and gauges, geographic maps and charts.
- Dashboarding: Integration of information from multiple components into a unified display to facilitate development.
- Data Sandbox Environment: Isolation of computing environment in which a program or file can be executed without affecting the production environment of the services.

MoHUA has setup up the India Urban data exchange platform (IUDX), to allow various data providers and consumers to share and consume structured and unstructured data streams/sets. This platform shall facilitate managing the data streams/sets covering following aspects:

a) Metered Control Access of Data through Subscription

b) Authentication and Authorization of Consumers

c) Data economy

d) Ensuring Privacy and Security Aspects

e) Integration with various platforms using standard APIs like REST

f) Designing demand and consumption insights through platform

g) Ensuring Data Validity and Feedback

Smart City Open Data should be shareable with Data Exchange Platform via integration using Web Services (SOAP or RESTful Service).

Data Protection: Data protection is applicable throughout the "collection to retention" lifecycle of the data in a city. While implementing data protection, the city must keep in mind that they should be fair in data collection, use the data for specific purpose only and collect only the information needed for that purpose, keep the data accurate and only for as long as it is needed. Bidder should ensure that data is safe and secure at all times.

Following capabilities need to be developed on a longer run and have to be kept in mind by the bidder:

Analytical Modeling: Bidder needs to enable Analytical model creation and cognitive computing capabilities for data insights generation.

- Model Building: Analysis and generation of mathematical representations of the system and its services, including the statistical models used to understand behaviors and patterns.
- Model Deployment: Deployment of models in an automated fashion, without the need of a human intervention in moving code or operate the target machine where the code shall run.
- Model Validation: Use of various measures of statistical validity to determine data or model problems.
- Big Data Algorithms: Design and development of algorithms to access large amounts of data from large data storage through queries, and derive streaming and real-time analysis from them.
- Machine Learning: Automatic development of models based on training data as well as back-propagation, or feedback loops enabling the ability to test and retrain the model while processing production data.
- Statistical Learning: Prediction of business metrics and variables for the future based on historic data.

Data discovery & mining: Bidder needs to enable Data synthesis and visualization methods in preparation of advanced data modelling activities.

- Analysis of data sets through visual and graphical methods to summarize their main characteristics.
- Development and management of workflows to conduct analytics on data.
- Registry of information for reusable components of many types, which are used to build, document and test data mining tools

5.3 Indicative KPIs

The performance of the data management in the city is dependent on a number of factors including its adoption by users of the department and how well it is implemented. There are a number of metrics that can be used to measure the performance and adoption of a data management capabilities such as:

- **Data quality:** Cities can measure the improvement in data quality by monitoring KPIs such as ratio of data to error, number/percentage of empty values in the dataset, etc.
- **Data Governance:** Some of the Indicative KPIs that can be monitored to evaluate the success of data governance implementation in the city are:
    - Percentage / Number of departments where data principles are adhered
    - Percentage / Number of information systems data elements that share a data functionality
    - Percentage / Number of business processes that utilize data principles
    - Percentage / Number of production reports (outputs) that utilize data principles
    - Percentage / Number of people that use data elements
    - Percentage / Number of integrated business processes
    - Number of Data Governance Policies Established
- Functional KPIs to be monitored - Data Management capabilities shall be empowered by implementation of the domain use cases listed in section 12: Domain Use Cases of this document.

While the above listed metrics are indicative only, Authority may decide to form a committee to monitor the progress and performance of the data management platform. Authority may also decide to carry out performance benchmarking exercises with the help of an external agency and it would be expected that the MSI shall tune the system to ensure those benchmarks are adhered to.

6. Geographical Information System

6.1 Geographical information System Overview

GIS is the foundation Layer of a smart city. The MSI shall implement an Enterprise-wide GIS for the planning, development and management of the city for sustainable growth. GIS shall provide location-based Intelligence as a part of Data-Smart cities strategy of MoHUA, to collaborate and share the information with city stakeholders.

6.2 Functional Requirements

Functionally, the enterprise GIS system should provide the following capabilities at a minimum:

a) Base Maps: Common set of Base Maps, over which the city functions can collaborate for a spatial decision support system. The Base Maps can be topographical, satellite image, street maps etc. on which different layers of information can be geo-referenced, like property, land use, water supply etc.

b) Data ingestion from different sources: Government Data bases, Enterprise systems, sensors, e-Governance applications, Survey Tools like GPS, Drones, GPR, LIDAR, Rest APIs etc.

c) Analysis: It shall facilitate a different type of trend and pattern base analysis, generating hotspots, concentration and dispersion patterns, interpolations, statistical models, based on what-if modelling and predictive modelling may be undertaken

d) Workflows: Location based workflows to generate alerts with locational intelligence and dashboards for status monitoring. The Enterprise GIS shall allow to create dynamic dashboards for monitoring and evaluation, Enterprise GIS shall enable user specific Web Apps and Maps

e) Visualization & Dashboards: Creation of workflow enabled/dynamic dashboards for monitoring, tracking and performance analysis of different smart city segments against thresholds/benchmarks. Enterprise GIS shall facilitate visualization of assets above the ground, below the ground, patterns in 2D and 3D along with Panoramic images.

MSI needs to ensure that enterprise GIS application that is implemented has base capabilities listed in Table 2 Functional capabilities of Enterprise GIS for Smart Cities of IS 18008.

MSI shall also undertake detailed assessment for integration of all smart city components under the scope of this project with GIS.

i. Bidders are required to carry out the seamless integration to ensure ease of use of GIS in the Dashboards in ICCC.

ii. If such data is already available with the city, it shall facilitate the same.

iii. Bidder is to check the availability of such data and its suitability for the project.

iv. MSI is required to update GIS maps from time to time.

6.3 Scope of Activities

6.3.1 As-IS Study

Bidder shall conduct a **"detailed "As-Is-Study"** of the existing maps and data available in the city in different formats (Paper Maps, CAD Maps, Satellite Images, KML Files and Digitized Maps etc.) The bidders need to assess the requirement of spatial data and provide the "Should-Be" study defining the data gaps, survey requirements and data models for the smart city, along with the workflows and the spatial decision support system.

6.3.2 Base Map Creation

Bidder shall create a base map of the city (if not already available) which shall be common across all the services like city surveillance, smart lighting, smart traffic, smart parking, solid waste management, city bus transport etc. The Base Map of the city is to be prepared at the scale of 1:4000 (Mentioned in AMRUT Guidelines) with Datum: WGS84 and Projection: UTM. For geo-referencing the base maps, there shall be 1 GCP per 5 Sq. Kms. The satellite image used for the preparation of the base map shall have a resolution of 0.5 meter (minimum) with PAN sharpened Natural Color Composite (NCC). All the layers shall be captured as Shapefiles (.shp) for easy integration. The layers of Base Map shall be following:

Base layers	Identified Sources
Administrative Boundary	District
Municipal boundary	ULBs
Zone Boundary	ULBs
Ward- Boundary	ULBs
Streams, Creek and Water Bodies	Satellite Images
○ Natural Land Use ○ Agriculture ○ Wasteland or Barren Lands ○ Forested land	Satellite Images
Roads: National; State; Expressways, City/Municipal/ (line features)	Satellite Images
Railway (line features)	Satellite Image
Airport (Polygon features)	Satellite Image

Built-up areas (polygon feature)	Satellite Images
Other landmarks such as Religious Places, Important Features like Monuments, etc. (Polygon or Point)	Satellite Images and GPS points collected

6.3.3 Survey based on data gaps from AS-IS study

The bidder is responsible for undertaking the Survey based on the data gaps identified through "As-Is" as per the objectives of the city. The bidder shall also be responsible for ensuring appropriate geo referencing & geo tagging of all the Smart City Components/Assets on the map including Wi-Fi locations, bus stops, bus routes, bin locations, transfer stations, street poles, high masts, traffic signals, PA & VMD systems etc.

6.3.4 Create City GIS Layers & GIS Data Models

The City GIS layers have to be created from different sources in Shape files, .Shp Format, with standards mentioned for the base maps.

The suggestive GIS layers shall involve the following:

i. **Administrative Boundaries:**
    a. Planning area boundary
    b. Health District
    c. Police Beat Boundary
    d. Utility Zones

ii. **Urban Development Plans:**
    a. Master Plan/Zonal Plans or City Development Plans
    b. Infrastructure Plans
    c. Transport Plans

iii. **Property Layer:**

    (If the City intends to integrate the property GIS data from e-Governance). If the GIS data is already available for property, then it can be integrated in the portal:

    a. Building footprint
    b. Property

iv. **Road Layer:**

    The road layer shall be updated using the high-resolution satellite images and other sources. The road details may be added like:

    a. Hierarchy of Urban Road: Arterial and Sub Arterial roads

b. Road Centre Line

c. Road Infrastructure: Bridge, Subway, Underpass, Flyover

d. Right of Way

e. Footpaths

f. Electric poles

g. Markings of infrastructure of utilities

h. Junctions

i. Signals

v. Urban Infrastructure & Utilities

The utility Map is not envisaged to be created under Smart City, however if there is existing Electricity, Telephone, Water supply, Sewage and Drainage Network Maps, it shall be integrated.

a. **Water Supply Network-** Lateral Lines, Distribution Lines, Valves, Pump, OHT, Underground, Joints and Fittings, Underground Reservoirs, Flow Meter, SCADA, Pressure meter

b. **Sewerage Network** - Lateral Lines, Distribution Lines, Manholes, STPs, Pumping Station

c. **Telephone- Network**, Fitments, manhole

d. Electric poles, Electric line, Substations, Transformers

e. Fire hydrant points.

vi. Points of Interest data to include:

a. **Health services** (Hospitals, Blood Banks, and Diagnostics center, Ambulance Services, Other Medical Services, etc.)

b. **Community services** (fire stations, police stations, banks, ATMs, post offices, educational facilities, Govt. Buildings etc.)

c. **Business Centers** (shopping malls, markets, commercial complexes etc.)

d. **Transportation Nodes** (bus stops/Terminus, parking areas, Fuel Stations)

e. **City level Local landmarks** with locally called names.

vii. Smart City components:

a. Intelligent Traffic Signals/Blinkers

b. Surveillance System (Fixed and PTZ Cameras)

c. ANPR Cameras

d. Red Light Violation Detection System at Intersection

e. Variable Message Display (VMD) Boards

f. Passenger Information System (PIS) for Bus Shelters

g. Surveillance System & Passenger Information System (PIS) for Bus Terminals

h. Smart Parking System

i. Environmental Sensors

j. RFID Tags for Bulk Generators

k. Surveillance System for Secondary Collection Centers, SWM Plant Vulnerable Garbage Points

l. Smart Street Lights

m. Wi-Fi Locations

n. Emergency Call boxes

o. Smart Schools

p. Smart Health Centers

q. Add/Modify

The MSI shall build Spatial Data Models, which provide guidelines regarding what Data needs to be gathered for city management. The Data Model shall be rule based with defined Cartography, Relationship, Schemas and Taxonomies. Sample City Data models should be referred from section 5.6 of IS 18008 (Part 1). Version management shall be there in data model for regular GIS update and archiving old data. The data model shall have validation rules with domains and subtypes, design workflows and map properties, label and annotations classes, dataset design and tools for enterprise-wide base map creation & updating.

The MSI shall regularly update and manage existing base map features until the agreement period. The MSI is responsible for studying the existing applications in the city and the requirements for integration with GIS to generate department specific workflows and applications.

6.3.5 Implement GIS System

The MSI shall implement GIS system involving:

- Creation of GIS portal- Citizen's Portal with Functionalities
    - The City GIS layers
    - Proximity analysis
    - Routing to specific location
    - Location based grievance reporting
    - Events notification
    - Sharing Geolocation on social media
    - Crowdsourcing Apps for Citizen's Feedback
    - Query Functions

- Geospatial Analysis of different type like buffering, aggregate points, summarize points, calculate density, Hotspots generation, Find Outliers, Cluster points, etc.

- Creation of Enterprise-wide GIS portal for use by stakeholders
  - Access through user management
  - Generating Department specific queries and spatial reports
  - Generating Department Specific workflow based Dashboards for monitoring the smart city parameters against benchmarks
  - Generating Department specific web and Mobile GIS Apps
  - Generating integrated spatial workflows.

6.3.6 IoT and ICCC Integration

- **Geotagging of IoT Assets:** Mapping of all the IoT assets over GIS platform's base map using Geotagged location of the sensors and devices – Smart Poles, Environment sensors, PTZ cameras, Bin Sensors, Public Announcement Systems (PAS), junction boxes, Emergency systems etc.
- **Using buffer tools** to mark the area of coverage, for devices like PTZ Camera, ANPR camera, it shall analyze the total coverage of the devices for optimum locations.
- **Integration of the IoT data with GIS:** The sensors/devices connectivity to the cloud through a variety of methods including: cellular, satellite, WiFi, Bluetooth, low-power wide-area networks (LPWAN), or connecting directly to the internet via ethernet.
- **The GIS complements IoT platforms**: The IoT platform integration with GIS to expand its capabilities with spatiotemporal analytics, visualization and dashboards.
  - Ingestion from Edge of the IoT device into IoT platform which integrates with GIS Platform
  - Stream Analytics
  - Actions (including Actuation): when threshold is reached or in terms of events.
    - Data Store
    - Device Management
    - Batch Analytics
    - Management Console
    - Visualization
    - Dashboards
- ICCC integration with GIS for operational locational intelligence and generate spatial analysis like hot spots, integrated workflows for geo event generation, Proximity analysis for location of nearby supports of maintenance or operations management

6.3.7 Create City Data Hub (optional)

Creation of City data hub to enable the users working on open GIS data and APIs to support creating Maps and Apps. These Hubs are intended to provide open GIS data to be utilized by different stakeholders and shall have following capabilities:

- Maps and Apps to make it easier for Authority to visualize the data
    - Informative Charts
    - Interactive maps
    - Narrative Story Maps (for publishing Smart City Policies and stories)
    - Dashboards
    - Data driven microsites
- Collaboration place: Engagement Platform to connect with trusted members of community
    - Government
    - Local Business
    - NGOs
    - Academia and research
    - Citizens
- Capture Data and Input from Various sources: Enlist the City data Hub participants for community engagement and the data required in a useful digital format
    - Urban Problems and Initiatives-related
    - Surveys
    - Development Proposals
    - Events and Meetups
- Tools for Innovation: make it easy for others to find and use the community's data
    - Civic Developers
    - Volunteers
    - Students
    - Open Source Community
- Creation of Sector Specific Geo-Data Model
    - Integration of GIS with other applications in the municipality for the Spatial Decision Support System

6.4 Bill of Material

MSI shall submit various components of GIS covering the following, but not limited to:

- Concurrency of users at any one time to be clearly mentioned
- Defining Bill of quantities with respect to various steps required for Geospatial enablement of the city
    - GIS Hardware Infrastructure
        i. Web Servers
        ii. Application server
        iii. Database server
        iv. GIS Software
        v. Desktop software for data creation and administration
        vi. Web GIS server Software
    - Survey (if required)
        i. Field survey
        ii. Lidar/UAV survey
        iii. GPR Survey
        iv. Secondary data collection
    - Services
        v. GIS Application development and integration
        vi. Data Migration and conversion
        vii. Capacity building and training

7. IoT platform

7.1 Overview

The authority plans to have large number of IoT field devices installed in a geographically widespread area across the city. IoT (Internet of Things) field devices range from sensors (environmental, cameras, pressure, wind, rain, water flow, microphones, touch screens etc.) to actuators (valves, pumps, switches, streetlights, displays, speakers etc.). These shall come in a variety of forms (smartphones, feature phones, IoT devices, etc.).

Managing such a large no. of devices requires a standards compliant and robust management framework. To enable the cities carry out management of such a large no. of IoT devices, MSI shall propose and implement a standards compliant IoT Management framework. For more information on the standards to be complied with,

Please refer Annexure-xxxx for BIS standards for IoT System Reference Architecture- IS 18004.

7.2 Functional Capabilities

The proposed solution for the IoT Management platform/ framework shall have the following minimum functionalities, but not limited to:

- Remote device configuration
- Device Authentication and Authorization
- Device Key Management
- Device Monitoring
- Remote diagnosis
- Secure firmware updates/upgrades
- Multi-tenant operations dashboards.
- Ability to take actions on configurable conditions, which are guided through workflows
- Ability to send alert on any incidents in the network proactively
- Perform analytics, predictions across city-wide operations

Device Onboarding and Provisioning

The IoT platform shall provide:

- Organization & vendor management – authority, MSI, OEM, Service providers, Contractors etc.
- Device ownership management
- Device registration
- Device Inventory Management
    - Device usage lifecycle from entry to exit
    - Device inward and outward

- Device inventory register

Device Connectivity

The IoT platform shall provide connectivity to following last mile scenarios:

- Device to platform
- Device to gateway to platform
- Device to gateway to server/cloud to platform

The platform shall support all prevalent IoT & Industrial IoT communication protocols including:

- MQTT
- AMQP
- CoAP
- OPC
- BACnet
- Modbus
- Any other applicable standard protocols

Device Scalability

The platform shall provide systematic capabilities to scale the deployed IoT devices with ease using containerization technology.

The platform shall provide ETL and ELT data pipelines capability that can be dynamically scaled horizontally to manage big data throughput coming from multiple devices without latency and data loss.

Device Monitoring and Control

The platform shall provide abilities to:

- Group devices by domain, OEM, device type, connectivity
- Manage device connection quality and service status
- The platform shall provide ability to do device firmware updates over the air with following functions
    - Support OTA updates for all types of device last mile connectivity i.e. LoRaWAN, Zigbee, GSM, Wi-Fi, Bluetooth
    - Manage formation of multicast groups based on device types, vendors/OEM etc. for deployment
    - Manage device downtime for deployment
    - Manage firmware patches for all device types
    - Automatic fragmentation of firmware patches as per data rate of the last mile connectivity and assure updates are successful without data loss.

- Conduct device checks and repeat firmware updates in the event of any failures

MSI shall comply with techno-functional specifications as mentioned in section 8.11 of IS18000 and IS 18004 IoT Reference Architecture.

8. DC-DR/ Cloud Infrastructure

8.1 Overview

The DC-DR/ Cloud Infrastructure/ services are planned by the Authority and shall support multiple stakeholders in their effort to deliver various urban services for meeting citizens' requirements.

Whether Authority chooses the Cloud or On-Premises model, the Smart City ICT infrastructure shall meet certain key functional requirements and it should cover at the minimum, but not limited to, the following infrastructure components:

- Compute Infrastructure
- Data Storage Infrastructure
- Data Networking
- Security
- Smart city applications

The bidder is expected to propose the solution that meets following minimum requirements.

[Below provided functional requirements are indicative and Authority may add/modify further as per requirements]

8.2 Functional Requirements

The Authority has identified Data Center, near line Data Center and Disaster Recovery Center as one of the important core IT components for efficient delivery for the citizen services.

The Authority has considered [Cloud based/On-Premises/Hybrid model] to meet city requirements.] While subscribing to Cloud to suite the functional, scalability and performance requirements, Various prevalent deployment models (IaaS, PaaS, SaaS) may be adopted to design and deploy the use cases.

[These different cloud models may be used in combination in a manner that is similar to that used in a traditional IT environment, with underlying infrastructure supporting platforms and services.

- IaaS model: The Authority may choose this model to utilize only the virtual machines, storage services (IaaS) from the CSP and deploy/manage their own application or database software
- PaaS model: The Authority may opt for taking platform services (e.g., database, containers, developer tools, AI/ML capabilities) where the application/database software including the underlying Virtual Machines is managed by the CSP.
- SaaS model: Where available, the Authority may take the entire software as a service (referred as SaaS) without having to invest on the application development, middleware licenses and underlying infrastructure. The mix of the above models for an application typically depends on the application (e.g., granularity of control) and business (e.g., need for ease of management) requirements.

In case of On-premises model, the system shall be hosted in the site identified by Authority, which shall be either the existing State Data Centre (SDC) or existing/newly created facility of the city.]

Some of the indicative key components to be considered are listed below:

- Smart City Applications
- Compute
- Storage
- Data Networking
- Cyber Security
- Infrastructure Management System
- Passive Infra and Physical security
- (Add more/Modify)

The MSI is required to Provide a robust, fault tolerant infrastructure with enterprise grade SLAs with an assured uptime as per SLA defined in the Vol-3 of the RFP. The MSI shall not delete any data at the end of the O&M period (for a minimum of ….days beyond the expiry of the O&M period) without the express approval of Authority.

The Solution/Services proposed by the MSI is broadly categorized into the following components

- DC-DR Build services- (in case of On-Premises option)
- Cloud Service
- IT Infrastructure implementation services.
- Operations and Management

8.2.1 Option 1) Data Centre and DR – on the Cloud

[Note: In this model", Authority does not procure or own any DC/DR IT infrastructure and the same are procured as services from a MeitY empaneled Cloud Service Provider (CSP) by the MSI and in turn provided "as a service" to Authority. MSI may value-add further to meet the requirements of Authority. However, MSI shall be responsible for end-to-end SLA & information security requirements of Authority]

8.2.1.1 The MSI shall ensure the following functional requirements are met

#	Parameter	Functional Requirement	Bidder's Response (How functionality shall be met)
1	Availability	DC and DR shall be operational 24 x 7 x 365 with no single point of failure (NSPoF) at any of the following component level: o Power	

		○ Cooling ○ Fire protection ○ Data Network ○ IT infrastructure ○ Physical security	
2	Certifications	DC and DR shall comply with the following standards: ○ Tier III or above by UPTIME/TIA-942 ○ ISO27001, ISO 27017, ISO 27018, ISO 20000-9, ISO/IEC 20000-1. The CSP should be MeitY empaneled /MeitY funded under GI Cloud (MeghRaj) Initiative	
3	"Audit Rights with provisioned cloud services	Management console to the Authority. The MSI shall allow review of the provisioned resources (e.g., cloud services, network & security controls, utilizations etc) and view the configuration of each; Logs of all user activity within an account and any other logs (e.g., n/w traffic, account activity, resource inventory, configuration history, and configuration change) that are captured for audit purpose. The CSP must provide access to the cloud	
4	Cloud Services	MSI shall provide details of all the IT services procured from the CSP along with: ○ Availability parameters ○ SLA parameters ○ Cyber Security Controls	
		The procured list of services by MSI shall meet all the functional requirements specified in the RFP	
5	DR Location	As per MeitY guidelines	
6	DR Services	DR Management services shall provide facilities to measure the RTO and RPO parameters regularly. [RPO: Amount of data loss tolerable to Authority] [RTO: Time required to resume services in DR for Authority]	

		Procured list of services by MSI shall meet all the functional requirements for the IT infrastructure given in the RFP	
		DR Management services shall enable Authority to carry out automated DR switchover both in cases of emergencies and during planned DR drills	
		DR Management services shall enable Authority to carry out phased restoration to switchback services to normal operations in DC	

8.2.1.2 Responsibility Matrix - CSP and MSI.

An indicative list of the responsibilities between CSP and MSI is as below:

#	Control	CSP	MSI
1	ISO 27001 Compliance & Certification - CSP Managed Infrastructure	Y	N
2	ISO 27017 Compliance & Certification	Y	N
3	ISO 27018 Compliance & Certification	Y	N
4	ISO 2000 Compliance & Certification	Y	N
4	Physical Infrastructure (hardware, software, networking, and facilities) under the responsibility of the CSP - Data Center Physical Security & Environmental Controls - Supply Chain Security - Personnel Security - Network Security: Firewall and Other Boundary Devices - Network & Security Continuous Monitoring - Asset Management, Maintenance, and Refresh - Configuration and Change Management - Vulnerability Management - Information Security Incident Response & Management - Resource / Capacity Planning - Business Continuity and Resiliency - Media Protection - Decommissioning / Secure Equipment Disposal	Y	N
5	Hypervisor Security and Patch Management	Y	N

6	Host Operating System (Security, Patch Management)	Y	N
7	Conduct a well architected framework review of deployed infrastructure and workloads. Submit the report to Authority once an year	Y	N
8	Conduct a security review of all the deployed infrastructure and submit reports to Authority once an year	Y	N
9	Virtual Infrastructure (e.g. Compute, Storage) Provisioned in Cloud under the responsibility of the MSP - Network & Data Security - Continuous Monitoring - Incident Management - Content Lifecycle Management - Capacity Planning - Backups & Archival - Business Continuity - Provisioning & De-Provisioning of Cloud Services - Termination / Deletion	Provides Self-Service Capabilities	Implementation / Configuration / Monitoring Responsibility
10	Guest Operating System (Security, Patch Management)	Provides Self-Service Capabilities	Implementation / Configuration / Monitoring Responsibility
11	NOC / SOC for the Virtual Private Cloud (VPC) Environment Provisioned in Cloud by the MSP using the audit trail, configuration logs, access logs, network traffic logs,..	Provides Self-Service Capabilities	Implementation / Configuration / Monitoring Responsibility
12	Cloud Services - Load Balancers - Virtual Isolated Network - VPN Gateway - Firewall	Provides Self-Service Capabilities	Implementation / Configuration / Monitoring Responsibility
13	Service to monitor, store, and analyze log files from various cloud services provisioned in the Cloud	Provides Self-Service Capabilities	Implementation / Configuration / Monitoring Responsibility

14	Auto Scaling Capability	Provides Self-Service Capabilities	Implementation / Configuration / Monitoring Responsibility
15	Service to record API calls - 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.	Provides Self-Service Capabilities	Implementation / Configuration / Monitoring Responsibility
16	Service to capture resource (cloud services) inventory, configuration history, and configuration change notifications to enable security and governance	Provides Self-Service Capabilities	Implementation / Configuration / Monitoring Responsibility
17	Notification of security and privacy events affecting Cloud services	Provides Self-Service Capabilities	Monitoring / Necessary Action Responsibility
18	Up-to-the-minute information on service availability and notification of interruptions to each individual service and a full status history of each individual service health.	Publishes Information	Monitoring / Necessary Action Responsibility
19	Alerts and remediation guidance when underlying cloud services are experiencing events that may impact the provisioned services. View into the performance and availability of the cloud services underlying the provisioned resources.	Publishes Alerts & Guidance	Monitoring / Necessary Action Responsibility
20	Services to optimize costs & identify security gaps,	Provides Self-Service Capabilities	Monitoring / Necessary Action Responsibility
21	DDoS Protection Service	Y	N
22	Web Application Firewall (WAF) Service	Provides Self-Service Capabilities	Implementation / Configuration / Monitoring Responsibility
23	Identity & Access Management Service	Provides Self-Service Capabilities	Implementation / Configuration / Monitoring Responsibility

24	Multi-factor Authentication Service	Provides Self-Service Capabilities	Implementation / Configuration / Monitoring Responsibility
25	Key Management & Encryption Service (Data at rest and Data in Transit)	Provides Self-Service Capabilities	Implementation / Configuration / Monitoring Responsibility
26	Uptime SLAs for Cloud Services	Y	N
27	Transition Out / Exit Management - Services to export Virtual Machine Images - Services to export customer content / Data	Provides Self-Service Capabilities	Implementation / Exit Management Responsibilities

8.2.1.3 Security Compliances and Governance

While selecting the CSP, the MSI shall ensure compliance to following security controls for cloud services:

- The CSP/Service Provider should be empaneled by MeitY for providing cloud services. The CSP's facilities/services shall be certified to be compliant to the following standards: ISO 27001, ISO 27017, ISO 27018, ISO 20000-9, ISO/IEC 20000-1. SOC1, SOC2 certifications. CSP/Service Provider shall take appropriate measure for their cloud services to secure Authority's content against accidental or unlawful loss, access, or disclosure.
- The CSP/Service Provider shall comply with any security requirements applicable to CSPs/Service Providers published (or to be published) by MeitY or any standards body setup / recognized by Government of India from time to time and notified to the CSP/Service Providers by MeitY as a mandatory standard. (Refer MeitY published guidelines/reference document)
- The CSP/Service Provider shall meet all the security requirements indicated in the IT Act 2000, the terms and conditions of the Provisional Empanelment of the Cloud Service Providers and shall comply with the audit criteria defined by STQC directorate.
- Incident Management shall be done by MSI.
- Periodic secure code review shall be performed for cloud applications and compliance to secure software development lifecycle.
- Data encryption at rest / transit depending on sensitivity of data shall be implemented using Authority managed keys, which are not stored on the cloud. Data communications should be encrypted in transit and no access over public network should be allowed
- Appropriate encryption mechanisms such as "two-way" shared key symmetric encryption, "two-way" public/private key asymmetric encryption, "one-way" salted hash encryption, etc. should use to secure data at any tier of the application. Due care must be taken to ensure that

cryptographic modules used by the application are compliant with international standards both from vendor and algorithm perspectives.

- Key management process shall be properly documented and should entail key distribution plans which detail out the scenarios in which key management components are encrypted or decrypted and their physical form
- The CSP/Service Provider shall undertake to treat information passed on to them as classified. Such Information shall not be communicated / published / advertised by the CSP to any person/organization without the express permission of the Authority.
- MSI shall inform all security breach incidents to Authority on real time.
- CSP/Service Provider shall ensure data confidentiality i.e. the data shall not be accessible by anyone other than the Authority, unless legally required and related risk shall be covered by CSP/Service Provider.
- E-Discovery shall be included as clause in SLA with CSP/Service Provider. It is the process of locating, preserving, collecting, processing, reviewing, and producing Electronically Stored Information (ESI) in the context of or criminal cases/proceedings or investigation. Logging and reporting (e.g., audit trails of all access and the ability to report on key requirements/indicators) must be ensured.
- The Law Enforcement Agency as mandated under any law for the time being in force may seek access to information stored on cloud as provided by the CSP/Service Provider. The onus shall be on the CSP/Service Provider to perform all due diligence before releasing any such information to any such law enforcement agency. The process for release and transfer shall be detailed in the agreement and approved.
- CSP/Service Provider must ensure location of all data related to Authority to be stored in India only. The CSP/Service Provider must explicitly detail the access to data being stored and guarantee that there shall be no access to the data or its derivatives to any other commercial entity or any access to foreign entities.
- The CSP/Service Provider's services offerings shall comply with the audit requirements defined under the terms and conditions of the Provisional Empanelment of the Cloud Service Providers (or STQC /MEITY guidelines). The Audit, Access and Reporting Requirements should be as per the terms and conditions of the Provisional Empanelment of the Cloud Service.
- CSP/Service Provider's exit Management Plan shall include - Transition of Managed Services & Migration from the incumbent cloud service provider's environment to the new environment and shall follow all security clauses for smooth transition.
- SLA with MSI shall cover performance management & dispute resolution escalation. Guidelines on Service Level Agreement issued by MeitY lists out the critical SLAs for cloud services.
- Identification and problem resolution (e.g. helpline, call center, or ticketing system) mechanism must be defined and approved

- Change-management process (e.g. changes such as updates or new services) must be defined with sufficient staging and testing.
- Appropriate segregation of Virtual Private Cloud (VPC) security rules defined as part of firewall should implement role-based access management, Logging and monitoring.
- VPN gateway must be setup to ensure controlled access, appropriate security rules must be employed to encrypt outward data flow, IDS, IPS, API Gateways to be setup and ELB logs to be maintained for any activities and access and exceptions to carried out in the cloud setup, Database logs to be routed as part of the Logging VPC setup.
- Digital Certificate shall be implemented for secure access.
- Web Application Firewall must be provided, Host IPS must be setup on all the Web servers, Web servers must be configured as per the CIS hardening guidelines and baseline security requirements, logging and monitoring should be enabled.
- Application access between hosted Smart City applications shall be segregated, internal infrastructure and external traffic, Role based access must be defined, hardening of database instances as per the CIS baselines configuration guidelines in the cloud setup must be ensured, Logging and monitoring must be enabled.
- The proposed CSP/Service Provider architecture may have multiple Data Centers grouped through a low-latency network to support redundancy, higher degree of High-Availability and Fault Tolerance.
- The CSP/Service Provider should adhere to the model framework for cyber security (K-15016/61/2016-SC-1, Government of India, and Ministry of Urban Development) and also section 9 of this RFP. The certification requirements for CSP/Service Provider for this model framework shall be as per MeitY guidelines.
- The MSI shall provide required DR planning. The following are the key DR requirements for the envisaged solution:
    - The solution should be designed for an Active-Active/Active-Passive DC/DR architecture. In case of Active-Passive architecture, then DR should be provisioned with ……% capacity as provisioned in the DC. System Architecture to be designed to achieve (i) [Zero min RPO and 30 minutes RTO] for critical applications and (ii) [15 min RPO and 30 minutes RTO for non- critical application]. [The authority may decide applicable RTO/RPO as per the uptime requirements.].
    - The MSI shall be responsible for provisioning of replication bandwidth between DC & DR.
    - The MSI shall offer services from DR at the time of outages in the DC.
    - All servers should be replicated, and automation must be part of the software functionality to failover/failback to the DR-DC adhering to the specified RPO and RTO.
    - Failover scenario: The proposed solution should allow pre-built recovery plans for various servers which includes target server configuration, IP configurations, network configuration etc. Test DR Failover scenario should not affect the primary server at all.

- Failback Scenario: The proposed solution should ensure failback to original DC and should take care of replication of only incremental change (changed data after failover) from DR to DC.
- DR drills needs to be performed half yearly (or as per Authority requirements) to check for disaster preparedness and a report to be submitted to Authority. The MSI shall also provide a plan for handling the DR scenario including the roles and responsibilities for each stakeholder.
- MSI shall pre-check the feasibility of whether the application workload works seamlessly in case Active-Active scenario is proposed
- The MSI shall undertake to treat information passed on to them as classified in a secure way. Such Information shall not be communicated / published / advertised by the CSP/Service Provider to any person/organization without the express permission of the Authority.
- MSI shall inform all security breach incidents to Authority in real time.

8.2.2 Option 2) Data Centre and DR Services – Hosted Model

[In the "Hosted model", Authority procures its own DC/DR IT infrastructure but due to space, electrical power and time constraints, may request the MSI to house/host them at a Hosting Service Provider (HSP) premises. In this case, the Service Provider provides only basic services such as power, cooling, fire protection, etc. and no IT services.]

If Authority plans to opt for the "Hosted model", then MSI along with the Hosting Services Provider (HSP) partner shall ensure the following functional requirements are met:

#	Parameter	Functional Requirement	Bidder's Response (How functionality shall be met)
1	Availability	DC and DR shall be operational 24 x 7 x 365 with no single point of failure (NSPoF) at any component level: o Power o Cooling o Network cabling o Fire protection o Physical security	

2	Certifications	DC and DR shall comply with the following standards: o Tier III or above by UPTIME/TIA-942 o ISO27001 certified, ISO 27017, ISO 27018, ISO 20000-9, ISO/IEC 20000-1. o The HSP should be MeitY empaneled /MeitY funded under GI Cloud (MeghRaj) Initiative	
3	Rackspace and caging	HSP shall provide: o Dedicated and sufficient racks and rack space for Authority. o Provide additional min 10% rack space area for any immediate exigencies. o The entire dedicated rack space area including the expansion area shall be caged with biometric access control.	
4	Physical access	DC and DR shall be physically accessible to Authority or Authority appointed organizations to carry out any activity within the DC/DR, audits and inspections any time of the year	
5	DR Location	As per MeitY guidelines	

8.2.2.1 Compute Infrastructure

The compute resources are key components of the IT infrastructure that hosts a variety of smart city applications rendering various services to the citizens. Compute nodes may be bare metal, virtual machines or containerized. Irrespective of the type of compute resources, the key indicative functional requirements are given below.

#	Category/ Parameters	Functional requirement	Bidder's Response (How functionality shall be met)

1	Components	Compute resources shall use only latest editions/ versions of industry standard components for: ○ Processors ○ Memory ○ Interconnect components ○ I/O interfaces and adapters ○ HDD	
2	Availability	Compute resources hosting citizen centric and other city applications should be highly available to enable Authority to meet the demands of the citizens and other stakeholders.	
3	Isolation	Fault or failure of a compute node, hosting a city service or application shall not impact other services or applications running on other compute. Any downtime of applications or services due to such a failure shall be taken into account for SLA measurements.	
4	Security	Compute nodes shall be secured and deployed based on parameters such as: ○ Purpose (for example, compute & storage nodes for a database) ○ Designation (for example, Production or UAT compute & storage) ○ Hosted service, application or data (for example, payment gateway services) ○ Internet or Intranet facing (for example, Internet facing compute & storage nodes to be hosted on DMZ)	
5	Scalability	Compute nodes should be capable of dynamically scaling up or down to optimally cater to the demand requirements. Scaling up or down requests shall be serviced within [XX] hours of raising the request by Authority, which shall be considered for SLA measurements.	
6		Compute nodes shall have their functionalities exposed through a secure and easy to use interface for:	

	Operations and Management	○ Power cycle (power on/off through a soft operation) ○ Diagnosis and troubleshooting ○ Firmware updates and upgrades ○ Installation and configuration ○ Lights out operation ○ Console access ○ Virtual media device	
		Access to the above capabilities shall be provided only to authenticated and authorized resources.	
		Capability to provide access over mobile devices through a secure mobile App.	
		Capability of sending logs to a central logging solution	
7	Integration and Automation	Shall provide for RESTful APIs for integrating management tools and automated provisioning. List of APIs to be provided	
8	OS support	Should support latest versions of industry standard, leading operating systems as required by the application being hosted. (List of OSes supported along with version to be provided)	
9	Response time	End-to-end response time through all intermediary security devices shall be within [XX] seconds as given by the Authority SLA.	
10	Compute self-administration	For self-administration, a secure, easy to use interface shall be provided: ○ Dynamically scale up or down resources for an application or service, as applicable ○ Perform management tasks on the compute & storages (power cycle and remote management) ○ Perform OS upgrades and updates ○ Provide for VPN connectivity to access the compute & storages and deploy applications remotely	

8.2.2.2 Data Storage

Storage is a key component of the IT infrastructure for Authority that helps it to preserve critical data. Storage may be Direct Attached Storage (DAS), Storage Area Network (SAN) based, Network Attached Storage (NAS) or Software Defined Storage (SDS). Irrespective of the type, the following are the key indicative functional requirements for the storage to be met. The metric that shall be used to measure the requirement is given along for easy reference.

#	Parameter	Functional Requirement	Bidder's Response (How functionality shall be met)
1	Components	Storage systems shall use only industry standard components for: o Interconnect cables o HDD	
2	Availability	Storage system should be highly available to enable Authority to meet the demands of the citizens and other stakeholders	
3	Isolation	Fault or failure of any storage component shall not impact running compute & storages, applications, data availability, data access or data integrity Any downtime of applications or services due to such a failure shall be considered for SLA measurements	
4	Data protection and retention	City data should be available on online storage accessible 24 x 7 x 365 Data older than X days should be on off-line storage for X days/years as required by Authority (Note: City to define the Classes of the data in city data policy)	
		Data stored on off-line storage should be made available on online storage within X minutes/hours whenever demanded by Authority	
5	Data integrity	Storage shall be configured to ensure no data corruption at any point in time	
6	Security	Access to data shall be provided only to authenticated and authorized resources such as applications, users and systems. No direct access to disks or devices shall be permitted.	

7	Scalability	Storage systems shall be dynamically scaled up or down to optimally cater to the demand requirements. Scaling up or down requests shall be serviced within [XX] hours of raising the request by Authority, which shall be considered for SLA measurements.	
8	Storage type support	Storage system shall provide support for storing all types of data: o Structured o Unstructured o Streaming video	
9	OS and file system support	Shall support the 64-bit versions of operating systems and file systems as demanded by the solution being deployed	
10	Usable storage space	Shall provide for sufficient storage space for all solutions being implemented with headroom for periodic data growth over the agreement period, as given by Authority. Storage calculation to be provided by MSI Used storage space shall not exceed more than 70% of the usable capacity at any given time. 30% headroom should always be available.	
11	Operations and Management	Storage capabilities and functionality should be exposed through a secure and easy to use interface for: o Power cycle (power on/off through a soft operation) o Diagnosis and troubleshooting o Firmware updates and upgrades o Installation and configuration o Lights out operation o Disk and Volume configuration Access to the above capabilities shall be provided only to authenticated and authorized resources. The Capability of sending logs to a central logging solution should be available	
12	Integration & Automation Management Tools	Shall provide for RESTful APIs for integrating management tools for automated provisioning and management tools [List of Management Tools to be provided]	

13	I/O service time	Storage I/O service time shall be within Y milliseconds to enable applications to have the response time of X seconds (Ref. Compute & storage specifications). The iOPs should be designed as per RFP requirement.	
14	Storage self-administration	For self-administration, a secure, easy to use web-based interface shall be provided: ○ Dynamically scale up or down storage resources (disks/volumes) for an application or service, as applicable ○ Perform management tasks on the storage (power cycle and remote management) ○ Perform housekeeping tasks on storage (archive, compress least accessed data or infrequently used data) ○ Perform firmware upgrades and updates ○ Provide for VPN connectivity to access the storage for remote management	

8.2.2.3 Data Network

Data Network shall be provisioned as part of Authority's IT infrastructure for communication locally within the DC & field location as well as over the Internet. Networks may be implemented using physical routers or switches or using Software Defined Networking (SDN) virtual switches or routers. Whatever the type, following are the key indicative functional requirements.

#	Parameter	Functional Requirement	Bidder's Response (How functionality shall be met)
1	Components	Network routers or switches shall use only industry standard components for interconnect cables and interface components should be L3 manageable	
2	Availability	Network routers or switches should be highly available to enable Authority to meet the demands of the citizens and other stakeholders	
3	Isolation	Fault or failure of any core or intermediary network component shall not impact running compute & storages, storage, applications, data availability, data access or data integrity. Any downtime of applications or services due to such a failure shall be considered for SLA measurement.	

4	Scalability	Switches and routers should be scalable and modular. There should be sufficient headroom for additional modules to be installed and configured. Scaling (horizontal or vertical) requests shall be serviced within X hours of raising the request by Authority, which shall be considered for SLA measurements.	
		Support as many VLANs that are required to be created as part of the solution.	
5	Protocol	Shall support both IPv4 and IPv6 simultaneously.	
6	Ports	Switches shall support standard speed host ports and high-speed uplink ports with auto-negotiate capability	
		Shall provide for as many no. of ports as required by the solution.	
		No. of used ports shall not exceed more than 70% of the total port capacity at any given time. 30% headroom should always be available.	
7	Access control	Should be able to control access based on MAC, Protocol, IP address and port	
8	Operations and Management	Network routers or switches shall expose their capabilities and functionalities through a secure and easy to use interface for: o Power cycle (power on/off through a soft operation) o Diagnosis and troubleshooting o Firmware updates and upgrades o Installation and configuration o Lights out operation o Switch or router configuration Access to the above capabilities shall be provided only to authenticated and authorized resources. Capable of sending logs to a central logging solution	

9	Network self-administration	For self-administration, a secure, easy to use interface shall be provided: ○ Dynamically configure or reconfigure networks and ports as required ○ Perform management tasks on the network router or switch (power cycle and remote management) ○ Perform firmware upgrades and updates ○ Provide for VPN connectivity to access the routers or switches for remote management	

8.2.3 Option 3) Data Centre On-premises Model and DR on Cloud /Hosted model.

[In the "On-premises model" for DC, Authority builds the DC at its own/state level real estate and hosts the IT infrastructure within this DC. In this case, the MSI shall build the DC based on the physical specifications provided by Authority and provide services for the same. After completing the DC physical build, the MSI shall install and configure the IT systems within the DC. The MSI is still responsible for the overall SLA in this model also. Authority may follow either the "Cloud model" or the "Hosted model" for the DR site].

The MSI shall ensure the following functional requirements are met:

#	Parameter	Functional Requirement	Bidder's Response (How functionality shall be met)
1	Availability	MSI shall build the DC for 24 x 7 x 365 with no single point of failure (NSPoF) at any component level: ○ Power ○ Cooling ○ Network cabling ○ Fire protection ○ Physical security	Uptime or Availability
2	Certifications (DC)	○ Tier III or above by UPTIME/TIA-942 ○ ISO27001 certified, ISO 27017, ISO 27018, ISO 20000-9, ISO/IEC 20000-1	

3	Rack space and caging	MSI shall: ○ Provide for sufficient rack space area for hosting all proposed racks ○ Leave min 10% rack space as space for future expansion ○ All rack space should be clearly demarcated ○ Rack space including future expansion area shall be caged with biometric access control ○ For DR, please refer to provisions in Option 1 & 2 above.	
4	Physical access	Multi-factor physical access shall be provided for access to the DC.	
5	Compute/storage / Data network	Please refer to provisions in Option 2 above.	
6	DR	For DR, please refer to provisions in Option 1 or option 2 above.	

[City may add additional DC/DR hosting specifications]

8.3 Implementation Services- on premised model

The MSI shall be responsible for implementing and integrating the IT solutions to enable the city stakeholders achieve their objectives. The IT infrastructure must be made ready before city specific applications can be implemented.

Following are the implementation services to be provided by the MSI:

#	Parameter	Functional Requirement	Deliverables
1	Environmental planning	MSI shall optimally size all environmental requirements, as applicable: ○ Racks and rack space ○ Power requirements ○ Cooling requirements ○ Passive cabling requirements ○ Wi-Fi access points in operational area ○ Operational space requirements	1. Rack schematics 2. Power schematics 3. Passive cabling drawings 4. Wi-Fi access points 5. DC floor plan 6. Staff seating plan

2	Preparation of Disaster Recovery Operational Plan	The MSI shall provide detailed operating procedures for each application during the following scenarios. These shall be mutually agreed upon with Authority during the project kick off. a) Business as usual: the primary site is functioning as required, procedures for ensuring consistency of data availability at secondary (DR) site. b) Disaster: Declaration of disaster, making the DR site live for production, ensuring availability of users to the secondary site. c) Operations from DR site: Ensuring secondary site is addressing the functionality as desired x	
3	IT infrastructure sizing for both DC and DR	MSI shall optimally size all IT infrastructure requirements, including, but not limited to: ○ Compute & Storage ○ Data Storage (online and offline) ○ Network ports (core and access) ○ No. of security zones ○ No. of VLANs in each zone	Sizing calculations and justifications
4	Bandwidth and User load sizing	MSI shall be responsible for sizing the user load per application being deployed, field devices being deployed and assess the network bandwidth required for: ○ WAN (Field to DC) ○ Internet ○ DC to DR for replication ○ ICCC to DC and DR	Bandwidth sizing calculations and justifications
5	Project Planning	MSI shall be responsible for overall project planning, resourcing and scheduling to meet the implementation timelines proposed by	1. Detailed Project Plan document

		Authority. As part of planning, MSI shall provide: ○ Project plan ○ Staffing plan ○ Project Organizational structure ○ Detailed activity list for each subproject ○ Project risks and mitigation plan ○ Internal and external dependencies ○ Communication plan ○ Stakeholder communication ○ Documentation plan ○ Roles and Responsibilities matrix ○ Escalation matrix ○ User Acceptance Testing plan ○ Success criteria and Sign-off ○ Operations and Management plan	2. Organizational structure and resource details 3. RACI matrix 4. Testing strategy document 5. Templates for various documents 6. Operational Plan
6	Planning and Design – IT Infrastructure solutions	MSI shall plan and design the DC Architecture as per the SLA requirements of Authority: ○ IT infrastructure architecture ○ IP address and network planning and design ○ DNS planning and design ○ Enterprise Directory design ○ Infrastructure security planning and design ○ Identity and Single Sign On (SSO) design ○ Application Integration solution planning and design ○ End user (all stakeholders) accessibility design	1. High level design 2. DC Low level design

7	DR Planning and Design	MSI shall plan and design the DR strategy and recovery procedures as per the RTO and RPO requirements of Authority: ○ DR strategy ○ Business Impact Analysis of the solutions deployed ○ DR IT infrastructure architecture ○ DR Network, IP planning and design ○ Infrastructure security planning and design at DR ○ Data replication methodologies for forward and reverse replication ○ Periodic data consistency check report ○ Detailed Disaster Recovery switchover steps and procedures for every solution deployed ○ Detailed switchback and restoration procedures for every solution deployed ○ DR management – Automation and monitoring	1. DR strategy 2. DR Low level design 3. DR Management document 4. DR detailed steps and procedures
8	DC Implementation services	MSI shall install and configure the IT infrastructure and the proposed solutions in compliance with the availability requirements of Authority with No Single Point of Failure (NSPoF)	Installation reports
9	DR Implementation services	MSI shall install and configure the IT infrastructure and the proposed solutions in compliance with the availability requirements of Authority at DR.	Installation reports
10	Solution Implementation Services	MSI shall install and configure all IT solutions that have been proposed as below, but not limited to: ○ Enterprise Directory ○ Identity Management and Single Sign-On (SSO) ○ Collaboration	For each solution: 1. Installation reports 2. Solution Architecture documents

		○ Enterprise Service Bus (ESB) and Application Integration platform ○ API and Service management ○ Data Management ○ ICCC Application platform ○ Mobile enablement ○ Enterprise Management ○ Citizen web portal and related	3. Solution Operations documents 4. Integration guides 5. User guides
11	Integration services	MSI shall integrate with the following solutions if they already exist with Authority or as common services for the city: ○ Payment gateway ○ SMS gateway ○ Email gateway	
		If Authority or the city does not have an SMS gateway, MSI shall propose and procure SMS gateway services. MSI shall calculate the no. of SMS messages that shall be generated and validate the same with Authority before going ahead with the procurement of such services	
12	Procurement of certificates	If Authority does not have a registered DNS domain and SSL/TLS certificates, then MSI shall carry out: ○ DNS domain registration ○ Procure SSL/TLS certificates Based on the requirement, MSI shall decide in coordination with Authority whether to procure domain, wildcard SSL/TLS certificates. Certificates must be procured from vendors licensed by Controller of Certifying Authorities (CCA) of India	

8.4 Operations and Management

Operations and management require a robust framework to ensure that ICT systems perform at the required level. The MSI shall take up Operations and Management post UAT and acceptance by Authority.

#	Parameter	Requirement	Deliverables
1	Operations and Management processes design	MSI shall design appropriate operational processes for Authority as below, but not limited to: ○ Resources on-boarding ○ Helpdesk services ○ Service catalogue ○ User Management ○ Change Requests ○ Service Requests ○ Incident Reporting and tracking ○ Security Emergency ○ Patch Management ○ SLA monitoring and reporting ○ Application on-boarding	1. Process documentation for each of the listed topics 2. Checklists as applicable (e.g., Application go-live checklist)
2	Operations and Management services	MSI shall provide the following 24 x 7 x 365 Operational and Management services and resources for: ○ Helpdesk services ○ Physical infrastructure management and monitoring ○ IT infrastructure administration and monitoring ○ Network administration and monitoring ○ Security management and monitoring ○ Application and compute & storage performance monitoring	1. Periodic Availability (uptime, downtime) reports 2. Periodic resource utilization reports 3. SLA reports 4. Application performance reports 5. Security incident reports 6. Network bandwidth utilization reports 7. Service ticket reports

		○ Data replication and DR readiness monitoring	8. RTO and RPO reports
3	DR drills	MSI shall be responsible for conducting periodic DR drills, min. 2 per year or as prescribed by Authority	DR drills report
4	Security Vulnerability and Penetration testing	MSI shall carry out periodic (min. 1 per year or as prescribed by Authority) Security vulnerability and Penetration testing of the IT infrastructure, by CERT-IN empaneled Information Security auditors	Audit report

The MSI shall put an effective monitoring and management system be put in place with following minimum considerations:

#	Parameter	Requirement
1	Functionalities	The proposed solution shall include the following functionalities, but not limited to: ○ Helpdesk services ○ IT Asset and configuration Management ○ Network Monitoring and Management ○ Server Monitoring and Management ○ Application Monitoring and Management ○ End user response time monitoring and management ○ Incident Reporting and tracking ○ SLA monitoring and reporting
2	Auto discovery capability	Proposed solution shall have capability to automatically discover manageable elements connected to the infrastructure and map the connectivity between them. It should include, but not limited to: ○ Servers ○ Storage ○ Network switches ○ Routers ○ Any IP device

3	Thresholds and alerts	Proposed solution shall have capabilities to set various performance thresholds on devices and generate alerts in real-time, when those thresholds are breached Solution shall have capabilities to send the generated alarms in real-time over (not exhaustive): o Mobile SMS o Email o On screen o Mobile App o WhatsApp
4	Configuration Management	Capable of baselining device configuration and track all configuration changes
5	Performance Management	Capable of monitoring and reporting minimum, maximum, current values of all parameters as below, but not limited to: o CPU o Memory o Storage I/O o Storage capacity o Network I/O o Network utilization o Processes o Users
6	Analysis	Proposed solution shall be capable of performing various analysis. Some indicative lists are: o Root cause analysis o Performance analysis (historical and current) o Helpdesk process analysis o Incident and problem analysis

Important Notes:

- MSI shall provide interoperability support with regards to available APIs, data portability etc. for Authority) to utilize in case of Change of CSP, migration back to in-house infrastructure,

burst to a different cloud service provider for a short duration or availing backup or DR services from a different service provider.

- The MSI shall be fully responsible for tech refreshes, patch management and other operations of infrastructure that is in the scope of the MSI during the agreement period.
- Authority shall retain ownership of all virtual machines, data, templates, clones, and scripts/applications created for the Authority application.
- Authority retains the right to request (or should be able to retrieve) full copies of these virtual machines at any time.

9. Cyber security

9.1 Overview: City Cyber security

Advanced and integrated technology to deliver services to the citizens in an efficient manner (as per the scope of this RFP), may expand the cyber threat landscape of the city, and therefore, the authority has planned to consider the cyber security requirements in a comprehensive manner. The objective of the Authority from Cyber security and privacy perspective is to:

- Deliver services to citizens in a safe, secure and reliable manner
- Protect the confidentiality, integrity and availability of the data processed during city operations
- Maintain the privacy of the personal data of the citizens collected while provisioning city services
- Provide City services in compliance to GoI Regulations with regard to the security and privacy of the data
- Protect the City infrastructure and data from existing and emerging cyber security and privacy threats
- Create Cyber security awareness for all the stakeholders involved, and citizens at large
- Resolve cyber security incidents

9.2 Cybersecurity Requirements

Minimum cyber security requirements that must be met by the MSI throughout the duration of the contract are detailed in the following sections. The MSI shall bring appropriate tools, technologies and solutions (which together shall be referred to as security solutions), deploy qualified and experienced cyber security and privacy professionals and implement appropriate policies to meet the security requirements. At any time during the execution of the agreement, if any security solutions intended to meet the security requirements are found to be insufficient / ineffective, the MSI is expected to bring additional numbers or additional solutions to compensate for the requirement.

9.2.1 Cyber Security Structure

The MSI shall deploy a team of qualified and experienced cyber security and privacy professionals which shall include Security Governance Expert, Vulnerability assessment and penetration tester, Security Network Architecture Expert, Security Risk and Compliance Manager and many others, as detailed in “Vol I - Man Power Requirement”. The cyber security team shall work in cohesion to implement and maintain the desired level of information security.

This cyber security team shall perform the following responsibilities:

- Provide information security directives, management direction, security strategy and support for information security initiatives
- Evaluate and constantly strive to improve the security posture of Authority
- Develop and monitor a strategic, comprehensive information security program

- Ensure security solutions are implemented as per Authority's security requirements

9.2.2 Cyber security framework

[The MSI shall implement Cyber Security and Privacy Framework and security policies aimed at building a secure and resilient cyberspace for citizens and stakeholders of Authority. The Framework shall be designed to protect cyberspace information and infrastructure; build capabilities to prevent and respond to cyber-attacks; and minimize damages through coordinated efforts of institutional structures, people, processes, and technology.

This shall be implemented based on the following guidelines / standards:

- MoHUA guidelines vide circular K- 15016/61/2016-SC-1 dated 20th May 2016
- Government of India guidelines on Data Security
- IT Act
- CERT-IN guidelines
- CMP guidelines on countering cyber-attacks
- International standards including ISO 27001
- NIST Cyber Security Framework

The MSI shall ensure implementation of Smart City Cyber Security Policy and related procedures is in line with relevant national and international standards. The MSI shall implement Standard Operating Procedures for smooth Operations and Maintenance of IT infrastructure.

Security procedures including, but not limited to the following, shall be implemented:

- Asset management
- Change management
- User access management
- Patch management
- Back up management
- Incident management
- Communications security
- Supplier relationship
- Cryptography
- Secure software development
- Physical and environmental security
- Business Continuity and Disaster Recovery
- IOT Security

- Minimum security baseline (hardening) documents for:
    - IT systems and databases (e.g., operating systems, databases)
    - Network and security devices (e.g., firewall, switches, routers)
    - IOT devices (e.g. sensors, actuators)
    - Other systems (e.g. CCTV, OT, etc.)
    - Integration between various components

A security baseline document shall define a set of minimum-security requirements which shall be met by any given service or system implemented in the city. All systems/services shall be implemented ensuring the compliance to defined security baseline.

9.2.3 Cyber Security Governance

MSI shall put Cyber security governance in place to ensure cyber security aspects are considered for the Authority in a comprehensive and continuous manner:

- MSI shall establish Cyber security organization structure with clearly defined security roles and responsibilities with skilled cyber security professionals throughout the duration of the contract
- MSI shall conduct Risk Assessment and develop a secure network architecture considering security across all the layers: Application, Data, Communication and Sensor layers.
- MSI shall facilitate management reporting in form of dashboard for security maturity across different areas on a regular basis
- MSI shall implement security controls as required for the protection of the Authority's services and data

9.2.4 Secure Design and operations

MSI shall ensure that security is integral throughout the development life cycle of Authority. Smart city architecture shall be designed in a secure manner, considering security across all the four layers: Application layer, Data Layer, Communication layer, and Sensor layer in line with national and international standards, security policies and procedures, and Cyber security Model framework for smart cities. The implementation and operations shall be performed in a secure manner in compliance to the Cyber security framework and policies and procedures as detailed above.

9.2.5 Security Operations Center

Security Operations Centre shall be setup to ensure continuous monitoring and manage cyber security operations pertaining to Authority. Security Operations Centre shall be a secure facility dedicated to maintaining situational awareness to detect, respond and respond to cyber threats/incidents. It shall include the following:

- Design, implementation and operations of Security Operations Centre

- Ensure that appropriate logs are enabled, captured and retained for analysis from all the relevant systems and devices
- Setup the processes to perform security monitoring on a 24x7 basis. MSI may consider remote monitoring to optimize efforts (upon consultation with authority).
- Design other SOC processes including incident handling and escalation, incident investigation, use case update, etc.
- Implement appropriate ticketing system to report and manage security incidents
- Establish appropriate mechanism to respond to security incidents

Cyber Incident Management teams need to be set up to manage and mitigate the cyber incidents and risks for the Authority. All the information on incidents be shared regularly with Indian Computer Emergency Response Team (CERT-ln) and NCIIPC (National Critical Information Infrastructure Protection Centre) and take help to mitigate and recover from the incidents in compliance to GoI regulation.

9.2.6 Information Security Assessment

MSI shall perform Information security assessment of the Smart City services and related applications before Go-Live and on a regular basis (half-yearly by MSI and annually by an external agency) after the Go-Live to ensure continuity of cyber security for the Authority. The assessment shall be performed in line with defined policies and procedures, Cyber security model framework, international standards, Government of India guidelines and Regulations. The assessment shall include the following:

- Security network architecture
- Network Topology and placement of security products in the network
- High-Level Design (HLD) and Low-Level Design (LLD) documents
- Zoning and network segregation
- Security operations review including change management, incident management, back-up management
- Vulnerability assessment and penetration testing of all the applications and IT infrastructure
- Application Source Code review
- Configuration review of servers, databases, and network devices
- Compliance to Regulatory and MoHUA requirements
- Security Operations Centre
- BCP and DR Plan

An Independence shall be maintained during the assessment, and the team carrying out the assessment exercise shall be different from the implementation team. Systematic actionable need to be derived post assessment and necessary changes shall be performed in a prioritized and timely

manner to enhance the cyber security maturity. Volunteer disclosure process may be delineated along with collaboration with White Hat groups.

9.2.7 ISO 27001 readiness

Information Security Management System (ISMS) shall be established in line with ISO 27001 standard for the Authority covering the following:

a) Define the following as required by ISO 27001:
    i. ISMS Policy
    ii. ISMS Scope
    iii. Cyber security policy, procedures, and guidelines
    iv. Risks and Opportunities
    v. Statement of Applicability
    vi. Risk Assessment Methodology
    vii. Security awareness
    viii. ISMS Assurance process
b) Co-ordinate with respective stakeholders to perform the risk assessment and implementation of security requirements
c) Provide security awareness trainings
d) Facilitate the internal review
e) Support during certification audit by an external agency appointed by Authority.

9.2.8 Business Continuity Planning and Disaster Recovery

MSI shall develop Business continuity and disaster recovery plan to ensure the continuity of the Smart City services. A Disaster Recovery plan for critical infrastructure and related applications shall be developed to support operations in an event of a disaster. Details of Mean Time To Failure (MTTF) and Mean time to repair (MTTR) shall be defined in the BCP and DR plan. The Business continuity and disaster recovery plan shall be tested on a periodic basis.

9.2.9 SLA management framework:

MSI shall establish an SLA management framework to monitor and report the SLAs on a regular basis. The framework should cover the following:

a) Define SLA framework for the monitoring and reporting
b) Implement and review SLA monitoring tools in line with the SLA objectives
c) Establish the process for collection of raw data, and measurement methodology for the calculation of SLA
d) Analyze the SLA data and prepare SLA reports on a regular basis

e) Review and enhance the SLA management framework on a yearly basis to improve the SLA measurement and reporting

f) Penalty for non-compliance with SLA

9.2.10 IOT Security

9.2.10.1 Discovery capabilities:

a) Asset discovery capability for operational technology environment, captures configuration data that passive scanning may not be able to deliver.

b) Alert authority about any unauthorized configuration change, identifying malicious silent installs as well as sophisticated cyber-attacks in real time if integrated with city SIEM and Integrated command and control center.

9.2.10.2 Identity and Access Management:

a) Identity and access management for operational technologies/sensors/smart devices to provide single management interpretation of access requests, reporting, analytics, and automated provisioning, as contained within a centralized directory service for unparalleled control, the configuration depends upon whether it is isolated i.e. demilitarized or connects with external systems such as cloud.

9.2.10.3 Authentication:

a) Device centric authentication capabilities to provide a critical foundation for establishing and maintaining trust in the IoT/OT devices, applications and data that are driving data collection, analytics, decision-making, and the automated processes that manage physical control systems.

b) The process of introducing and on boarding devices into an IT/OT environment must be securely controlled while meeting the specific requirements of different OT environments. Capability may provide several environment alternatives for device registration models, including automated device registration which enables secure, without manual intervention, physical control, or system access to target devices.

9.2.10.4 Authorization:

a) The environment authorization policies to determine what authenticated devices may do. An authenticated ID is used by devices such as sensors, human machine interface, traffic lights etc., the identified device may execute its functioning only if authorization policies allows i.e. post grant of permissions.

b) Operations are advised to be divided into categories such as control and data plane. Control plane allows city officials to perform administrative tasks like creating or updating certificates, things, rules etc., whereas data plane API allows sending and receiving data from cloud. Policy-based authorization is a powerful capability. It gives complete control over what a device, user, or application can do in IoT and OT environment of a smart city.

9.2.10.5 Secure Remote Administration

a) Securing remote access creating usable guidance as it pertains to control systems environments must include both users and the technology to be accessed remotely.

b) Common elements, such as users, roles, existing technology and architecture types, to be reviewed and their attributes can be leveraged.

c) Access to and from critical control system assets in the modern environment is usually LAN based, but still should be considered remote if the operator is traversing across different networks. Virtual Private Networking (VPN) is often considered the best approach in securing trans-network communication.

d) Set requirements on collection, receipt, transmission, storage, disposal, use and disclosure of cities confidential information especially for the assets which are accessed remotely.

9.2.10.6 Network Segmentation:

a) Appropriate tools and processes should be deployed for segmentation of field sensors to the overall network.

9.2.10.7 Network Binding

a) All sensors deployed as part of IT and IT based systems in the city should talk only to the authorized wireless network, and do not hook on to the rogue networks. All traffic from the sensors in the city to the application servers should be encrypted Secure Socket Layer (SSL) and authenticated prior to sending any information. The data at rest and in transit must be encrypted.

9.2.10.8 Hardening:

a) All devices and systems deployed in the city should be hardened and have the ability to be upgraded remotely for firmware through encrypted and signed images files with authentication mechanism to complete the operation.

9.2.10.9 Vulnerability Disclosure:

a) IOT product and solution providers should have a vulnerability disclosure process.

9.2.11 Security Controls for Cloud Services

The security controls for creating and managing cloud services shall comply with the following requirements. MSI along with CSP/Service Provider shall ensure:

a. The CSP/Service Provider should be empaneled by MeitY for providing cloud services. The CSP's facilities/services shall be certified to be compliant to the following standards: ISO 27001, ISO 27017, ISO 27018, ISO 20000-9, ISO/IEC 20000-1. SOC1, SOC2 certifications. CSP/Service Provider shall take appropriate measure for their cloud services to secure Authority's content against accidental or unlawful loss, access, or disclosure.

b. The CSP/Service Provider shall comply with any security requirements applicable to CSPs/Service Providers published (or to be published) by MeitY or any standards body setup

/ recognized by Government of India from time to time and notified to the CSP/Service Providers by MeitY as a mandatory standard. (Refer MeitY published guidelines/reference document)

c. The CSP/Service Provider shall meet all the security requirements indicated in the IT Act 2000, the terms and conditions of the Provisional Empanelment of the Cloud Service Providers and shall comply with the audit criteria defined by STQC directorate.

d. Incident Management shall be done by MSI.

e. Periodic secure code review shall be performed for cloud applications and compliance to secure software development lifecycle.

f. Data encryption at rest / transit depending on sensitivity of data shall be implemented using Authority managed keys, which are not stored on the cloud. Data communications should be encrypted in transit and no access over public network should be allowed

g. Appropriate encryption mechanisms such as "two-way" shared key symmetric encryption, "two-way" public/private key asymmetric encryption, "one-way" salted hash encryption, etc. should use to secure data at any tier of the application. Due care must be taken to ensure that cryptographic modules used by the application are compliant with international standards both from vendor and algorithm perspectives.

h. Key management process shall be properly documented and should entail key distribution plans which detail out the scenarios in which key management components are encrypted or decrypted and their physical form

i. The CSP/Service Provider shall undertake to treat information passed on to them as classified. Such Information shall not be communicated / published / advertised by the CSP to any person/organization without the express permission of the Authority.

j. MSI shall inform all security breach incidents to Authority on real time.

k. CSP/Service Provider shall ensure data confidentiality i.e. the data shall not be accessible by anyone other than the Authority, unless legally required and related risk shall be covered by CSP/Service Provider.

l. E-Discovery shall be included as clause in SLA with CSP/Service Provider. It is the process of locating, preserving, collecting, processing, reviewing, and producing Electronically Stored Information (ESI) in the context of or criminal cases/proceedings or investigation. Logging and reporting (e.g., audit trails of all access and the ability to report on key requirements/indicators) must be ensured.

m. The Law Enforcement Agency as mandated under any law for the time being in force may seek access to information stored on cloud as provided by the Service Provider. The onus shall be on the CSP/Service Provider to perform all due diligence before releasing any such information to any such law enforcement agency. The process for release and transfer shall be detailed in the agreement and approved.

n. CSP/Service Provider must ensure location of all data related to Authority to be stored in India only. The CSP/Service Provider must explicitly detail the access to data being stored

and guarantee that there shall be no access to the data or its derivatives to any other commercial entity or any access to foreign entities.

o. The CSP/Service Provider's services offerings shall comply with the audit requirements defined under the terms and conditions of the Provisional Empanelment of the Cloud Service Providers (or STQC /MEITY guidelines). The Audit, Access and Reporting Requirements should be as per the terms and conditions of the Provisional Empanelment of the Cloud Service.

p. CSP/Service Provider's exit Management Plan shall include - Transition of Managed Services & Migration from the incumbent cloud service provider's environment to the new environment and shall follow all security clauses for smooth transition.

q. SLA with MSI shall cover performance management & dispute resolution escalation. Guidelines on Service Level Agreement issued by MeitY lists out the critical SLAs for cloud services.

r. Identification and problem resolution (e.g. helpline, call center, or ticketing system) mechanism must be defined and approved

s. Change-management process (e.g. changes such as updates or new services) must be defined with sufficient staging and testing.

t. Appropriate segregation of Virtual Private Cloud (VPC) security rules defined as part of firewall should implement role-based access management, Logging and monitoring.

u. VPN gateway must be setup to ensure controlled access, appropriate security rules must be employed to encrypt outward data flow, IDS, IPS, API Gateways to be setup and ELB logs to be maintained for any activities and access and exceptions to carried out in the cloud setup, Database logs to be routed as part of the Logging VPC setup.

v. Digital Certificate shall be implemented for secure access.

w. Web Application Firewall must be provided, Host IPS must be setup on all the Web servers, Web servers must be configured as per the CIS hardening guidelines and baseline security requirements, logging and monitoring should be enabled.

x. Application access between hosted Smart City applications shall be segregated, internal infrastructure and external traffic, Role based access must be defined, hardening of database instances as per the CIS baselines configuration guidelines in the cloud setup must be ensured, Logging and monitoring must be enabled.

y. The proposed CSP/Service Provider architecture may have multiple Data Centers grouped through a low-latency network to support redundancy, higher degree of High-Availability and Fault Tolerance.

z. The CSP/Service Provider should adhere to the model framework for cyber security (K-15016/61/2016-SC-1, Government of India, and Ministry of Urban Development) and also section 9 of this RFP. The certification requirements for CSP/Service Provider for this model framework shall be as per MeitY guidelines.

9.2.12 Indicative Key Performance Indicators

MSI shall prepare Key performance indicators to assess the security maturity in discussion with the Authority. The key performance indicators shall include the following:

- Number of documented security procedures covering each area of operations (e.g., change management, user access management)
- Number / percentage of systems / devices configured as per hardening guidelines
- Number / percentage of Systems with updated patches
- Number / percentage of Systems with updated latest Anti-virus signatures
- Average number of days to deactivate access of former employee / contractor / third party user
- Percentage of total vulnerabilities identified during different assessment closed
- Number of security awareness training sessions conducted
- Number of security assessments (internal and external) conducted by teams independent of implementation team
- Total number of incidents reported
- Percentage of incidents responded / recovered within agreed timeframe
- Total / percentage of systems monitored on a regular basis (e.g., through security operations center)

The KPI shall be assessed and renewed annually. The suggested KPIs may also include;

i. Number/percentage of devices/end points providing security logging.
ii. Number/percentage of devices meeting regulatory requirements.
iii. Number/percentage of events requiring escalation (for reasons other than severity)
iv. Number of security incidents reported
v. Down time during incidents
vi. Total/percentage of network traffic including east/west passing through
vii. Total/percentage of network traffic including east/west for which logging is done.

9.2.13 Cyber security Service Level Agreement (Please also refer Volume III of this Model RFP)

MSI shall ensure that the Cyber security services are maintained at an appropriate level, and shall ensure the service level as defined below:

SLA Parameter	Definition	Service Levels	Penalty
Uptime			

Application uptime	Uptime of Smart city applications shall be maintained as per the threshold level on a monthly basis (24x7) MSI, in discussion with the Authority, shall prepare a list of the applications to be monitored for SLA	99.5%	X% of the monthly payment
Application Response time	Response time of Smart city applications shall be maintained as per the threshold level on a monthly basis (24x7) MSI, in discussion with the Authority, shall prepare a list of the applications to be monitored for SLA	99.5%	X% of the monthly payment
Infrastructure uptime	Uptime of IT infrastructure (systems, devices) shall be maintained as per the threshold level on a monthly basis (24x7) MSI, in discussion with the Authority, shall prepare a list of the systems / devices to be monitored for SLA Note: For calculation of this SLA, in case of cluster/HA implementation, the cluster/HA shall be counted as one unit.	99.98%	Y% of the monthly payment
Security breach / incidents			
Security Breach	MSI to ensure zero security breaches (internal or external) that result in compromise of the security of the data and systems.	0 violations	A% of the monthly payment
Reporting of security breach	MSI to report the security breach to Authority and other relevant bodies, as discussed with Authority, within 24 hours of reported breach along with the detailed analysis	100%	B% of monthly payment
Security incident classification	Incidents shall be classified correctly based on the approved classification criteria in the security incident management policy and process.	>=99% of security incidents classified correctly	C% of monthly payment
Security incident response and resolution	Response and resolution time for Critical, Medium and Low priority tickets	>99% of the issues in the particular	D% of monthly payment

	<table><tr><th>Priority</th><th>Response time (Hrs.)</th><th>Resolution Time (Hrs.)</th></tr><tr><td>Critical</td><td>0.5</td><td>4</td></tr><tr><td>Medium</td><td>1</td><td>8</td></tr><tr><td>Low</td><td>2</td><td>48</td></tr></table> ○ "Response Time" means time taken to acknowledge the tickets. ○ "Resolution Time" means time taken to close the tickets after providing the root cause analysis or resolution of the issue. Root cause report to be sent within 24 hours of reporting / resolution of the ticket. The resolution and/or root cause should be acceptable to the Authority. ○ SLAs to be calculated for each Priority type on a monthly basis	Priority bucket are addressed within time on a monthly basis	
Security Operations			
Update of security patches	Security patches to be evaluated and updated within 24 hours of patch release on all the relevant systems and reported to Authority as per the process	0 violations	A% of monthly payment
Updates of rules, policies, and signatures on security devices (e.g., anti-virus, Firewall, IPS, SIEM, WAF)	Rules, policies and signatures to be updated on respective security devices as per the agreed timelines MSI shall prepare the matrix for updating in discussion with Authority.	>99%	B% of monthly payment
Change Management	Changes to the systems / applications shall be tracked and performed as per the Change management process. Authority approval shall be required for each change as per the change management process.	>99%	C% of monthly payment
Security Assessment	Security assessment to be performed by MSI team before go Live, (independent of implementation team) on a half-yearly basis, and by an external agency	100%	D% of monthly payment

	(appointed by Authority) on a yearly basis		
Closure of vulnerabilities	Vulnerabilities identified during any assessment or reported by any stakeholder need to be closed as per below criticality and timelines: o Critical – within 8 hours of time o Medium – within one week o Low – within two weeks Criteria for classification of vulnerabilities shall be developed and approved by Authority. Any exception in the closure of vulnerabilities shall be approved by Authority. Open vulnerabilities shall be monitored on a regular basis, and any balance opening from previous month shall be considered for SLA calculation in the current month.	99%	E% of monthly payment
Note: Penalty captured above is indicative and need to be updated by Authority as per the payment milestone and criticality of SLA.			

10. City Communication Network

10.1 Overview

Communication being a key driver for implementation of smart city initiatives across the {CITY_NAME}, a robust communication network is one of the key foundational requirements on which future ICT based 'Smart' initiatives shall be designed and built. Accordingly, Authority has decided to establish a citywide network infrastructure that shall act as the backbone for effective implementation of smart city initiatives across the {CITY_NAME}.

MSI is expected to help {CITY_NAME} build a converged network, bringing together different city smart urban solutions on a single foundational network infrastructure. The converged network shall facilitate information exchange between resources and applications across different domains. Key deliverables envisaged are to provide IP connectivity that shall enable the citizens to avail varied services under smart city initiatives.

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. The Authority may go for CAPEX/ OPEX model to implement a secure fiber network backbone across {CITY_NAME}.

The expected benefits to be derived from city network backbone are:

- **Connectivity –** Network that interconnects citizens, government, business and communities.
- **Smartness –** Network that allow better management and control to offer richer application experiences
- **Secure, private and resilient –** Network that is resilient & built considering security standards and best practices with stability in bandwidth provisioning and resilient
- **Efficient –** Network that is capable to deliver the envisaged bandwidth and related services
- **Scalable –** A network that can scale up to cater required bandwidth for deployment of future smart city initiatives

The Authority shall evaluate from various options available for sourcing the network connectivity from telecom service provider or establish its own fiber network in the city. The communication network shall be based on MPLS and/ or equivalent or better network and/ or technology.

The communication network shall be a combination of wired and wireless connectivity, as per city requirements.

10.2 City Communication Requirements

City communication network is an important component of the project and needs very careful attention in assessment, planning and implementation. It is important not only to ensure that appropriate connectivity is provisioned within the required timelines but also ensure that it is reliable, secure and supports the required SLA parameters of Latency, Jitter, Packet Loss and Performance.

- In order to meet the project and SLA requirements as defined in the RFP, the MSI shall provision bandwidth/connectivity requirements phase wise. The network provisioning

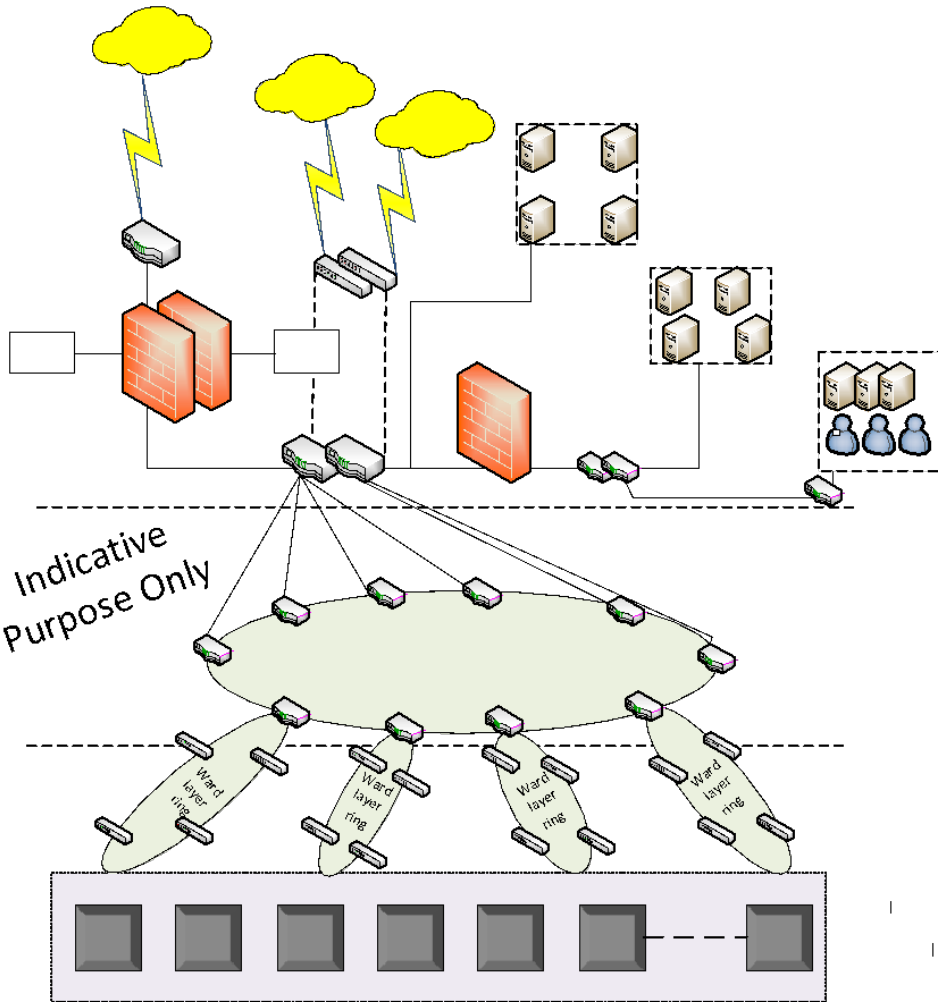
during the project implementation phase is to be taken care of by MSI at no extra cost to the Authority.

- The MSI should provide detailed network architecture of the overall system, incorporating findings of site survey exercise. The network so envisaged should be able to provide real time data streams to the Data Center, DR and ICCC. All the components of the technical network architecture should be as per applicable industry standard.
- The MSI shall prepare the overall network connectivity plan for this project. The plan shall comprise of deployment of network equipment at the junctions/locations to be connected over network, any clearances required from other government departments for setting up of the entire network.
- The network architecture proposed should be scalable and in adherence to network security standards. The last mile connection for IoT devices shall be on proven industry interfaces. Last Mile is to be defined as "the access link from the PoP location – (as per Telco Standards) to the field device".
- The actual bandwidth requirement to cater to the RFP requirements and to meet SLAs would be calculated by the bidder and the same shall be clearly specified in the technical bid with detailed calculations.
- Authority also requires the MSI to meet the parameters of video feed quality; security & performance and thus MSIs should factor the same while designing the solution.
- Authority reserves its right to ask the MSI to increase the bandwidth if the provided bandwidth is not sufficient to give the functionality of the system mentioned in the RFP and to adhere to the SLAs.
- The MSI shall submit detailed installation report for each component of the solution. The report shall be utilized during the acceptance-testing phase to verify the actual quantity of the equipment supplied and commissioned including network bandwidth performance.
- [Note: The City may opt for network connectivity "as a service" instead of own fiber network. However, the Functional aspects shall remain the same The MSI shall ensure the required performance for network and adherence to SLA for the complete project. In case MSI has to sign a contract with Telecom Service Provider(s)and Telecommunication guidelines of Government of India require the Authority to place Purchase Order to the Telecom Service Provider for bandwidth, Authority shall do so.]

10.2.1 Design Guideline

The overall network architecture is envisaged to be implemented in a three-tiered architecture.

The 3-tier architecture mentioned below is indicative and the bidder is required to propose its own architecture in the technical bid.



The envisaged layers of the City Communication Network are:

a) **Core Layer:** The Core layer shall form the backbone of the city communication network consisting of Compute, storage, application, links and connectivity to be established at the ICCC. This layer shall enable all applications hosted at ICCC to be accessed over the backbone for consumers and users. Core layer shall form the point of aggregation for all the traffic coming from the aggregation layer. The core shall adhere to ITU-T G.655 standards or any latest applicable standards.

b) **Aggregation Layer – Zone Level:** The aggregation layer is envisaged at Zone level. The traffic coming from respective wards shall get aggregated at the Zone level. A resilient and NSPOF design shall be proposed and implemented by the MSI to ensure high uptime. The aggregation layer shall further connect to the Core layer for forwarding the traffic to the Core layer.

c) **Access Layer –Ward Level**: The Access layer shall be formed at the wards of {CITY_NAME}. All the wards in the respective zone shall form individual rings to establish redundancy. The access layer shall enable the smart city solutions to connect to the network backbone.

d) **Services Layer – Smart City Solution Level**: The Service layer shall be formed at various locations within the city. The service layer shall enable the smart city solutions such as City

Surveillance, City Wi-Fi, Smart lighting, Smart parking, smart traffic etc. to connect to the network backbone.

Indicative locations for deployment of above layers:

#	Item	Deployment location
1	Core layer	ICCC, DC/DR, city operation center, CCC (at various line department's)
2	Aggregation layer	Identified aggregation point as mentioned location in ANNEXURE …. These are mostly zonal and tentatively identified government office buildings. However, MSI may estimate and propose the number of aggregation points as per their final solution design & network sizing.
3	Access layer	Aggregation/Access points to be identified by MSI based on network load and geographical coverage. These may overlap in order to provide required redundancy.
4	Services layer	The services layer is considered to be the edge locations/area where the smart city solutions shall be deployed like: o City Surveillance o City Wi-Fi o Solid waste management o Smart Lighting o Smart traffic o Smart Parking o Public transport system, o Environment sensors o Smart Governance and Citizen Services o [any other smart solution as proposed by the city]

11. ICCC Physical Build Infrastructure

11.1 IT and Non-IT Infrastructure at ICCC, DC, DR, Viewing Center

The MSI shall establish a state-of-the-art ICCC and viewing centers, the indicative key components for the same shall be as follows:

- Video Wall system
- Operator workstations
- IP Phones
- Active Networking Components (Switches, Routers, Firewall etc.)
- Passive Networking Components
- Electrical Cabling and Necessary LED Illumination Devices
- Workstations
- UPS and DG sets
- Access control system
- Building infrastructure management system
- ICCC furniture
- Add/modify

The MSI shall follow applicable standards while designing the ICCC physical build layout. Materials having the adverse impact on the environment and nature shall not be used. The entire design of the ICCC physical build infrastructure must be modular, Flexible, Dynamic, Scalable, Expandable and re-deployable to accommodate any technological changes / future needs which are not envisaged now.

it must be prepared in strict compliance to ISO 11064 i.e. Ergonomic Design of control centers. All applicable ergonomic parameters should be considered covering Lux level as per industry acceptable illumination levels, spatial arrangement for efficient & safe movement of operators within ICCC during normal and emergency situations, Ideal viewing angles (of operators) to ensure little head movement and minimal eye movement.

The MSI shall provide the IT physical build infrastructure at the following locations:

#	Location Type	Location	Approximate Area	Indicative Infrastructure
1	Integrated Command & Control Center (ICCC)	…….	…….SFT	a. Video Wall, size …..” in …..matrix
				b. Operator Workstations: …. Nos
				c. Simultaneous Viewing Capability: All live Cameras / smart components feeds coming at the ICCC
				d. Contact Center Workstations: …. Nos

				e. IP Phones: … Nos
				f. non-IT Infrastructure including 24/7 power, Civil/ interior work, Infrastructure Management System- as per requirements
2	Data Center (ICCC premises) / State Data Center (SDC) or any other location as per Authority requirement [For on-prem solution option]	[City]	….. SFT	a. Non-IT Infrastructure including 24/7 Power, Civil/ interior work and infrastructure management system -- as per requirements
				b. Servers Infrastructure
				c. Storage Infrastructure
				d. Data Security Infrastructure
				e. Data center Infrastructure
				f. ICCC and other smart urban applications
3	Viewing Center	Location-n	…….SFT	a. Display Monitor …": No.
				b. Operator Workstation: …. No
				c. Simultaneous Viewing Capability: Any …Cameras/smart component assigned as per jurisdiction
4				d. Non-IT Infrastructure including Power, Civil/ interior work, infrastructure management system

* Any other items as required to be included in the above list provisioned at above mentioned locations.

The building for ICCC shall be identified by the authority. If required, till the time ICCC is operational, MSI is expected to establish ICCC at …. Once the main location is operational, then the MSI shall migrate the partial/temporary infrastructure to the main location The site location for ICCC building is shown below:

[Note: Authority to specify Lat./Long. and the schematic of ICCC building site]

The Data Center shall be located on cloud/ at ICCC premises / State Data Center (SDC) / or any other location as per Authority requirement and city readiness.

1. Data Center developed by MSI should be as per Telecommunications Infrastructure Standard for Data Centers (TIA 942). In case Data center is opted on Cloud, Cloud service provider shall furnish the declaration/ TIA 942 certification that Data center offered are Tier III and above.

11.1.1 Location of Deployment of Smart Components

The geographic distribution of various smart urban components is as below:

(To be finalized by the city as per scope of smart components)

#	System Description	No. of Locations
1	Intelligent Traffic Signals/Blinkers	… Locations
2	Surveillance System (Fixed and PTZ Cameras)	… Locations
3	ANPR Cameras	… Locations
4	Red Light Violation Detection System at Intersection	… Locations
5	Variable Message Display (VMD) Boards	... Locations
6	CCTV Cameras for buses	… Locations
7	Passenger Information System (PIS) for Bus Shelters	… Locations
8	Surveillance System & Passenger Information System (PIS) for Bus Terminals	… Locations
9	Surveillance System for Bus Depots	… Locations
10	Smart Parking System	… Location
11	Environmental Sensors	… Locations
12	RFID Tags for Bulk Generators	… Locations
13	Surveillance System for Secondary Collection Centers, SWM Plant and Vulnerable Garbage Points	… Locations
14	Smart Street Lights	… Locations
15	Wi-Fi	… Locations
16	Emergency Call Boxes	… Locations
17	Viewing Centers (if any as required by the city)	… Locations
18	Data Center (DC)	At … (decided by the Authority) Cloud/On Premise
19	Disaster Recovery (DR) Center	Cloud
20	Respective Line department Command & Control Centers (CCC)	At … (Provide longitude and latitude)
21	Mobile command Center	….(Nos)
22	Integrated Command & Control Center (ICCC)	At … (Provide longitude and Latitude)
23	Add more/modify	

The Indicative list of locations are provided at Annexure …

11.1.2 Assessment, Site Survey & provisioning of field level infrastructure

- Prior to the site clearance, the MSI shall carry out survey of all locations including field locations, DC, ICCC, CCC/viewing centers, route plan for laying of the passive components etc.

The Authority shall be fully kept informed of the results of the survey and the amount and extent of the demolition and site clearance shall then be agreed with the Authority.

- The requisite permissions of Right of Way (RoW) should be sought by the MSI as per relevant regulations. The MSI shall be reimbursed for the fees incurred for the RoW permissions by the Authority.
- The site survey shall include, to a minimum;
    a. The Location of all field systems and components proposed at the junctions, (KML /KMZ file, GML, GeoJSON, GPX,OSM, SHP plotted on GIS platform) including city communication Network Provider's Point of Presence (PoP)
    b. Identification of height and foundation of Cameras, Traffic Signals and Standard Poles for Pedestrian signals, Height and foundation of Poles, cantilevers, gantry and other mounting structures for field devices.
    c. Design of Cables, ducts routing, digging and trenching, Network layout plan etc.
    d. Electrical power provisioning
    e. Data Centre design/ICCC design

Road signs

All existing road signs which are likely to be affected by the works are to be carefully taken down and stored. Signs to be re-commissioned shall be cleaned, provided with new fixings where necessary and the posts re-painted in accordance with Authority guidelines. Road signs, street name plate, etc. damaged by the MSI during their operation shall be repaired or replaced by MSI at no additional cost.

Electrical works and power supply

The MSI shall directly interact with electricity/ other utility companies in the city for provision of electrical power supply and other clearance at identified locations in the city. The Authority shall be responsible to pay the electricity bills including recurring charges etc. to the electricity board directly. MSI should consider all the necessary equipment's/components/systems required for raw power conversion and stabilization as part of the overall proposed solution.

Lightning-proof measures

The MSI shall comply with lightning-protection and anti-interference measures for system structure, equipment type selection, equipment earthing, power, signal cables laying.

The MSI shall describe the planned lightning-protection and anti-interference measures in the As-Is report. Corresponding lightning arresters shall be erected for the entrance cables of power line, video line, data transmission cables.

The Internal Surge Protection Device for Data Line Protection shall be selected as per zone of protection described in IEC 62305, 61643-11/12/21, 60364-4/5. Data line protection shall be used for security systems, server data path and other communication equipment. Data line protection shall be installed as per zone defined in IEC 62305.

Earthing System

The entire applicable IT infrastructure i.e. field locations/traffic junctions and ICCC/CCC/DC/DR shall have adequate earthing. Further, earthing should be done as per local/state national standard in relevance with IS standard.

- Earthing should be done for the entire power system and provisioning should be there to earth UPS systems, Power distribution units, AC units, etc. Authority 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.
- 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.

Junction boxes/Poles

- The MSI shall mount the field sensors like the cameras, traffic sensors, environmental sensors and traffic light aspects, active network components, controller and UPS at all field locations on poles, cantilever, Gantry as the case may be.
- (If applicable) At selected traffic junctions, the infrastructure of poles and cantilevers shall be provided by the Authority for mounting/installing the traffic light aspects. The details of such traffic junctions/locations are provided in Annexure ….
- The Junction Box needs to be appropriately sized in-order to accommodate the systems envisaged at the Junctions. The Junction Box for UPS with Battery bank needs to be considered separately. MSI shall ensure the Junction box design keeping in mind the scalability requirements of the project.
- The junction box should be designed in a way that, separate compartment shall be available for separate system (i.e. ITMS Controller, Mini server, Active component, etc.). Each compartment shall have lock & key facility. There should be provision made to integrate the systems if required.

Cabling

- The MSI shall provide standardized cabling for all devices and subsystems in the field.
- MSI 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.
- 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.
- Cabling must be carried out per relevant BIS standards. All cabling shall be documented in a cable plan by the MSI.

12. Domain Use Cases

12.1 Indicative /Partial List of Use cases

ICCC are intended to be the brain and nervous system of the city for monitoring & managing various key functions. ICCC in {CITY-NAME} shall be driven by following use cases to deliver specific outcomes for various departments and stakeholders of the city.

Following indicative use cases shall be enabled by the ICCC:

[City to add/ modify/ select from this indicative list]

#	Use Case	Description
1	Automatic Number Plate Recognition (ANPR)	It should be possible to capture the number plate of two wheeler and four wheeler vehicles. o Read and convert the license plate number into a text string of the vehicle with 95% detection accuracy. o Store the JPEG image of the license plate in the database with other metadata such as time stamp, location, camera, etc. o Classify the vehicles in categories such as four-wheeler light and heavy motor vehicles, three wheelers, auto rickshaws and two wheelers o Detect color of the vehicle (in day time) o Set separate recording duration for event information (number plate as text), media clips (pre and post event recording) and ANPR picture snapshot.
2	Suspect Vehicle Detection	It should be possible to store the number plates of the vehicles under various lists such as stolen, suspicious, blacklisted, etc. The analytic should detect such vehicles in the field of view of the cameras in real time by matching the number plate.
3	Vehicle Search	Platform should provide the feature to search the vehicles based on the number plate (partial or full), class of the vehicle (four-wheeler light and heavy motor vehicles, three wheelers, auto rickshaws and two wheelers, etc.), color of the vehicle and location.
4	Vehicle Detection	Platform should detect and generate an alert for various cases as mentioned below: o Detect the vehicle which stops in a patch of the road and halts more than the user configurable duration o Detect the congestion on the road due to vehicle pile-up.

		○ Detect the vehicle stopped on the road in the no parking zone for more than the user configured duration ○ Detect the vehicle moving in the wrong way for the configured patch of the road ○ Detect polluting vehicles on the road emitting unusual black or white smoke
5	Speed Violation Detection	Platform should detect the speed of the vehicle. The platform should have following minimum features: ○ Capable of detecting speed of vehicles up to 250 kmph. The solution should be certified in India by reputed Indian test laboratory. ○ Ability to apply speed limits based on the vehicle category and generate an incident when the vehicle violates the speed limit with number plate of the vehicle. ○ Ability to define pre and post event video clip and the availability of at least three snapshots associated with the event. ○ Allow the operator to flag the event for storing the event perennially. ○ Record and store the continuous video of the speed detection cameras. ○ Ability to assign overview evidence camera with speed camera which should capture the violating vehicle in the field of view which covers at least three lanes. ○ Set separate recording duration for event information (number plate as text), media clips (pre and post event recording) and ANPR picture snapshot.
6	Red Light Violation Detection	Platform should have the following minimum capabilities: ○ Capture the License Plate of the vehicles violating the red light or stop line when the signal is Red. ○ Provision to either detect red light status by taking the signal feed from the traffic signal controller or by video analytics method using an evidence camera. The evidence camera should record the evidence snap showing the violating vehicle and the traffic signal status. ○ 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. o Functionality export the violation evidence with water mark and encryption as per the techno-legal requirements. o 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 control room. It should be possible to intimate the incidence in real time through SMS to the designated mobile phone. o Allow mapping of multiple ANPR cameras to a single evidence camera associated with the traffic junction. o The system should allow restricting an operator to a single or multiple traffic junction/s and associated cameras. o Set separate recording duration for event information (number plate as text), media clips (pre and post event recording) and ANPR picture snapshot.
7	Free Left Blocking	The platform should have the following minimum features: o Detect the vehicle blocking the free left traffic wherever it is allowed. o Capture the number plate of the vehicle blocking the free left traffic from the front side. o Generate an automatic alert with the details of the vehicle blocking the traffic.
8	No Helmet Detection	Capture image of two-wheeler rider not wearing helmet. Provide Automatic Number Plate Recognition (ANPR) of violating vehicle with auto-localisation and OCR conversion. Capability to detect the no helmet instance for the rider and the pillion. Differentiate between a helmet and various other conditions such as the bald head, person covering the

		head with a cap or dupatta or pagdi, or any other headgear. Differentiate between the person sitting on the motor bike and the pedestrian in the close proximity of the motor bike. Detect the speed of the motor bike. Identify and eliminate non-standard crash helmets like industrial safety helmets, sports helmets (cricket, cycling, etc.) and treat them as no helmet instance.
9	Triple Ride	Capture image of two-wheeler along with the riders riding triple seat Provide Automatic Number Plate Recognition (ANPR) of violating motor bike with auto-localisation and OCR conversion. Detect the No Helmet violation for persons riding in triple ride.
10	No Seatbelt Detection	The platform should detect the following use cases along with the license plate of the vehicle captured. Capture driver and/or front passenger who is not wearing a seatbelt. Provide Automatic Number Plate Recognition (ANPR) of violating vehicle with auto-localisation and OCR conversion.
11	Driver on Phone while driving	Capture driver who is talking on cell phone while driving by holding the phone to the ear. Provide Automatic Number Plate Recognition (ANPR) of violating vehicle with auto-localisation and OCR conversion.
12	Vehicle Classification and Counting	The platform should classify the vehicles based on the categories such as four-wheeler light and heavy motor vehicles, three wheelers, auto rickshaws and two wheelers. The platform should also count vehicles based on the categories and should store the results in the database.
13	Crowd Detection & Headcount	The platform should have the capability of detection of a crowd within the Field of View of the camera. It should be possible for the operator to define the number of persons for the crowd definition. The platform should generate the crowd formation alert with estimate of the number of persons in the crowd based on the headcount.
14	Sudden Commotion in the Crowd	The platform should have the capability of detection of a crowd within the Field of View of the camera.

		The platform should generate the alert when there is a sudden commotion in the crowd.
15	Fighting Detection	The platform should detect two or more persons involved in violent fighting in the field of view of the camera. The platform should generate an alert upon detection
16	Person Falling Detection	The platform should detect the person falling all of a sudden in the field of view of the camera and does not get up within the pre-configured duration of time. The platform should be able to detect one or more persons falling simultaneously.
17	Smart Archived Video Search	It should provide the feature to select a region within the field of view of the camera to show only the frames pertaining to the motion detected in the selected region. The search feature should allow the operator to view the thumbnails of the recorded video to quickly locate the area or incident or object of interest in the scene. The segment of interest within the thumbnails should be further drilled down to another set of thumbnails with lower interval. This drill-down of thumbnails should allow the operator identify the segment of interest quickly. The software should allow the operator to demarcate a person in the scene. The operator should be able to select other cameras for search. The matching attribute search results should be displayed in a grid. The system should allow the operator to search an object by demarcating the object on screen. The analytics should search the video and quickly show the video clip to indicate who left the object in the scene. The system should have built-in tool to summarize the selected video segment and reconstruct the moving objects in the summarized video with a time stamp indicated on each moving object. The operator should be able to click on the time stamp and the system should start the playback video from that time stamp. The video scrubbing tool should show the thumbnail images as the operator moves the cursor on the timeline. The system should have a tool which shows the alerts generated on the selected camera in the alerts timeline.

		It should start playing the pre and post video of the event and jump to the next event. This should allow the operator to investigate the events on a camera for a particular time – event-by-event.
18	Investigation Scene Rebuilding	It should be possible to select the cameras for synchronized and simultaneous archived viewing. It should be possible to record the videos being rendered from these cameras into a single video. Such a single video should support up to eight such cameras in vertical, horizontal or overlay fashion. An easy feature of cloning the time stamp from one camera to multiple other cameras for synchronous archived viewing should be available. For quick investigation of the alerts, it should be possible to configure cameras in small functional group(s). In case of an alert in any one camera in the group, live video from other cameras in the group should be popped up automatically on the operator screen.

(Example) Other use-case with Cross-domain Dataset:

Domain	Use Case	Cross Domain Dataset
Parking	Commercial viability of a parking lot based on geographic profile, like movie theatres, highly rated restaurants, markets and other high-footfall places in the area.	Parking location, POI, rating, hours, weekdays, holidays, user ratings
	Public parking slot availability prediction	Historical parking data, weather, event, holidays, GIS
	Prediction of expected waiting time for next parking availability	Historical parking data, weather, event, holidays, GIS
	List of Vehicles parked for abnormally long time	Times series data for parking occupancy
Mobility- Traffic	Traffic-Accident predictions	Historical accident data, road geometry, weather, GIS
	Predicting Traffic jams	Historical data, traffic flow, weather, GIS, ECB data, Dial 100 data
	Traffic Congestion Trend Analysis: Forecasting of traffic congestion at Junction / Areas/ Roads based on historical data.	Traffic flow data (Junction volume count/ junction delay/ queue length)

	Estimating pollution because of traffic on the road	Traffic flow data (VKT approximation), environmental sensor data
	Green Corridor creation during emergency, visits	Request from ICCC, ATCS API
Waste Management	Bin Pickup Readiness Prediction Classification (i.e. next day prediction)	Historical Data, GIS
	Bin Pickup Readiness Prediction Regression (i.e. next 7 days prediction)	Historical Data, GIS
	Route Optimization	Bins Data with location, Traffic API, Vehicle location
Safety and Security	Crisis Management	Point of Interest, Tweets, Traffic, ECB Data, Dial 100 API
	Crowd Management	Point of Interest, Tweets, Video Feed, Traffic, ECB Data, Dial 100 API
Smart Water	Estimating water needed for a day -	Water consumption data, leakage data, outage data, weather data, water quality data
Flood Modelling	Flood risk assessment due to rain at different locations on the road network	Lat-long, sensor data, weather data
	Flood risk assessment due to cloud-burst, Tsunami	Lat-long, sensor data, weather data
Video Analytics	Identifying car with high speed	Speed violation data with car plate and lat-long
	Red Light Violation Detection	Red light violation data with car plate and lat-long
	Identifying car moving in wrong direction	Traffic camera feed
	Identifying car color	Traffic camera feed
	Identifying if car is a Taxi	Traffic camera feed
	Object Identification and its application on Bin pickup monitoring, thief monitoring	AVLS data
	Facial Recognition and identification	FRS data, criminal database
	Prevent crowd gathering beyond permitted threshold	People count, modeling data
	Trash or road not clean	Image as well as service request details from citizen

		app/ portal, Service Management API
Sensor Data	Identifying malfunctioning sensors and data noise removal	
	Forecasting model for parking occupancy, noise, temperature, AQI, ambient light based on time series model	time stamp, lat-long, observed value; weekdays; holidays; hour of the day
	Lighting Policy based on sunlight/ambient light	time stamp, lat-long, observed luminosity value
Social (Text Analytics)	Twitter Sentiment Analysis	Tweets
	Crisis Management	POI, Tweets, Traffic
	Analytics for blog; sentiment, key points, user comments	Blogs, news
Urban Resilience	Solid Particles Dispersion Modeling	chemical data, meteorological data, location, source strength
	Heavy Gas Plume Modeling	
	Heavy Gas Puff Modeling	
	Light Gas Plume Modeling	
	Light Gas Puff Modeling	
	Model which integrates all of the above models and automated model selection and prediction	
	Model to predict gas leak location etc. in relation with environment sensor data	
	Pool Fire Modeling	
	Jet Fire Modeling	
	Fire Ball Modeling	
	Estimating outflow due to total pipe rupture	
	Estimating outflow of pressurized liquefied gas	
	Estimating Highway Pollution levels because of vehicle movement	Traffic, vehicle type, meteorological data
	Estimating Highway Pollution because of vehicle movement integrated with traffic API	Traffic API, vehicle type, meteorological data

Annexures-Advisories/ Guidelines/ Standards

The list of annexures in this document are as given below:

i. Annexure I- Office Memorandum - Implementation of PAN city smart solutions
ii. Annexure II- Cyber Security Requirement for Smart City- Model Framework
iii. Annexure III- Advisory - Preparing DPR/RFP for pan city smart solutions
iv. Annexure IV- Promotion of Payments through cards and digital means in the Smart Cities
v. Annexure V- Advisory No.6: Strategy for Smart Health in Smart Cities Mission
vi. Annexure VI- Advisory No.7: Role of Infrastructure and Communication Technologies (ICT) in the development of smart infrastructure
vii. Annexure VII- Advisory No.10: Laying of Common Duct for OFC network in Smart Cities on Public Private Partnership (PPP) DBOT Hybrid Annuity Model
viii. Annexure VIII- Advisory No.11: Strategy for ensuring Universal Access IT systems to empower citizens with disability to access these systems with ease
ix. Annexure IX- Advisory No.12: Setting up smart classrooms in Government schools in the 100 smart cities under Smart Cities Mission
x. Annexure X- Advisory No 18: Implementation of Pan-city ICT solutions/Integrated Command and Control Centers (ICCCs) in Smart Cities
xi. Annexure XI - List of MeitY provided core infrastructure services (Ready to be integrated with new/existing solutions)

Annexure I- Office Memorandum - Implementation of PAN city smart solutions

K-14012/101(02)/2018-SC-III-A
Government of India
Ministry of Housing & Urban Affairs
SC-III-A

Nirman Bhawan, New Delhi
Dated : 3rd April, 2018

OFFICE MEMORANDUM

Subject: Implementation of PAN City Smart Solutions –reg.

This is in continuation of Advisory No. 2 issued on 30th June 2016 for "Preparing DPR/RFP for Pan City Smart Solution", Advisory No. 7 dated 27th February, 2017 on "Role of Information and Communication Technologies (ICT) for Development of Smart Infrastructure", Office Memorandum No. K-15016/61/2016-SC-I dated 20th May, 2016 on "Cyber Security Model Framework for Smart Cities" and D.O. Letters dated 27th April, 2017, 18th September, 2017 and 28th November, 2017.

2. PAN City Smart Solution is one of the strategic components under the Smart Cities Mission. The Cities are implementing the PAN city Smart Solutions in an integrated manner through Integrated Command and Control Centre (ICCC). In this regard, it is reiterated that while preparing the DPR/RFP for ICCC, the cities may take adequate precaution to ensure wider industry participation. It is also reiterated that the DPR/RFP may be based on the outcomes to be achieved and are Technology/Vendor neutral.

3. The objective is to develop such use cases which are relevant to the city requirements and are based on reliable technology framework. Therefore, while preparing the DPR/RFP, it may be ensured that the technical requirements/specifications are functional in nature and non-restrictive. The bidder's Proposal may be evaluated on the basis of the merit of the solution proposed, focused on outcome.

4. It may also be kept in mind that the Pan City Smart solutions proposed adhere to future scalability, Technology neutrality, interoperability, open standard and reliability, apart from following e-Gov standards and guidelines released from time to time.

(Sanjay Sharma)
Under Secretary to the Govt. of India
Tel:- 23061081

To

The Principal Secretaries of Urban Development of all States/UTs.

K-15016/61/2016-SC-I
Government of India
Ministry of Urban Development

Nirman Bhawan, New Delhi
Dated: 19th May 2016

OFFICE MEMORANDUM

Subject: Cyber Security Model Framework for Smart Cities.

The undersigned is directed to convey that the National Security Council Secretariat, Government of India in consultation with the Industry (NASSCOM, DSCI) has prepared a Cyber Security Model framework which consists cyber security requirements which may be necessary to be incorporated while inviting proposals/offers from the companies implementing Information Technology and applications as part of project on Smart Cities. A copy of the Cyber Security requirements is enclosed.

2. It is requested that this Model framework may be considered while implementing solutions for setting up Smart Cities.

Encl.: As above.

(Sanjay Sharma)
Under Secretary to the Government of India
Tel. No. 23062908

The Principal Secretaries (UD)/
State Mission Directors/Municipal Commissioners
in respect of 98 Cities

Copy to:

1. PPS to AS (SC)
2. PS to JS (AMRUT)/JS (W&H)/JS (SBM)
3. PS to Director (SC-I)/Deputy Secretary (SC-III)

Annexure II- Cyber Security Requirement for Smart City- Model Framework

NATIONAL SECURITY COUNCIL SECRETARIAT
NEW DELHI

Cyber Security Requirement for Smart City – Model Framework

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

The reference architecture of Information Technology (IT) infrastructure in Smart city suggested by National Institute of Standards and Technology (NIST) serves as a common starting point for system planning while promoting interoperable functional building blocks, which are required in a smart city.

2. The message exchange between various applications in the smart city should be fully encrypted and authenticated. Any application outside the Data Centre (DC) should talk to the applications hosted in the datacenter through only predefined APIs.

3. While it is necessary to converge multiple infrastructures into one Central platform for ease of management, it is mandatory that such applications hosted in the central data center support multi-tenancy with adequate authentication and Role based access control mechanism for each tenant pertaining to their respective infrastructure.

4. In multi-tenant architecture, there should be provisions for flow of normalized data only to respective tenant partition(s) in a predefined manner with adequate authentication and encryption mechanism.

5. The smart city architecture should be capable of managing heterogeneous data, which would be continuously communicated through numerous devices following different protocols. In order to ensure that the flow of data between devices does not run into latency issues, appropriate protocols need to be deployed so as to minimize latency. The following communication protocols could be used for the different layers for data flow:

Between applications and back end systems: HTTP, SQL, FTP, SNMP, SOAP, XML, SSH, SMTP

Between back end systems and field devices: Message Queue Telemetry Transport (MQTT), XMPP, RESTful HTTP, Constrained Application Protocol (CoAP), SNMP, IPv4/6, BACnet, LONworks, Low Power Wide Area Network (LoRa), Fixed, 4G/5G, Wi-Fi, WiMax, 2G/3G From field devices: ZigBee oIP, ETSI LTN, IPv4/6, 6LowPAN, ModBus, Wi-Fi, 802.15.4, enOcean, LoRA, RIFID, NFC, Bluetooth, Dash7, Fixed, ISM & short-range bands.

6. Data Layer (termed as City Digital platform/ fabric) should be capable of communicating with various types of sensors/ devices and their management platforms/applications for single/multiple services irrespective of software and application they support. Data exchange between various sensors and their management applications must strictly happen through this layer, thus making it one true source of data abstraction, normalization, correlation and enable further analysis on the same. Adequate security checks and mechanisms as described in later points to be deployed to protect data layer from data confidentiality breach and unauthorized access.

7. The entire Information Technology (IT) infrastructure deployed as part of Smart city should follow standards like – ISO 27001, ISO 22301, ISO 37120, ISO 3712, ISO 27017, ISO 27018, BSI PAS 180,BSI PAS 181, BSI PAS 182, for Wi-Fi access – PEAP (Protected Extensible Authentication Protocol), 3rd Generation Partnership Project (3GPP), etc. as appropriate.

8. Application Program Interfaces (APIs) should be published and the IT systems be running on standard protocols like JSON / XML or REST etc.

9. From a network security perspective all information that flows on the network should be encrypted to ensure safety and privacy of confidential data. The devices at each endpoint of the network should be authenticated (using mechanisms based on attributes one of which could use passwords). The authentication system so used on these endpoint devices should ensure that only authorized users are sending data over the network, and there is no rogue data that is sent to the control systems to generate false alarms or sabotage the systems.

10. Wireless broadband plan and architecture for the specific City may be prepared detailing the existing Fiber System and other supporting infrastructure so as appropriately interfacing another or citywide wireless network.

11. All sensors deployed as part of IT and IT based systems in the Smart cities should talk only to the authorized wireless network, and do not hook on to the rogue networks. The guidelines to secure wi-fi networks as published by Department of Telecom must be followed.

12. Wireless layer of the Smart City Network should be segmented for public and utility networks by using Virtual Private Networks (VPNs) or separate networks in the wired core, so that any traffic from the Internet users is not routed into the sensor networks and vice-versa.

13. All traffic from the sensors in the Smart city to the application servers should be encrypted Secure Socket Layer (SSL) and authenticated prior to sending any information. The data at rest and in transit must be encrypted.

14. Authentication of sensors in the Smart city should happen at the time of provisioning the sensors, and adding them into the system, and should be based on physical characteristics of the sensors like MAC ID, Device ID etc.

15. Sensors deployed in solutions to set up Smart city should be hardened devices with the ability to be upgraded remotely for firmware through encrypted image files.

16. As various sensors use multiple protocols to communicate with the underlying network with varied security capability, the system should allow provisioning necessary

authentication and encryption at the gateway or the nearest data aggregation level if the sensor is not able to do the same.

17. The Sensors or edge device deployed in Smart city should not have any physical interface for administration. Monitoring of systems and networks should be undertaken remotely.

18. The sensors deployed in Smart city should be of low power consumption and should work on self-sufficient power sources.

19. All devices and systems deployed in Smart city should be hardened and have the ability to be upgraded remotely for firmware through encrypted image files with authentication mechanism to complete the operation.

20. All the sensors in the Smart city should connect to a completely separate network.

21. The data center should be segmented into multiple zones with each zone having a dedicated functionality e.g. all sensors for one operational domain can connect to the data center in one zone, and the Internet facing side of the data center should be in another zone.

22. The Internet facing part of the data center should have a Demilitarized zone where all the customer application servers would be located that are customer facing. Only these servers can access the data from the actual utility application servers on predefined ports.

23. The customer application servers should be accessed only by the web server that is hosted in a different zone of the data center.

24. The following should be implemented in the data centre - firewalls, Intrusion detection & Intrusion prevention systems, Web Application Firewalls, Behavioral analysis systems for anomaly detection, Correlation engine, Denial of Service prevention device, Advanced Persistent Threat notification mechanism, Federated Identity and access management system, etc.

25. Security Information and Event Management (SIEM) monitoring on all Smart City networks, devices and sensors to identify malicious traffic.

26. All "applications" and "apps" will undergo static and dynamic security testing before deployment and be tested with respect to security on regular basis at least once in a year.

27. All applications and "Apps" deployed as part of Smart city be hosted in India.

28. The said architecture provide:

(a) Automatic and secure updates of software and firmware etc.

(b) All systems and devices should provide auditing and logging capabilities.

(c) Ensure vendor compliance to remove any backdoors, undocumented and hard cored accounts.

(d) End-to End solution should be provided with annual end-to-end service availability of 99.999 percent. The end to end service agreement should be in place for minimum period of five years form the date of operations of the systems.

29. Appropriate teams may be set up to monitor cyber incidents and mitigation of same.

30. All the information on incidents be shared regularly with Indian Computer Emergency Response Team (CERT-In) and NCIIPC (National Critical Information Infrastructure Protection Centre) and take help to mitigate and recover from the incidents.

Annexure III- Advisory - Preparing DPR/RFP for pan city smart solutions

Ministry of Urban Development
Smart Cities Mission

Advisory No. 2 — **30th June, 2016**

Subject: Preparing DPR/RFP for Pan City Smart Solutions.

1. Pan city development envisages application of IT to improve, Governance, delivery of Public Service and Infrastructure in Smart Cities. Smartness means applying frugal innovation, building on existing infrastructure and service to get more out of them, making better use of resources etc. The DPRs/RFPs for Smart Solutions for the States will be developed by the PMC. While preparing the DPRs/RFPs, the Cyber Security Model framework circulated vide this Ministry's OM No. K-15016/61/2016-SC-I dated 20th May, 2016 should be incorporated.

2. Based on model RFP prepared by DietY, the broad Scope of Work will include:

i. Preparation of DPR
ii. Carrying out Business Process Re-engineering (BPR)
iii. Development of Technical Requirements and Solution Design
iv. Bid Process Management (Including RFP Preparation)
v. Project Management and Change Management Support
vi. User Acceptance Testing (UAT) Management
vii. Third Party Assessment (TPA)

3. A useful example is the RFP developed by the MMRDA for the Bandra -Kurla Complex (BKC). The BKC model is based on System Integrator model, including following components.

(a) Smart BKC Street Infrastructure setup

(b) Public Wi-Fi and related wired network infrastructure
i. Free outdoor public Wi-Fi
ii. Paid premium outdoor public Wi-Fi
iii. Wi-Fi and Wired Internet access at MMRDA exhibition grounds

1

(c) Smart Parking with 'Parking Management and Guidance System' and related street infrastructure

i. Smart Indoor Parking
ii. Smart Outdoor Parking
iii. Smart Street Parking

(d) Citizen Mobile Application and Online Citizen Portal

(e) Integrated Building Monitoring System Dashboards (Integrating information from BKC buildings and creating information dashboards)

(f) Environmental Indicators Dashboards and related Street Infrastructure

i. Noise Sensors
ii. Air Quality Sensors
iii. Weather Sensors

(g) Integrated Industry Standard Open Platform

(h) A Centralized Command and Control Center for centralized monitoring & decision making related to:

i. Network and Security Management Solution
ii. Centralized System Security Solution
iii. Core Computing and Data Processing infrastructure
iv. Integration with Third Party Shared Services
v. Managed hosted Data Center (DC)
vi. Private Cloud based Disaster Recovery (DR)

(i) Comprehensive Project Management Solution -web-based

(j) Convergence Points

i. Video Surveillance
ii. Intelligent Streetlights

4. The broad scope of work, output and deliverables mentioned above are only indicative and given for facility of reference. Each City may need to customize them as per their actual requirements. All the above documents are also available on the Mission website.

2

Annexure IV- Promotion of Payments through cards and digital means in the Smart Cities

Smart City

Ministry of Urban Development

Smart Cities Mission

Advisory No. 4 18th July, 2016

Subject: Promotion of Payments through cards and digital means in the Smart Cities.

1. The Cabinet Secretariat vide its Order dated 1st April 2016, constituted a Task Force under the chairmanship of Secretary, Department of Investment & Public Assets Management (DIPAM) for ensuring implementation of the Cabinet decisions on promotion of payments through cards and digital means.

2. The Task Force is of the considered view that the digital infrastructure proposed in smart cities, should ensure sufficient touch points that facilitate digital payments for goods and services offered in smart cities. Smart cities may, therefore, include digital payments infrastructure requirement while sizing up their infrastructure requirements. Software/Applications for various services, e.g. integrated transport network, utilities, etc. in smart cities should facilitate multiple digital payment options at no extra cost to the customer.

3. Pan city development envisages application of IT to improve governance, delivery of public services and infrastructure in Smart Cities. Smartness means applying frugal innovation, building on existing infrastructure and services to get more out of them, making better use of resources, etc. All cities are, therefore, advised to take into consideration decision of the Task Force and ensure inclusion of sufficient touch points along with necessary infrastructure to facilitate digital payments for goods and services offered in smart cities.

Annexure V- Advisory No.6: Strategy for Smart Health in Smart Cities Mission

Ministry of Urban Development

Smart Cities Mission

Advisory No. 6

Subject: Strategy for Smart Health in Smart Cities Mission.

1. One of the purposes of the Smart Cities Mission is to improve quality of life, especially of the poor, in order to make Smart Cities inclusive in nature (Guidelines 2.6). At present, private out of pocket expenses (OOPE) on health comprises 64% of total health spending in India. Generally, health related expenditure consists of – medicines, diagnostics and consultation. Compared to a rural household, an urban household spends 5 times more on diagnostics, 2.6 times more on medicines and 2.4 times more on doctors' fees. Therefore, reducing high OOPE incurred by urban residents, especially the slum dwellers, leads to more inclusive cities.

2. The strategy of Smart Health is based on the providing cheaper doctor consultation, reasonably priced medicines and affordable diagnostics. This can be done by converging different schemes. The Figure 1 gives the convergence of three schemes of Government of India with programmes of State Governments:

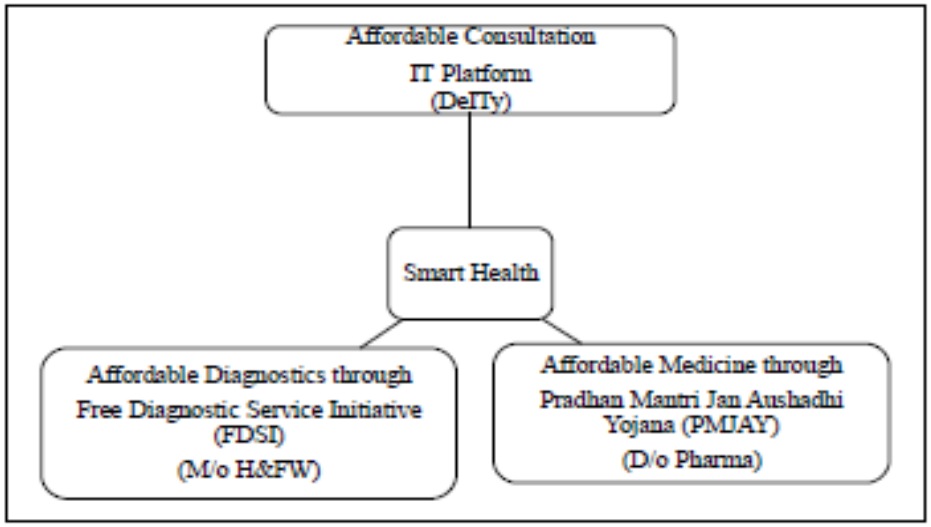


Figure 1. Smart Health convergence of programmes

- Consultation through IT Platforms: For instituting round-the-clock doctor consultations, a unique version of telemedicine can be designed by establishing an IT platform to match patients and doctors, bringing convenience to patient doorstep. Doctors volunteering for this programme, will provide services to patients on their mobile phones. For this purpose, the Smart Cities may develop special apps or use existing apps. The instituted apps and/or the IT platform will link general physicians and specialists in hospitals to patients in slum localities for online consultation. The app may have an instant messaging service for simple medical queries.

- Delivering affordable quality medicines: Pradhan Mantri Jan Aushadhi Yojana (PMJAY) scheme of Department of Pharmaceuticals, Ministry of Chemicals and Fertilizers can be used to provide affordable, quality generic medicines. Many States have their own schemes for giving free medicines also.

- Delivering affordable Diagnostics: Complementing the free medicine scheme, free diagnostic services can also be made available under a hub-and-spoke model, floated by the Ministry of Health under the Free Diagnostics Service Initiative (FDSI). Under this scheme, a set of essential diagnostic services at each facility level has been identified. Diagnostic tests are allowed to be conducted by private providers (PPP model), empanelled by the Government.

- In the hub-and-spoke model, samples are collected at peripheral facilities/collection centers (including Mobile Medical Units) and safely transported to a central laboratory which will act as the Hub, which can be a District Hospital Lab/Medical College/or a public or private laboratory set up for the purpose.

3. The broad scope of work, output and deliverables mentioned above are only indicative and given for facility of reference. Each city may customize as per their requirements.

Annexure VI- Advisory No.7: Role of Infrastructure and Communication Technologies (ICT) in the development of smart infrastructure

Smart City

Ministry of Urban Development

Smart Cities Mission

Advisory No. 7

Subject: **Role of Information and Communication Technologies (ICT) in the development of 'smart' infrastructure.**

1. The role of Information and Communication Technologies (ICT) in the development of 'smart' infrastructure cannot be over emphasized. A robust communication network & reliable IT connectivity is a prerequisite for creating smart infrastructure across various segments / verticals in the proposed Smart Cities.

2. Based on the advice of Department of Telecommunication (DoT), it is recommended that the following aspects may be taken into consideration while planning and creating such infrastructure:

   i. City wide ducts for robust fibre optic network for reliable communication and IT infrastructure including in-building solutions.
   ii. Adherence to global & Indian standards for smart city communications.
   iii. Adopting solutions that ensure interopenability.
   iv. Smart services across various verticals should necessarily be IP based. DoT has informed that it has already mandated use of IPv6 to all stakeholders including State Governments

3. The principles mentioned above are indicative and given for facility of reference. Each city needs to customize as per their requirements, based on the principles mentioned above.

Annexure VII- Advisory No.10: Laying of Common Duct for OFC network in Smart Cities on Public Private Partnership (PPP) DBOT Hybrid Annuity Model

Smart City

Smart Cities Mission
Ministry of Urban Development

Advisory No. 10 **14th July, 2017**

Sub: Laying of Common Duct for OFC network in Smart Cities on Public Private Partnership (PPP) DBOT Hybrid Annuity Model

In order to have proliferation of broadband in the country, one of the most consistent issues observed is the issue of obtaining Right of Way (RoW). Further, the levies are not uniform and vary from state to state and city to city. While the charging mechanism may vary from one place to another, the common point is that the charges are very high. The time taken to obtain the RoW clearance is too long. Further, un-coordinated development activities such as road expansion, laying of electrical cable, etc are undertaken by multiple agencies and private contractors, result in frequent cuts in cable, leading to depreciated life of the cable and increase in operating costing for service providers.

2. The Smart Cities Mission guidelines para no. 6.2 gives the essential features in a smart city. One such feature is visible improvement in the area (e.g. replacing overhead wiring with underground wiring. In addition, paras 2.4 & 2.5 of the guidelines identify implementation of robust IT connectivity and digitalization as a core infrastructure. It is accordingly envisaged that a common duct for OFC be laid in the smart cities to meet these mission objectives.

3. The Telecom Regulatory Authority of India (TRAI) has carried out a feasibility study for laying of common duct for optical fiber. The report may be referred to at https://smartnet.niua.org and http://smartcities.gov.in. The Smart Cities may carry out the project development exercise such as preparation of technical and financial feasibility and procurement of concessionaire through the smart city PMC.

4. One of the potential models for implementation of the project highlighted in the feasibility study carried by TRAI is 'DBOT Hybrid Annuity'. The key features of the model are as under:

a. **Project funding:** Under this model, the concessionaire shall be responsible to design and develop and finance 60% of the project cost. The remaining 40% of the project cost shall be contributed by the Smart City in five equal installments linked to the project completion milestone.

b. The concessionaire shall have to initially bear the 60% of the project cost through a combination of equity and debt and undertake the construction activity. The balance 40% shall be released by the employer upon utilization of concessionaire's contribution.

c. **Bid Parameter:** The least NPV of the quoted project cost + NPV of Annuity Payment + NPV of the O&M for entire operation period shall be the bid parameter.

d. **Annuity Payment:** The Annuity payment to the concessionaire shall be made for the 60% of the contribution on a bi-annual basis.

e. **O&M:** The concessionaire shall be responsible for the maintenance of the facility during the concession period. The payment towards the O&M shall be paid by the employer bi-annually as per the concessionaire's financial quote. The O&M payment shall be linked with the performance standards w.r.t. O&M subject to inflation index (WPI and CPI in the ratio of 70:30).

f. **Concession period:** The concession period can be 15-20 years (including construction period) depending upon the financial viability assessment.

g. **Revenue:** The right to generate revenue shall remain with the city. However, the concessionaire shall be responsible for assisting the city in various means to monetize the infrastructure.

5. The Smart Cities may take proactive measures to undertake this project so as to make visible improvement in the area and provide robust IT connectivity in the City. The Cities have the flexibility to structure the project as per the techno-commercial feasibility assessment.

****

Annexure VIII- Advisory No.11: Strategy for ensuring Universal Access IT systems to empower citizens with disability to access these systems with ease

Smart City
MISSION TRANSFORMATION

Smart Cities Mission
Ministry of Housing & Urban Affairs

Advisory No. 11 **15th January 2018**

Sub: Strategy for ensuring Universal Access IT systems to empower citizens with disability to access these systems with ease

The objective of Smart Cities Mission (SCM) is to improve the quality of life of citizens living in cities in an inclusive way. Hence it is imperative that all the projects taken up under the Area Based Development and Pan city Smart Solutions should be disabled friendly. Many cities have included disabled friendly features in the RfPs while implementing the infrastructure projects. The disabled friendly features should also be included while taking up the Pan city Smart Solutions such as Integrated Command and Control Centres. All Smart Cities must ensure such features while conceptualizing and implementing the Integrated Command and Control Centre projects.One of the examples is the Integrated Command and Control project being implemented by Naya Raipur Smart City. Some of the important features of the projects are as under.

- All smart city initiatives to have mandatory inclusion of digital accessibility implementation guidelines.
- New Portals/ web sites/ mobile app/ internal application system to have digital accessibility inclusion
- Incorporating accessibility into design phase of new engagement where the citizen centric and internal users is high.

- Mandatory insertions of accessibility requirements specifications while designing DRPs and preparation of RFP for new software procurement system
- Formulating Accessibility requirements while designing new web portal / mobile apps for government client
- Incorporating accessibility may lead in service differentiator for smart cities among all the states in India.
- Build accessibility into designing workflow / system processes.
- Visually impaired people can listen to the websites to use them
- People with color blindness can distinguish content using different colors
- Hearing impaired person can read the video
- People with changing abilities due to aging can use resources easily
- People with motor disabilities can use aids or tools which can help them using devices
- People with cognitive difficulties can understand better with the help of assistive technologies

2. The broad scope of work, output and deliverables mentioned above are only indicative and given for facility of reference. Each city may customize as per their requirements.

****

Annexure IX- Advisory No.12: Setting up smart classrooms in Government schools in the 100 smart cities under Smart Cities Mission

Smart City
MISSION TRANSFORMATION

Smart Cities Mission
Ministry of Housing and Urban Affairs

Advisory No. 12 **3 August 2018**

Subject: Advisory on setting up smart classrooms in Government schools in the 100 smart cities under Smart Cities Mission.

1. Smart Cities Mission statement and Guidelines document prescribes development of core infrastructure elements which comprises one of the strategic component viz. smart solutions for education, to help in providing quality education to students studying in various Government schools in the smart cities. The students exposed to such smart solutions/ ICT technologies in schools will also be in a position to utilize the opportunities provided by these cities.

2. The objective is to bring state of the art education to the students through innovative teaching and learning methods by use of ICT technology. A smart classroom typically includes components like digital textbooks, multi-media contents, smart boards, LED screen, laptops with internet connectivity, Video conferencing system, microphones, amplifiers and speakers, Wi-Fi, document cameras, scanners, school MIS, digital library, 3D printing lab, tele-education, etc.

3. Few of the cities have already taken smart classroom initiatives and are witnessing positive social impact. The same is required to be expanded to Government schools in the 100 smart cities.

4. It is therefore requested that all cities selected under the Smart Cities Mission assess the needs for infusion of technology to improve learning outcomes in Government schools in these cities. Various models of such technology are well established and cities may choose the relevant ones, depending on their specific needs. The selection of projects in the smart cities is the discretion of the cities and hence, the cities are requested to follow suitable processes for initiating action as per this advisory.

5. The components mentioned under point # 2 above are broad and indicative. The cities may customize the same as per their requirements.

*****

Some standards to be followed in the project duration are:

#	Component/Application/System	Prescribed Standard
1.	Information Security	ISO 27001
2.	IT Infrastructure Management	ITIL specifications
3.	Service Management	ISO 20000 specifications
4.	Project Documentation	IEEE/ISO/CMMi (where applicable) specifications for documentation

Apart from the above the MSI need to ensure compliance of the project with Government of India IT security guidelines including provisions of:

a) The Information Technology Act, 2000" and amendments thereof and

b) Guidelines and advisories for information security published by Cert-In/Meity (Government of India) issued till the date of publishing of tender notice. Periodic changes in these guidelines during project duration need to be complied with.

While writing the source code for application modules the MSI should ensure high-quality documentation standards to improve the readability of the software module. An illustrative list of comments that each module contained within the source file should be preceded by is outlined below:

a) The name of the module

b) The date when module was created

c) A description of what the module does

d) A list of the calling arguments, their types, and brief explanations of what they do

e) A list of required files and/or database tables needed by the module

f) Error codes/Exceptions

g) Operating System (OS) specific assumptions

h) A list of locally defined variables, their types, and how they are used

i) Modification history indicating who made modifications, when the modifications were made, and what was done.

Apart from the above MSI needs to follow appropriate coding standards and guidelines inclusive of but not limited to the following while writing the source code -

a) Proper and consistent indentation

b) Inline comments

c) Structured programming

d) Meaningful variable names

e) Appropriate spacing

f) Declaration of variable names

g) Meaningful error messages

Annexure X- Advisory No 18: Implementation of Pan-city ICT solutions/Integrated Command and Control Centers (ICCCs) in Smart Cities

Ministry of Housing and Urban Affairs
Smart Cities Mission

Advisory No. 18 **Date:06th November, 2020**

Implementation of Pan city ICT solutions/Integrated Command and Control Centers (ICCCs) in Smart Cities.

Cities under the Smart Cities Mission (SCM) have undertaken several initiatives in the effort to make their cities 'smart'. Many of the projects being undertaken by the cities include technology interventions under ICT solutions that seek to create a digital layer in urban governance. In order to streamline the process of implementation of technology intensive projects that emphasize the use of IT and ICT solutions, the Mission had earlier issued Advisory no 02 & 07 and OM dated 03rd April, 2018, advising cities on aspects that need to be consideredwhile framing the Bid Documents for such technology projects.

2. In order to encourage 'Make in India' and promote manufacturing and production of goods and services in India with a view to enhancing income and employment, Department for Promotion of Industry, and Internal Trade (DPIIT) has notified the Public Procurement (Preference to Make In India), Order 2017 (PPP-MII) on 15th June 2017,which has recently being amended vide DPIIT order No. P-45021/2/2017-PP(BE-II) Dated 4thJune, 2020.

3. The Mission has been reiterating the importance of 'Make in India' initiative to the cities, wherein for projects funded by the Central Government, Smart Cities SPVs have been advised to ensure adequate competition and provision of level playing field in the procurement / tendering process for domestic players without any discrimination. Accordingly, cities have been advised to insert necessary provisions in the tender documents regarding compliance with PPP-MII provisions for such projects.

4. However, it is seen that complaints of domestic manufacturers / suppliers are being received through DPIIT/ Department of Telecommunications (DoT) and by this Ministry regarding violation of the provisions of PPP-MII Orders in tenders floated by Smart City SPVs. A significant number of these complaints are related to ICCC projects wherein RFPs issued by Smart Cities SPVscontainclauses that limit such provisions and work against

providing a level playing and creating a conducive environment for bidders, especially Indian manufacturers.

5. Some of the complaints received by the Mission are listed below:

i. Provisions of PPP-MII are not being followed in spirit by the cities. Even in Bid Documents where the applicability of PPP-MII is mentioned as a broad statement, the sub-clauses of the tenders restrict their applicability. Regular complaints have been made to DPIIT, Department of Telecommunications (DoT), Ministry of Housing and Urban Affairs (MoHUA) andconcerned smart cities, by the Indian Manufacturers affected by these restrictive provisions.

ii. Restricting Industry Participation- It has been observed that certain technical eligibility conditions as well as product specifications are being included in Bid Documents to restrict participation, to the disadvantage of Indian Manufacturers. This may lead to cartelization by the Bidders and higher project costs for the city.

iii. Many of the Bid Documents prescribe qualifying criteria specifying the Original Equipment Manufacturer (OEM) / Master Systems Integrator (MSI) in multiple sections of the Bid Document (including in technical specifications) in a fragmented manner leading to ambiguity and conflicts.

iv. There is no provision in Bids that give relaxation / support to encourage start-ups and MSMEs, thereby depriving the development of wider vendor base.

v. Restrictive OEM clause- In some cities, the Bid Document specifies procurement of multiple products from a single source OEM.

vi. Restricting acceptance of certification from Indian Certifying bodies/institutions- In many cases, the Bid Documents require certification from International certification organisations, to which many of the Indian Manufacturers have limited access to.

vii. Technical evaluation process (QCBS method of selection)- At times, the evaluation methodology under Quality-cum-Cost Based Selection process is not properly defined,giving marks to bidders in a granular fashion. This may lead to bias and undue benefits to certain Bidders.

6. In the above background, it is advised that the following points may be taken into consideration while framing the Bid Documents for Smart Cities Projects that include implementation of Pan City ICT solutions / ICCC in Smart Cities.

i. Bid Documents may include a provision for applicability of Government of India directives under PPP-MII for projects covered under the scope of the same.It should be ensured that clauses in any part/section of the Bid Document, including Bill of Quantity (BOQ) and specifications, should be in consonance with PPP-MII.

ii. No global tenders may be invited by the Smart City SPVs if the value of procurement of goods and services is less than Rs. 200 crore. Further, any bid condition that is arbitrary, excessively restrictive, or discriminative towards the participation of Indian manufacturers should be avoided. These may, *inter alia,* include:

   a) Qualification criteria requiring performance in countries outside India.
   b) Over prescription ofrequirement for technical and financial eligibility credentials *vis-à-vis* the nature, scope and value of bid.
   c) Restricting the participating to Bidders who are listedwithnon-government global certification entities *vis.*Gartner /IDC/ Navigant/ Forrester/ IHS and others..
   d) Mandatory clauses requiring certifications from global certifying bodies only and not accepting Indian certifications.

iii. While framing the technical specification and BOQ, references to a particular make / brand / technology / system that is unique or proprietary to a single source should be avoided.

iv. The technical/financial eligibility criteria in the RFP should be in alignment with project objectives, project value and skill set requirements for efficient and effective operations of the system, and should avoid over-specifying the same.

v. Smart City SPVs may specify functional requirement to provide level playing field and equal opportunities to prospective Bidders. The system should be based on city-specific use-cases and relevant KPIs

vi. A reasonable methodologyshould be arrived at for defining experience / credentials of the Bidder/OEM *vis.* specifying experience of implementation of minimum quantity of works (as per Bid requirements) in similar projects.

vii. As far as possible, the evaluation criteria should be objective, tangible and supported by a documentary evidence. There should be minimal scope for subjectivity in calculation of scores while evaluating the credentials.

viii. Framing of Bid Documents and Invitation of Bids should be as per Model Bid Documents issued by Central Government / State Government departments, as updated from time to time.

ix. Reasonable opportunity should be given to all prospective Bidders by inviting them for pre-Bid discussions and addressing their queries through timely addendum / corrigendum in the Bid Document.

x. In order to promote Startups / MSMEs, Smart City SPVs may consider reserving certain value of procurement of goods and services through such firms. Necessary relaxations in qualifying criteria, requirement of Earnest Money Deposit in Bids, and other provisions prescribed by Central Government / State Government for promotion of such entities may be considered while framing the Bid Document.

7. Deviation from the above points, having a material effect on the Bidding process, to the extent of being restrictive or discriminative to Indian manufacturers in view of PPP-MII, may be done only after taking prior approval of this Ministry. Proposals for such deviation should be routed through the Head of Department (Additional Secretary / Principal Secretary / Secretary) in the controlling Ministry of the State Government.

***

Annexure XI – Incorporation of e-Gov standards and Policies

A standard is defined as a technical specification, recommended practices or guidelines available to the public, drawn up with the cooperation and consensus or general approval of all interests affected by it, based on the consolidated results of science, technology and experience, aimed at the promotion of optimum community benefits and approved by a body recognized at the national, regional or international level. e-Governance standards prescribe set of rules, conditions or requirements that play an important role in building the architecture of Smart city as well as e-Governance.

The essential requirements of interoperability, security, usability, universal design and reduction in cost can only achieved through standardization and use of standards. The standards should at least comply with the published eGovernance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time).

The table below provides a brief description of the e-Governance standards approved by Ministry of Electronics and IT and also provides guidance on their relevance and usage in RFPs for various Smart City and e-Governance projects.

#	Standard	Description	Target Audience	Mandatory/ Recommended
1	**Standards and Specifications for e-Pramaan: Framework for e-Authentication**	This standard aims at providing guidelines for all central and state ministries, departments and government agencies towards adopting an appropriate authentication model for online and mobile based delivery of public services. It describes broad level specifications for developing the e- Pramaan authentication system. It elucidates the rationale, use cases and process flows to be used for detailed design. It also elucidates the standards that will be used to develop the components, APIs as well as the protocols for the framework.	• Security • Architects • Technical • Consultants • Application • Developers	**Recommended** standard
2	**Biometric Standards**	The Indian Government encourages use of biometric data for identification and verification of individuals in e-Governance applications. The biometric data includes: (a) fingerprint image, (b) minutiae, (c) face image and (d) iris data.	• All e-Governance projects of the Central and State Government or any other Organization which need to comply with this standard for the purpose of interoperability • All Integrators/Service providers for Indian e-Governance applications.	**Mandatory**
		Face Image Data Standards: This standard includes capture and	**Face Image Standards:**	

		storage specifications of face images for human visual inspection and verification of the individuals in Indian e-Governance applications. A possible future use of these images for computer based face recognition is kept in view during the capture and storage. It specifies a format to store face image data within a biometric data record compliant to the Common Biometric Exchange Formats Framework (CBEFF), given in ISO 19785-1. It also includes best practices recommended for implementation of the specifications in different categories of e-Governance applications. This biometric Standards would be applicable to all e-Governance applications in India as per the Government's Policy on Open Standards.	• e-Governance projects rolled out by Central and State • Governments or any other • organization using face images or face photographs. • Organization using face images or face photographs. • Photographers, who capture • facial images for e-Governance • applications. • All Integrators/Biometric Service providers.	
		Fingerprint Image Data Standards e-Government applications using fingerprinting technology deal with fingerprint data at multiple stages. It is possible that different fingerprint capturing devices and software (compression algorithms and matching algorithms) are used at different stages. The purpose of this standard is to ensure interoperability among various fingerprint sensors and algorithms by which the fingerprint images are captured/ stored by standardizing the specifications for fingerprint devices, fingerprint image, storage/transmission and minutiae.	• Vendors of fingerprint devices or software developers for conversion of images to different • Standard formats, quality evaluation software, minutiae • extraction and matching algorithms etc.	
		Iris Image Data Standards This standard ensures interoperability among the e-Governance applications requiring iris recognition, by standardizing iris specifications including the storage and transmission formats. It specifies Iris image data specifications, acquisition, storage and transmission formats. It also includes best practices for implementation of the Standard specifications in different categories of e-Governance applications, based on the volume of	• All those e- Governance projects where identity management is an important • issue e.g., cyber security, defence, counter terrorism • etc. • Vendors of Iris image acquisition devices or software • developers for conversion of	

		data and verification/ accuracy requirements. Thus, to allow the application developer maximum flexibility in usage of algorithms and devices from different vendors and to address interoperability requirements, the iris image must be captured and stored as per standard specifications.	• images as per the Standardized format	
3	**Digital Preservation Standard: e-Governance Standards For Preservation Information Documentation of e-Records (Metadata & Schema)**	The e-Governance standard for Preservation Information Documentation (eGOV-PID) of electronic records provides standard metadata dictionary and schema for describing an electronic record. The e-records have to be preserved in such way that it should be possible to find, read, represent, render and interpret them accurately as original along with all the associated information necessary for its comprehension in distant future. Most of the preservation information (metadata) can be automatically captured using this schema after the final e-record is created, as most of the required information is already present in an e-government system. Such preservation information documentation is necessary only for those e-records that need to be retained for long durations (e.g. 10 years, 25 years, 50 years and beyond) and the e-records that need to be preserved permanently. The implementation of this standard helps in producing a valid input i.e. Submission Information Package (SIP) for archival and preservation purpose.	• E-record producers and data managers • Departmental Record Officers (DROs) record keepers, archivists and preservation officers • All stakeholders in central and state government, as well as public and private organizations involved in execution, design, development and implementation of e-Governance applications. • Central, state, district level archiving organizations	**Mandatory**
4	**Localisation & Language Technology Standard & "Best Practices For Localization of e-Governance applications in Indian**	**Character Encoding Standard** Character Encoding standard aims at facilitating global data interchange in all constitutionally recognized Indian languages and addresses specific areas of Localisation issues. **Fonts Standard** Fonts standard aims at providing a single International Standard to comply with UNICODE data storage. This ensures data portability across various applications and platforms. It **mandates** use of ISO/IEC 14496-OFF	e-Government Services providers in all Constitutionally recognized Indian Languages	Mandatory

	Languages	(Open Font Format) font standard for all 22 constitutionally recognized languages. It resolves the issues faced when mutually incompatible proprietary fonts of different standards are used in Government Offices, causing serious problems in information exchange amongst offices. **Best Practices** "Best Practices For Localization of e-Governance applications in Indian Languages" is available at URL: http://tdil.mit.gov.in/pdf/standards/Best_Practices_for_Localisation_of_e-Governance_Applications_in_Indian_Languages_Ver5.7.pdf "Best Practices for Localization of Mobile web applications in Indian Languages" is available at URL: http://egovstandards.gov.in/sites/default/files/Best%20Practices%20for%20Localization%20of%20Mobile%20Web%20Applications%20in%20Indian%20Languages.pdf These best practices should be followed in development of e-Governance application.		
5	**Metadata and Data standards**	The objective of Metadata and Data standards is to define standards to enable semantic interoperability and management of data. These Standards provide a way for information resources in electronic form to communicate their existence and their nature to other electronic applications (e.g. via HTML or XML) or search tools and to permit exchange of information between applications. Their adoption will enable easier, efficient exchange and processing of data. It will also remove ambiguities and inconsistencies in the use of data.	• All stake holders in Central and State Govt., as well as Public and Private Organizations involved in execution, design, development and implementation of eGovernance applications. • Administrative Governance Providers • Development schemes Providers • Welfare Scheme Providers • Disaster Management Groups etc.	**Mandatory**
6	**Quality Assurance Framework (QAF)**	The purpose of the e-Governance Quality Assurance Framework is to provide assurance that work products (solutions) and processes comply with predefined provisions and plans. It outlines a standard for use by senior administrators, project management personnel, external consultants and vendors involved in	• Policy makers • Administrators • Implementing • agencies • Project managers • Private sector • contractors • Consultants	**Mandatory**

		eGovernance implementation. It indicates the general operational principles and technical aspects that a quality assurance exercise should incorporate when customized to the requirements of a specific eGovernance project. The QAF is linked to the project lifecycle and integrates quality assurance requirements for all the necessary phases that a project goes through. The three principal objectives of quality assurance in eGovernance are: • Ensuring system (in terms of processes, products and services) requirements are defined (Definition) • Ensuring the system conforms to requirements (Verification) • Ensuring user satisfaction with the system, once it goes 'live' (Validation) The 3 objectives of quality assurance in an eGovernance project lifecycle can be achieved through the identification and application of Quality Gates (QG) at various phases of the project. Each QG consists of a set of quality baselines relevant to that project phase and is aligned with relevant IS/ ISO standards. QGS are categorized into essential and desirable. The essential QGs relate to four key areas: • Quality Processes in the Organisation (Gate 1) • Software Quality (Gate 2) \ • Information Security (Gate 3) • IT Service Quality (Gate 4) Desirable QGs relate to such aspects as project documentation, use of recognised standards and architectures, risk management, business continuity planning etc. The QAF will help in developing and maintaining sound relationship between private and public partners in case of PPP (Public-Private-Partnerships). It is also expected to facilitate greater clarity and granularity in RFP and contract		

		conditions as QAF provisions are based on internationally recognised standards		
7	**Conformity Assessment Requirement (CARE) for e-Governance applications**	Conformity Assessment provides an indicator of the degree of compliance of the solution to its requirements. For the purpose of eGovernance, Conformity assessment includes activities like sampling and testing; inspection, review, certification, management system assessment and registration etc. CARE outlines an approach to achieve the objectives of Quality Assurance through: a. mapping the solution architecture of an eGovernance system with CARE b. identifying the Component of Interest in the architecture, c. applying a relevant Quality Gate to the "Component of Interest" and finally d. assessing conformity of "Component of Interest" to the quality standards comprising that Quality Gate. The entire process of identifying Components of Interest and applying Quality gates is termed as Conformity Assessment. The "Component of Interest" is any module of the architecture of an e-Governance system that is intended to undergo a conformity assessment exercise. These modules are defined in the e-Governance Architecture consisting of the user layer, technology layer and organization layer. The level of assurance required on a particular module is based on the needs of the organization. A Quality Gate (QG) is a supporting set of processes which enables controls and assurance to achieve the desired level of confidence. The Quality Gates **should be identified in the RFP/ contract document by the project leader** and may be used for objective evaluation to ensure that the "Components of Interest" are capable of achieving predefined goals.	• RFP Writers • Solution • providers/vendors	M**andatory**

8	**Technical Standards For Interoper-ability Framework for e-Governance** **(IFEG)**	The purpose of these standards is to provide a framework for the selection of Standards to facilitate interoperability between systems developed by multiple agencies. It provides organizations the flexibility to select different hardware and software for implementing cost-effective e-Governance solutions. It, therefore, promotes technology choice, and avoids vendor lock-in. In Interoperability Framework for e-Governance (IFEG), the 'Areas' for e-Governance applications have been categorized under 7 broad domains: • Presentation and Archival • Process • Data Integration • Meta-data • Data Interchange • Network Access and Application • Security The Technical standards for IFEG in India describes technical standards to be adopted for e-Governance application under each of the domain covered under IFEG, as per the Policy on Open standards of e-Governance.	• Project Teams of e-Governance applications in all Departments at Central / State Government level • Contractual Policy framing agencies for development of e-Governance Applications • All integrators/ service providers for Indian e-Governance Applications	**Mandatory**
9	**Software development for Reengineering Cloud**	The eGov AppStore is a common platform to host and run applications (developed by government agencies or private players) at National Clouds under Meghraj, which are easily customizable and configurable for reuse by various government agencies or departments at the central and state levels without investing effort in the development of such applications. The basic need for Software Development and Re-engineering Guidelines is to ensure development of Common Application Software (CAS) which can be configured as per different states / departments requirements without the need of modifying the core code of the application for a faster deployment so that time, effort and costs in developing applications are saved and to obviate duplication of efforts. It is therefore imperative that applications are developed in conformity to guidelines that makes	• Administrator • Implementing Agency • Consultants	**Recommended**

		them standardized and compatible for hosting and running across states. This need has translated in the conceptualization, development and roll-out of productized cloud enabled application which can be centrally run & hosted and are available to states for configuring them as per their relevant processes with minimal customization for rolling out the services in shortest time possible. It is envisioned that an application which is centrally run as a SAAS is easy to roll out to all interested parties at the same time and therefore such application's architecture and design should be compliant to common minimum practices / considerations that will convert it to standard product. A copy of the detailed guidelines http://MeitY.gov.in/sites/upload_files/dit/files/Application_Development_Re-Engineering_Guidelines.pdf		
10	**Policy On Collaborative Application Development by Opening the Source Code of Government Applications**	Government Departments and Agencies both at the centre and states are engaged in developing software applications and most such applications are running successfully in their own premises. However, there may be repetitive work going on. Many applications are being re-developed from scratch without reusing the already existing and running applications in other Departments. In the absence of a common Collaborative Application Development Platform, individual applications developed by Government Departments may end up with the same code being rewritten for similar application functionality, which is already available elsewhere. Lack of sharing of the source code prevents the code from scrutiny, thus denying the opportunity for further improvements. These inefficient practices may lead to wastage of time, efforts and public money, which could have been put to more productive use alternatively. Several hundreds of custom application software are running	• Administrator • e-Governance project teams in all Departments of Central / State Governments • Consultants • Implementing Agency	**Mandatory**

		across Central/ State Government Departments and Agencies, PSUs and urban local bodies. Hosting of the source code of these applications on a single unified platform which can be accessed by Government Departments/Agencies and the general public (with necessary access controls) would result in much faster application development in a better collaborative manner. Hence, GoI has notified "Policy On collaborative Application Development by Opening the Source Code of Government Applications" in the Gazette of India on 14.05.2015. The policy is available at http://www.egazette.nic.in/WriteReadData/2015/164611.pdf Further a Collaborative Application Development Platform is in final stage of development for hosting & sharing the source code with access control. (https://openforge.gov.in/) This policy is not applicable on software applications/ components/ products utilized or implemented for projects/organizations of national strategic importance and for those projects/applications that may have security implications. The policy does not apply to Commercial off the Shelf (COTS) software.		
11	**Policy on Adoption of Open Source Software for Government of India**	Government of India has notified "Policy on Adoption of Open Source Software for Government of India" in the Gazette of India on 02.04.2015 for adoption of Open Source Software in all e-Governance systems implemented by various Government organizations, as a preferred option in comparison to Closed Source Software. (available at URL http://www.egazette.nic.in/WriteReadData/2015/163746.pdf) The Open Source Software shall have the following characteristics: • The source code shall be available for the community/adopter / end-user to study and modify the software and to redistribute copies of either the original or modified software.	• Administrator • e-Governance project teams in all Departments of Central / State Governments • Consultants • Implementing Agency	**Mandatory**

		• Source code shall be free from any royalty. All Government Organizations, while implementing e-Governance applications and systems must include a specific requirement in Request for Proposal (RFP) for all suppliers to consider OSS along with CSS while responding. Suppliers shall provide justification for exclusion of OSS in their response, as the case may be. Government Organizations shall ensure compliance with this requirement and decide by comparing both OSS and CSS options with respect to capability, strategic control, scalability, security, life-time costs and support requirements. It is recommended to adopt Open Source Software in all e-Governance applications and systems implemented by Government Organizations. However, in certain specialised domains where OSS solutions meeting essential functional requirements may not be available or in case of urgent/strategic need to deploy CSS based solutions or lack of expertise (skill set) in identified technologies, the concerned Government Organization may consider exceptions, with sufficient justification		
12	**Policy on Open Application Programming Interfaces (APIs) for Government of India"**	Interoperability among various e-Governance systems is an important prerequisite for upgrading the quality and effectiveness of service delivery. It is also required in order to facilitate the single window concept of electronic services delivery by Government Organizations. The purpose of this policy is to develop interoperable ecosystem of data, applications and processes in Government which will make the right information available to the right user at the right time. Adoption of Open APIs in Government will enable quick and transparent integration with other e-Governance applications and systems	• Administrator • e-Governance project teams in all Departments of Central / State Governments • Consultants • Implementing Agency	**Mandatory**

		implemented by various Government organizations, thereby providing access to data & services and promoting citizen participation for the benefit of the community. Policy is available at http://www.egazette.nic.in/WriteReadData/2015/164238.pdf		
13	**Web Content Accessibility Guidelines** **(WCAG) 2.0**	The WCAG documents explain how to make web content more accessible to people with disabilities. Web "content" generally refers to the information in a web page or web application, including: • natural information such as text, images, and sounds • code or markup that defines structure, presentation, etc. Web Content Accessibility Guidelines (WCAG) is developed by W3C in cooperation with individuals and organizations around the world, with a goal of proving a single shared standard for web content accessibility that meets the needs of individuals, organizations, and governments internationally.	• Administrator • e-Governance project teams in all Departments of Central / State Governments • Consultants • Implementing Agency	**Recommended**
14	**Guidelines for Indian Government Websites** **(GIGW)**	These guidelines have been developed by National Informatics Centre (NIC) and adopted by Department of Administrative reforms and Public Grievances (DARPG) as a part of Central Secretariat Manual of office procedures (CSMOP). These Guidelines address the entire lifecycle of a website, web portal/application right from its conceptualisation to design, development, maintenance and management. The guidelines are available at http://darpg.gov.in/sites/default/files/Guidelines_for_Government_websites_0_0.pdf All Government websites must adhere to Guidelines for Indian Government Websites.	• Administrator • e-Governance project teams in all Departments of Central / State Governments • Consultants • Implementing Agency	**Mandatory**

List of MeitY provided core infrastructure services

(Ready to be integrated with new/existing solutions)

1 – MeitY Core Infrastructure Services-

S.No.	Service	Description	Available Software
1.	Identity Management for individual	Electronic Identity Verification	Aadhaar
2.	Address Management	Electronic address verification	Aadhaar, DigiLocker, LGD Directory
3.	Single Sign On	OAuth 2.0	DigiLocker
4.	Access Management	Electronic access for government officials	eParichay
5.	eSign	Electronic signature	eSign
6.	Entity Management	Electronic entity verification	PAN, GSTN, CIN
7.	GIS platform	Standardization of addresses (One Nation One Address) Electronic infrastructure mapping	NCoG
8.	Land Records	Electronic Land Records Management	BharatMaps
9.	Linguistic Support	Real time electronic translation and transliteration	eBhaasha
10.	Email Gateway	Government eMail	Email
11.	Messaging Gateway	Real time messaging, SMS	mSeva
12.	Document Management System for citizens	Electronic document management for citizens with nomination facility	DigiLocker
13.	Video Conferencing	Voice and video conferencing	Vidyo Connect
14.	API Gateway	Electronic data exchange	National Data Highway
15.	Payment Gateway	Electronic payment address	UPI, BHIM
16.	Collaborative SW Development	Versioning management	Open Forge
17.	Appstore	Storehouse of electronic applications	eGov Appstore
18.	Cloud Services	Provide cloud services IAAS, PAAS	MeghRaj
19.	Website Development	Easy website development	Swayam

S.No.	Service	Description	Available Software
20.	Programming for Services	Easy programming for service delivery	ServicePlus
21.	Service Delivery Tracking	Real Time Tracking of G2C service delivery to citizens	Etaal
22.	High Performance Computing	HPC in a Box computing solution	Param Shawak
23.	Identity Management System	Online authentication identity management system	E-Pramaan
24.	Integrity of Documents	A blockchain based proof of existence and proof of storage for checking integrity of documents	Abhedya

2 - Common Use Applications (Pan-India)

The list of envisaged and existing IndEA Common Use Applications is as below.

#	Service	Description	Available Software
3.	Integrated Service Management	Hand-held access to all G2C services of the Government and citizen feedback	Umang
4.	Document Management for Government	G2E service	eOffice
5.	Collaborative Government	Mode for electronic participation of citizens through contests, volunteering etc.	MyGov
6.	Government Procurement	Government eMarketplace for products and services	GeM
7.	Grievance Management related to citizens	Central System for taking citizen grievances	CGRAMS
8.	Human Resource Management	Software to help government officers track their leaves, performance appraisal, transfers, salary, attendance, leaves etc.	Supremo for IAS officers
9.	Project Management Information System	Project Management software customizable to administer government projects / schemes and collect Digital UCs	PMIS
10.	Learning Management System	eGov courses for government officers	LMS
11.	Knowledge	Storehouse of Government documents	KMS

#	Service	Description	Available Software
	Management System	regarding projects, services, assessments etc.	
12.	Court Management System	Manage all cases where Government is directly involved as one of the parties	eCourts
13.	Physical Access Management	Access Management for Government Offices	MyVisit
14.	Financial Management	Public Financial Management System	PFMS
15.	Right to Information	Common interface to submit RTI questions and received answers regarding the same	RTI
16.	Services Assessment	Assessment of service quality being delivered by Government Agencies	Umang- RAS

***