REQUEST FOR PROPOSAL

FOR

SELECTION OF MASTER SYSTEM INTEGRATOR FOR IMPLEMENTATION OF INTEGRATED COMMAND & CONTROL CENTER AND SMART COMPONENTS IN LUDHIANA CITY

Volume 2 – Scope of Work

Date: 06th December 2018

Invited by:
Ludhiana Smart City Limited (LSCL)
2nd Floor, Office of CEO,
Zone A- Ludhiana Municipal Corporation Office,
Mata Rani Chowk, Ludhiana, Punjab

Table of Contents

1. Disclaimer

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

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

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

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

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

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

The Bidder shall bear all its costs associated with or relating to the preparation and submission of its Bid including but not limited to preparation, copying, postage, delivery fees, expenses associated with any demonstrations or presentations which may be required by LSCL or any other costs

incurred in connection with or relating to its Bid. All such costs and expenses will remain with the Bidder and LSCL shall not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by a Bidder in preparation for submission of the Bid, regardless of the conduct or outcome of the Selection process.

2. Glossary

Terms	Meaning
LMC	Ludhiana Municipal Corporation
ANPR	Automatic Number Plate Recognition
LSCL	Ludhiana Smart City Limited
ATCS	Adaptive Traffic Control System
BOM	Bill of Material
CCTV	Closed Circuit Television
CCC	Command and Control Center
CONOPS	Concept of Operations
DC	Data Center
DRC	Disaster Recovery Center
FMS	Facility Management Services
GIS	Geographical Information Systems
GPS	Global Positioning System
GSM	Global System for Mobile Communication
ICCC	Integrated Command and Control Center
ICT	Information and Communication Technology
IP	Internet Protocol
IT	Information Technology
ITMS	Intelligent Traffic Management System
KPI	Key Performance Indicator
MLCP	Multi-Level Car Park
MPLS	Multi-Protocol Label Switching
MSI	Master Systems Integrator
ONVIF	Open Network Video Interface Forum
O&M	Operations and Maintenance
OEM	Original Equipment Manufacture
OFC	Optical Fiber Cable
OWASP	Open Web Application Security Project
PKI	Public Key Infrastructure
PIS	Public Information System
PA System	Public Address System
PoP	Point of Presence
PTZ	Pan Tilt Zoom
RFP	Request for Proposal

Terms	Meaning
RLVD	Red Light Violation Detection
RTO	Recovery Time Objective
RPO	Recovery Point Objective
SCADA	Supervisory control and data acquisition
SLA	Service Level Agreement
SMS	Short Message Service
SOP	Standard Operating Procedures
TPA	Third Party Auditor
UAT	User Acceptance Testing
UPS	Uninterrupted Power Supply
VM	Virtual Machine
VMD	Variable Message Display
VCA	Video Content Analysis

3. Introduction

3.1 Project Background

One of the primary objective of LSCL under its smart city mission is to enhance the safety and security, improve traffic management, improve efficiency of municipal services and promote a better quality of life for residents. In order to achieve these objectives, LSCL desires to foster the development of a robust ICT infrastructure that supports digital applications and ensures seamless steady state operations, city transport services, traffic management, surveillance, emergency response mechanisms, real time tracking of services and vital city metrics throughout the city and in government departments.

LSCL is considering the appointment of an agency to set up these priority initiatives identified under Smart City Mission which includes Integrated Command and Control center (ICCC) and Smart Elements like City Surveillance, Variable Message Displays, Public Address System, Electronic Call Box, etc. The project also envisage to integrate host of sub system with the Integrated Command and Control Centre

Main objective of the project is to break silos in the city within the departments and across the departments. Also to install appropriate check points for solutions implemented, so that the services delivered to the public are up to their expectation.

3.2 Project Objectives

The Ludhiana Smart City Limited (LSCL) under their PAN City Projects, have envisaged implementing Integrated Command & Control Center (ICCC) across Ludhiana city. LSCL plans to utilize information technology to modernize key functions of city operations including traffic management, Traffic control, Traffic Law enforcement, security and safety, e-governance, municipal operations, information dissemination etc. in the city to build a well-informed, connected, smart and smooth operations for citizens of the city.

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

ICCC enables collation of information and collaborative monitoring, thus helping in the analysis of data for quicker decision making. Intelligent operations capability ensures integrated data visualization, real-time collaboration and deep analytics that can help different stakeholders prepare for exigencies, coordinate and manage response efforts, and enhance the ongoing efficiency of city operations. The interface at ICCC gives a real-time and unified view of operations. Cities can rapidly share information across agency lines to accelerate problem response and improve project coordination. Furthermore, the ICCC will help in anticipating the challenges and minimizing the impact of disruptions.

Following are the intangibles that should be addressed by this intervention:

1. Enable real-time monitoring of the various facets of management of Ludhiana Smart City i.e. Security, Traffic and City Utilities.
2. 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.
3. Increase Operational Efficiency: City Authorities intends to spend more time on the public facing functions. Thus Information technology solutions should help in reducing the repetitive paperwork/records and making the back-office functions more efficient.
4. Improve Traffic Services: The traffic services to the public can be improved through the user friendly presentation of the various traffic information in real time.
5. Safety Improvement: The real-time traffic monitoring can prevent accidents by recognizing and thus responding to the potentially dangerous situation in advance.
6. Higher Productivity: Achieving improvement in the productivity, logistics and other economic activities by obtaining the precise-real time information on transport due to the availability of data on traffic flow in key areas of the city.
7. Real Time Information & Response: The real-time information at the ICCC shall enable the operator to take necessary actions based on the real time information and execute the required responses. It shall be possible to track a particular event using the cameras installed at the various locations.
8. Creating awareness and Education of public: Through sign boards, awareness on road traffic rules and safe driving precautions shall be imparted to road users.
9. Reduction in Social Cost: The overall social cost can be saved by easing the traffic congestion by utilizing the optimally allocated real time traffic information
10. Create a platform for sharing traffic information across the city: There is a critical need to create a platform for sharing traffic related information among traffic police and citizens in order to increase the effectiveness of Traffic Management.
11. Pollution Control: To reduce pollution with a cleaner Air in the city due to improved traffic
12. Security and Safety: Live Surveillance through a network of CCTV Cameras will help to identify, apprehend and prosecute offenders and provide live alerts in case of events and incidents.
13. Effective & Preventive Policing: The technological interventions proposed for traffic regulation enforcement and CCTV coverage will enable quick tapping of issues in the form of data and maps such as crime mapping, blind spots, accidental zones, peak hour traffic count, average travel time, etc. This will enable the police department to reduce crime and do preventive policing.
14. Reduce Congestion and Emissions: Smart parking enables better and real time monitoring and managing of available parking space, and guides residents and visitors to nearby

available parking facility resulting reduction of emission of CO2 and other pollutants. Thus it creates a better environment.

15. Provide capability to respond in a unified manner to situations on ground (both day to day and emergency situations) by creating a common operational picture for the relevant stakeholder
16. Provide and manage touch points from all concerned stakeholders during the lifecycle of various incidents
17. Define and manage the Key Performance Indicators (KPIs) for various systems deployed under enhancement and operational aspects of the City Management
18. Provide capability to conduct analysis for continuous improvement of city operations
19. Better management of utilities and quantification of services
20. Disaster Management and Emergency Response System
21. Asset Management
22. Provide and manage system for transit management
23. Generate Alerts over different modes of communication related to core systems deployed for objectives of smart city project

Ludhiana Smart City Limited envisages to create an Integrated Command and Control Centre with integration to existing sub systems and deployment of various other sub –systems.

a) Integration with existing control centers and other sub systems in the city (with provision for future scalability)
   - Smart Lighting,
   - Smart Governance,
   - City Surveillance and smart traffic (RLVD and ANPR),
   - Solid Waste Management,
   - Smart Parking,
   - City Bus ITMS,
   - Water SCADA
   - Sewerage,
   - Power SCADA
   - Health,
   - Education
   - GIS
   - Unified operations through integration of urban functions offered by the city administration

b) As art of this project Ludhiana SMART City Project also envisages deployment of following components to achieve the objectives:

- Implementation of command and control center along with DC and DR
- Deployment of various sensors (environment and weather sensors) throughout the city to improve situational awareness
- Deployment of Public Address System & Panic Button with Emergency Call Box to enhance public awareness and emergency response.
- Deployment of Various Cameras in municipal limits to improve various civic services like Solid Waste Management, Tahbazari Violations , SMART On Street Parking
- Deployment of Variable Messages Signboards for Public Information Display.

4. Project Components

4.1 Components & Services Overview

A. Physical City ICCC:

Ludhiana smart city has to implement, integrate and operationalize all the smart solutions/ components of the city. These smart ICT solutions VMD, City Surveillance, PAS, ECB, etc. have to be implemented by MSI to be selected through this RFP. Establishing the physical build of City command center with Video wall, local video storage, networking components etc. will also be responsibility of MSI.

LSCL intends to select a Master System Integrator (MSI) for city of Ludhiana by following competitive bidding process to design, develop, implement and maintain the Smart City System for a period of five years on turnkey basis. This document contains the following details:

- Scope of work that will be assigned to the MSI as part of this project
- Other terms and conditions of the envisaged Smart City System

B. City Operation/IoT Platform

The city operation platform will be hosted at the cloud and design, implementation and maintenance of the operation platform will be under the scope of MSI. MSI will work on integrating different components and services with the operation platform. The platform should have capability of integrating different field level devices in order to support IoT ecosystem.

C. Data Center/ Data Recovery

1. The infrastructure of Data Center for ICCC, shall be hosted at the same site as that of ICCC.
2. The MSI need to do the sizing of rack space required at facilities based on its capacity planning and sizing for the entire duration of the contract with adequate space for future expansion.
3. The infrastructure of Data Recovery shall also be hosted at Data Recovery Cloud.
4. The **Data on Cloud platform will EXCLUSIVELY reside in India ONLY** and not in any other country.

MSI will establish Integrated Command and Control center for Ludhiana comprising of various project modules/ components mentioned below:

D. Level 1: Integrated and View

Certain components will be integrated using direct feeds, dashboards and sharing of alerts/ actionable inputs for integrate and view operations, such as:

5. City Surveillance System (Police and Traffic)
6. Smart Governance (E-Governance)

7. Intelligent Transport Management System – City buses
8. Smart Energy (Power SCADA)
9. Smart Water (Water SCADA)
10. SMART Health
11. SMART Education
12. SMART Parking & Payment System
13. CCMS for LED Street Lights
14. GIS Based Property Management System
15. Smart Solid Waste Management – GPS Enabled Vehicle

E. Level 2: Implement, Integrate, Command, Control and Fully Operate

Following components will be implemented as a part of this project.

16. Integrated Command and Control Center (ICCC)
17. Geographical Information System (GIS)
18. Panic Button & Emergency Call Box
19. Public Addressal Systems
20. Environmental Sensors
21. Digital VMD's
22. CCTV Cameras Installed for various other civic purposes as part of Project

The following sections details out the status of systems which are envisaged for integration with the Command and Control Centre:

1. Services envisaged to be ready before the implementation of Integrated Command and Control Centre

S.No.	Modules	Present Automation Status	Planned Automation in next 1 years (Near Future Integration)
1	Smart Lighting	No	Yes
2	Solid Waste Management	Partial	Yes
3	Smart Traffic	Partial	Yes
4	City Surveillance	Partial	Yes

S.No.	Modules	Present Automation Status	Planned Automation in next 1 years (Near Future Integration)
5	Smart Governance	Yes	Yes
6	Smart Parking	No	Yes
7	Sewerage	Partial	Yes
8	Power SCADA	Partial	Yes
9	GIS	No	Yes

2. Services envisage to be ready in future:

S.No.	Modules	Present Automation Status	Planned Automation in next 1 years (Near Future Integration)	Future Integration
1	Water SCADA	No	No	Yes
2	Health	No	No	Yes
3	Education	No	No	Yes
4	Storm Water Drainage	No	No	Yes
5	City Bus ITMS	Partial	No	Yes

3. Services envisage to be ready along with ICCC as part of SI Scope

S.No.	Modules	Present Automation Status	Future Integration
1	Panic Button & Emergency Call Box	No	Yes
2	Public Addressal System	No	Yes
3	Environmental Sensors	No	Yes

S.No.	Modules	Present Automation Status	Future Integration
4	Digital Variable Messaging Display	No	Yes
5	CCTV Cameras	No	Yes

*These other services will be additional work and will be taken up as "Change request".

MSI shall be responsible to carry out the detailed survey prior to submission of bid for the complete solution component requirement in order to finalize infrastructure requirement, network bandwidth requirement, operational & administrative challenges etc.

The subsequent sections detail out the solution and scope with respect to each of the solution component. MSI shall note that the activities defined within scope of work mentioned are indicative and may not be exhaustive. 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 this RFP and factor the same in its response.

The scope of the project includes implementation of identified smart ICT solutions including establishment of city based Integrated Command and Control Center integrated with other implemented ICT solutions. Scope also includes conducting a detailed assessment of current state of city services being provided and accordingly plan, design a comprehensive technical architecture of city Integrated Command and Control Center (ICCC) and integrated it other components so that relevant current and future ICT project may be integrated with ICCC.

As part of scope the MSI is expected to integrate various other ICT initiatives of the city with ICCC. These ICT initiatives may be from other departments' services like Traffic, Police, and Transport etc. The MSI shall have the overall responsibility to design, build, implement, operate, and maintain the project for a period of five years from the date of successful commissioning.

Specifically, Following are the main activities to be carried out by MSI:

1. Project Planning, execution and Management
2. Assessment and Gap analysis of requirement for all smart city components under scope.
3. Solution Design, System Customization and development for all components mentioned in this volume.
4. ICT items Procurement, deployment and commissioning
5. Site Preparation including required civil work, LAN Networking
6. Application and general awareness Training
7. Business Process Reengineering for the selected applications/ services, if required

8. STQC Certification
9. UAT & Go live
10. Capacity Building
11. Technical Support
12. Operation & Maintenance (O&M) for 5 Years.

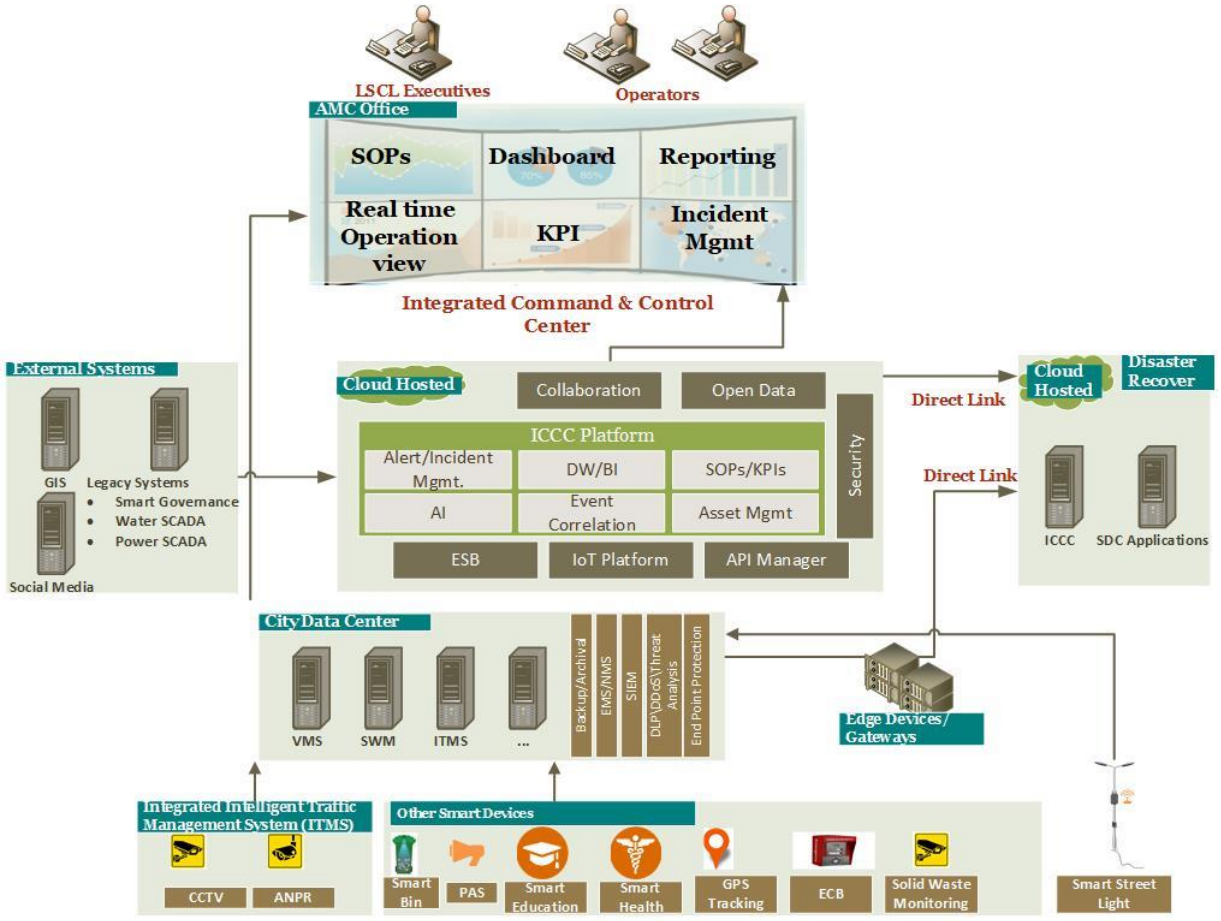
4.2 Project phases

The modules/ components mentioned in the above section will be implemented in the following two phases:

#	System Description	Phases
1.	Integrated Command and Control Center	Phase I
2.	GIS	Phase I
3.	Deployment & Integration of Field Level Edge Equipment (Cameras, PA System, Panic Button & Emergency Call Box, Environmental Sensors, and Digital Variable messaging Sign boards)	Phase I
4.	Integration with City Surveillance	Phase I
5.	Integration with SMART Governance	Phase I
6.	Integration with SMART LED lighting	Phase I
7.	Integration with Smart Traffic	Phase I
8.	Integration with Solid Waste Management	Phase I
9.	Integration with Power SCADA	Phase II
10.	Integration with Water SCADA	Phase II
11.	Integration with ITMS	Phase II
12.	Integration with SMART Parking	Phase II

4.3 Solution Architecture

The indicative solution architecture of ICCC and associated system components envisaged is as given below:



a. Field Devices

The field devices layer will contain display devices or bi-directional (input & output) devices connected to the network which will be used by citizens to consume - and for administrators to provide - actionable information. Such field devices include digital messaging boards, environmental data displays, etc.

This would also comprise of the sensors which will help the city administration gather information about the ambient city conditions or capture information from the edge level devices like cameras, environment sensors, GPS sensors, etc.

b. Data Center & Security

As ambient conditions, actuators and display devices are now connected through a network and send data to business applications, security of the entire system becomes paramount:

- Infrastructure security- including policies for identity and information security policies

- Network security- including policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources, etc.
- Identity and Access Management – including user authentication, authorization, SSL & Digital Signatures
- Application security- including Hosting of Government Websites and other Cloud based services, Adoption of Technical Standards for Interoperability Framework and other standards published by Government of India for various e-Governance applications
- End device security, including physical security of all end devices such as display boards, emergency boxes, kiosks etc.

Following security parameters should be included for all smart elements, but not limited to:

- User/administrator audit log activity (logon, user creation, date-time of PA announcements, voice recording etc.)
- Secured data storage (storage of video/image/voice/location/data captured by various smart elements)
- SSL/TLS encryption for web and mobile application based interfaces for sensitive data transfer
- Protection against Denial of Service (DoS) and Interference attacks to public Wi-Fi Devices
- SIEM security framework as mandated MoUD guidelines

c. Network

The secured network will serve as the backbone for the project and provide connectivity to gather data from sensors, share the data with business applications and transmit messages to display devices and actuators. It will support the Wi-Fi services and other smart elements (sensors and displays) at given locations. The network will be scalable such that additional sensors, actuators, display devices can be seamlessly added and more Wi-Fi spots created in future.

d. Enterprise Computing

The business applications will need the appropriate hosting infrastructure considering their criticality to deliver services. The IT Infrastructure required for hosting will include Storage, Compute and Processing capabilities that are aligned with the non-functional requirements for the business applications.

e. Applications

The Applications will contain data aggregation and management systems (rules engines, alerting systems, diagnostics systems, control systems, messaging system, events handling system), and reporting / dashboard system to provide actionable information to city administrators and citizens. Applications would comprise of the applications developed to receive data from field devices for each city domain. Applications in this layer will integrate with the ICCC solution to share data and also generate advanced analytics through correlations.

This will be an evolving layer with applications added as and when new functions are identified by the stakeholders.

f. Integration

While aspects of ambient conditions within the city will be gathered through various sensors deployed, some city specific data will come from other government and non-government agencies. It is through the integration layer – that data will be exchanged to and from the under lying architecture components and other data from system developed by government (such as police department, street lights department, water department transport organizations within Ludhiana, etc.) and non-government agencies. The various integrations have been listed below:

1) City Surveillance System (Police and Traffic)
2) Smart Governance (E-Governance)
3) Intelligent Transport Management System – City buses
4) Smart Energy (Power SCADA)
5) Smart Water (Water SCADA)
6) SMART Health
7) SMART Education
8) SMART Parking & Payment System
9) CCMS for LED Street Lights
10) GIS Based Property Management System
11) Smart Solid Waste Management – GPS Enabled Vehicle

g. Presentation

There will be two modes of presentation to the users accessing the ICCC system –

1) **Mobile UI** – Mobile based UI shall be for the senior management officials who would be accessing the system for very quick and faster flow of information exchange. This would cover less of the functions of the system as it would be largely designed for accessing by the senior management. Also it should provide field workforce app. which should have capability to assign task, task prioritization, route planning etc. Also field workforce can raise issues, get task assigned, provide status update etc. using this app.
2) **Web-based UI** – Web-based UI for the other officials who would be accessing the system for the information required for their respective departments

h. Integrated Command and Control Center

This is the overarching layer that integrates with the business applications that receive data from field devices. The Integrated Command and Control Centre application presents a Common Operating Picture which will enable citizens and administrators alike to get a holistic view of city operations. The application will integrate with the GIS layer to represent the real-time operational state on the map for easy visualization.

5. Scope of Services

5.1 Geographical Scope of services

The following is a summary of the geographical extent of the project.

#	System Description	Numbers
1.	Environmental Sensors	10
2.	Panic Button/ Emergency Call Box	50
3.	Public Address System	50
4.	Digital Variable Message Display	10
5.	City Surveillance System – Box Cameras	200
6.	City Surveillance System – PTZ Cameras	100
7.	Data Center (DC)	DC at ICCC site
8.	Data Recovery (DR) Center	DR Cloud
9.	City Operation/IoT Platform	Cloud hosted
10.	Integrated Command & Control Center (ICCC)	ICCC at identified location

MSI to discuss and confirm with LSCL the exact locations for the installation of components mentioned above.

MSI should ensure that **Data on Cloud platform MUST EXCLUSIVELY reside in India ONLY** and not in any other country.

5.2 Overview of Scope of Services

The MSI's scope of work shall include but will not be limited to the following broad areas. Details of each of these broad areas have also been outlined in Annexure II.

1. **Assessment, Scoping and Survey Study: Conduct a detailed assessment, scoping study and develop a comprehensive project plan, including:**
    a. Assess existing systems, street infrastructure and connectivity within the city for the scope items mentioned in section 4.1
    b. Conduct site survey for finalization of detailed technical architecture, gap analysis and project plan
    c. Conduct site surveys to identify need for site preparation activities
    d. Obtain site Clearance obligations & other relevant permissions
2. **Design, Supply, Installation, Commissioning and Testing which includes the following components:**
    a. Environmental Sensors

b. Variable Message Display

c. City Surveillance System

d. Public Address System

e. Emergency Call Box/ Panic Button

f. Integrated Control and Command Centre

g. Data Centre

3. **Operation and Maintenance Phase:** The selected vendor will also be responsible for supply of IT solution for the management of hardware and application software, networking, installation, Training, Maintenance and operations of the solution for the period of 4 years from the Go Live date (Refer Section 7), the O&M period will commence after Go-Live and will be for a period of 4 years. Warranty period of the product supplied under project i.e. hardware, software, IT/Non-IT etc., will be considered after Go-Live.

4. Integration with provisions available for Network Connectivity within the city which includes:

   a. Existing Fibre Optic Network (if available)

   b. Internet connectivity procured as part of this tender

5. Provisioning Hardware and Software Infrastructure which includes design, supply, installation, and commissioning of Cloud Platform, IT Infrastructure at Data Center (DC), Data Recovery Center (DRC), Integrated Command & Control Center (ICCC). This consist of:

   a. Basic Site preparation services

   b. IT Infrastructure including server, storage, other required hardware, application portfolio, licenses

   c. Command Center infrastructure including operator workstations, IP phones, joystick controller etc.

   d. Establishment of LAN and WAN connectivity between cloud, command center, DC and DR limited to scope of infrastructure procured for the project

6. Phase wise Integration of the ICT systems with Integrated Command & Control Center (ICCC):

   a. City Surveillance System (Police and Traffic)

   b. Smart Governance (E-Governance)

   c. Intelligent Transport Management System – City buses

   d. Smart Energy (Power SCADA)

   e. Smart Water (Water SCADA)

   f. SMART Health

   g. SMART Education

   h. SMART Parking & Payment System

i. CCMS for LED Street Lights
j. GIS Based Property Management System
k. Smart Solid Waste Management – GPS Enabled Vehicle

7. Capacity Building for LSCL and other end user department which includes preparation of operational manuals, training documents and capacity building support, including:

a. Training of the city authorities, police personnel and operators on operationalization of the system
b. Support during execution of acceptance testing
c. Preparation and implementation of the information security policy, including policies on backup and redundancy plan
d. Preparation of KPIs for performance monitoring of various urban utilities monitored through the system envisaged to be implemented
e. Developing standard operating procedures for operations management and other services to be rendered by ICCC

8. Preparation of system documents, user manuals, performance manuals, Operation manual etc.

9. Identification of Revenue generation opportunities by various smart solutions, planning and roll out of strategy

10. MSI would not hold any authority on the city data collected and only LSCL would be having all the rights on the data

11. Operations and Maintenance services for the software, hardware and other IT and Non-IT infrastructure installed as part of the project after Go-Live and for a period of 4 years from the date of Go-Live. Five years of warranty period of the product supplied under project i.e hardware, software, IT/Non-IT etc., will be initiated/considered after Go-Live only.

5.3 Assessment and Site Survey & Project Plan

After signing of contract, the MSI needs to deploy local team (based out of Ludhiana) proposed for the project and ensure that a Project Inception Report is submitted to LSCL which should cover following aspects:

1. Names of the Project Team members, their roles and responsibilities
2. Approach and methodology to be adopted to implement the Project (which should be in line with what has been proposed during bidding stage, but may have value additions / learning in the interest of the project).
3. Responsibility matrix for all stakeholders
4. Risks the MSI anticipates and the plans they have towards their mitigation

5. Detailed project plan specifying dependencies between various project activities / sub-activities and their timelines
6. The MSI shall conduct a comprehensive As-Is study of the existing infrastructure of Traffic Junctions, Locations of Public Wi-Fi Hot Spots, CCTV camera locations to establish the key performance indicators (KPIs) for the project. The KPIs of the study shall be included in the survey. Also, the existing infrastructure needs to be utilized to their maximum capacity.
7. The MSI shall study the existing business processes, functionalities, existing management systems and applications including MIS reporting requirements.

Additionally, the MSI should provide detailed designs specifying the following:

1. High Level Design (including but not limited to) 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
2. Concept of Operations for the TO-BE state that covers – Layout of the ICCC, Staffing Requirements, Standard Operating Procedures, Operations Model for 24/7 coverage, Roles and Responsibilities
3. Application component design including component deployment views, control flows, etc.
4. Low Level Design (including but not limited to) 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 Punjab
5. Location of all field systems and components proposed at the junctions, (KML /KMZ file plotted on GIS platform like google earth etc.)
6. Location of Network Provider's Point of Presence (PoP)
7. Design of Cables, Ducts routing, digging and trenching
8. Electrical power provisioning.
9. **Open Standards -** System should use open standards and protocols to the extent possible without compromising on the security
10. **Convergence** - LSCL has already initiated many projects which have state of the art infrastructure at field locations deployed under them. Under the smart city program, LSCL has envisaged to create a state of the art infrastructure and services for the citizens of Ludhiana, hence it is imperative that all infrastructure created under the project shall be leveraged for maximum utilization. Hence the MSI is required to ensure that such infrastructure will allow for accommodation of equipment's being procured under other smart city projects. The procedure for utilization of the infrastructure will be mutually agreed between the LSCL and MSI
11. Sub-contracting / Outsourcing shall be allowed only for the work which is allowed as mentioned in this clause with prior written approval of LSCL. However, even if the work is

sub-contracted / outsourced, the sole responsibility of the work shall lie with the MSI. The MSI shall be held responsible for any delay/error/non-compliance etc. of its sub-contracted vendor. The details of the sub-contracting agreements (if any) between both the parties would be required to be submitted to LSCL. Sub-contracting / outsourcing would be allowed only for work such as:

I. Field Surveys required for the projects in scope

II. Passive Networking & Civil Work during implementation,

III. FMS staff for non- IT support during post-implementation

5.4 Finalization of Detailed Technical Architecture

The MSI shall also identify the customizations/ workaround that would be required for successful implementation and operation of the ICCC project. The MSI shall submit the detailed Technical Architecture, which should take into consideration following guiding principles:

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

   The architecture should be scalable (cater to increasing load of internal and external users and their transactions) and capable of delivering high performance till the system is operational. In this context, it is required that the application and deployment architecture should provide for Scale-Up and Scale out on the Application and Web Servers, Database Servers and all other solution components. The data centre infrastructure shall be capable of serving the growing concurrent users requirement which would be increasing as the city would grow.

2. **Availability** - The architecture components should be redundant and ensure that are no single point of failures in the key solution components. Considering the high sensitivity of the system, design should be in such a way as to be resilient to technology sabotage. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage. The MSI shall make the provision for high availability for all the services of the system. Redundancy has to be considered at the core / data center components level.

3. **Security** - The architecture must adopt an end-to-end / End-Point security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc. MSI must make provisions for security of field equipment as well as protection of the software system from hackers and other threats. Using Firewalls and Intrusion Prevention Systems such attacks and theft should be controlled and well supported (and implemented) with the security policy. The virus and worm attacks should be well defended with gateway level Anti-

virus system, along with workstation level Anti-virus mechanism. There should also be an endeavour to make use of the SSL/VPN technologies to have secured communication between Applications and its end users. Furthermore, all the system logs should be properly stored & archived for future analysis and forensics whenever desired. LSCL would carry out the security audit of the entire system upon handover and also at regular interval during O&M period. Bidder's solution shall adhere to the model framework of cyber security requirements set for Smart City (K-15016/61/2016-SC-1, Government of India, and Ministry of Urban Development).

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

The systems implemented for project should be highly secure, considering that it is intended to handle sensitive data relating to the city and residents of the city. The overarching security considerations are described below:

a. The security services used to protect the solution shall include: Identification, Authentication, Access Control, Administration and Audit and support for industry standard protocols.

b. The solution shall support advanced user authentication mechanisms including digital certificates and biometric authentication.

c. Security design should provide for a well-designed identity management system, security of physical and digital assets, data and network security, backup and recovery and disaster recovery system.

d. The solution should provide for maintaining an audit trail of all the transactions and should also ensure the non-repudiation of audit trail without impacting the overall performance of the system.

e. The overarching requirement is the need to comply with ISO 27001 standards of security.

f. The application design and development should comply with OWASP top 10 principles

g. In the event of a breach or indicator-of-compromise, it becomes critical that forensic capability must be available to go back in time and to be able to regenerate the event for investigation purposes. The resulting RCA would help LSCL or Team managing the ICT Infra prevent itself from similar threats in the future.

h. To ensure protection of citizen data SOC and Managed Security Services to be used which will mandate undertaking SOC 2 Compliance by MSI.

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

5. **Interoperability** - The system should have capability to take feed from cameras installed by private / Govt. at public places, digitize (if required) & compress (if required) this feed & store as per requirements.
6. **Open Standards** - Systems should use open standards and protocols. Keeping in view the evolving needs of interoperability, especially the possibility that the solution shall become the focal point of delivery of services, and may also involve cross-functionality with the e-Government projects of other departments / businesses in future, the solution should be built on Open Standards. The MSI shall ensure that the application developed is easily integrated with the existing applications. The code does not build a dependency on any proprietary software, particularly, through the use of proprietary 'stored procedures' belonging to a specific database product. The standards should at least comply with the published eGovernance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time)
7. **Single-Sign On-** The application should enable single-sign-on so that any user once authenticated and authorized by system is not required to be re-authorized for completing any of the services in the same session. For employees of the department concerned, the browser based application accessed on the intranet, through single-sign-on mechanism, will provide access to all the services of the departments concerned (based on their roles and responsibilities), Help module, basic and advanced reporting etc. Similarly, for external users (citizens, etc), based on their profile and registration, the system shall enable single-sign on facility to apply for various services, make payments, submit queries /complaints and check status of their applications.
8. **Support for PKI-based Authentication and Authorization**- The solution shall support PKI based Authentication and Authorization, in accordance with IT Act 2000, using the Digital Certificates issued by the Certifying Authorities (CA). In particular, 3 factor authentications (login id & password, biometric and digital signature) shall be implemented by the MSI for officials/employees involved in processing citizen services.
9. **Convergence** - LSCL 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. Under the smart city program, LSCL has envisaged to create a state of the art infrastructure and services for the citizens of Ludhiana, hence it is imperative that all infrastructure created under the project shall be leveraged for maximum utilization. Hence the MSI is required to ensure that such infrastructure will allow for accommodation of equipment's being procured under other smart city projects. Equipment like Junction Boxes and poles deployed under the ICCC project at the field locations will be utilized to accommodate field equipment's created under the other projects of LSCL. The procedure for utilization of the infrastructure will be mutually agreed between the LSCL and Master System Integrator.

10. All the personnel working on the Project and having access to the Servers / Data Center should be on direct payroll of the MSI/OEM/Consortium partner. The MSI would not be allowed to sub-contract work, except for following:

    a. Passive networking & civil work during implementation and O&M period,

    b. Viewing manpower at ICCC during post-implementation

    c. FMS staff for non- IT support during post-implementation

    d. Services of professional architect for design of ICCC

    However, even if the work is sub-contracted , the sole responsibility of the work shall lie with the MSI. The MSI shall be held responsible for any delay/error/non-compliance/penalties etc. of its sub-contracted vendor. The details of the sub-contracting agreements (if any) between both the parties would be required to be submitted to LSCL and approved by the LSCL before resource mobilisation.

11. **GIS Integration**- MSI shall undertake detail assessment for integration of the e-Governance, Surveillance System and all other components with the Geographical Information System (GIS). MSI is required to carry out the seamless integration to ensure ease of use of GIS in the Dashboards in ICCC. If this requires field survey, it needs to be done by MSI. If such a data is already available with city, it shall facilitate to provide the same. MSI is to check the availability of such data and it's suitability for the project. MSI is required to update GIS maps from time to time.

12. **SMS Gateway Integration**- MSI shall carry out SMS Integration with the Smart City System and develop necessary applications to send mass SMS to groups/individuals. Any external/third party SMS gateway can be used, but this needs to be specified in the Technical Bid, and approved during Bid evaluation.

13. **Application Architecture**

    a. The applications designed and developed for the departments concerned must follow best practice and industry standards. In order to achieve the high level of stability and robustness of the application, the system development life cycle must be carried out using the industry standard best practices and adopting the security constraints for access and control rights. The various modules / application should have a common Exception Manager to handle any kind of exception arising due to internal/ external factors. 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)

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

c. MSI shall design and develop the ICCC System as per the Functional and System requirement specifications finalized.

i. The Modules specified will be developed afresh based on approved requirement.

ii. Apart from this, if some services are already developed/under development phase by the specific department, such services will be integrated with the ICCC System. These service will be processed through department specific Application in backend.

iii. The user of citizen services should be given a choice to interact with the system in local language in addition to English. The application should provision for uniform user experience across the multi lingual functionality covering following aspects:

- Front end web portal in English and local language
- E-forms (Labels & Data entry in local languages). Data entry should be provided preferably using the Enhanced Inscript standard (based on Unicode version 6.0 or later) keyboard layout with option for floating keyboard.
- Storage of entered data in local language using UNICODE (version 6.0 or later) encoding standard.
- Retrieval & display in local language across all user interfaces, forms and reports with all browsers compliant with Unicode version 6.0 and above.
- Facility for bilingual printing (English and the local language)

iv. Application should have a generic workflow engine for citizen centric services. This generic workflow engine will allow easy creation of workflow for new services. At the minimum, the workflow engine should have the following features:

- Feature to use the master data for the auto-populating the forms and dropdowns
- Creation of application form, by “drag & drop” feature using meta data standards
  - Defining the workflow for the approval of the form
  - First in First out
  - Defining a citizen charter/delivery of service in a time bound manner
- Creation of the “output” of the service, i.e. Certificate, Order etc.
- Automatic reports
  - of compliance to citizen charter on delivery of services
  - delay reports

d. 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).

e. The application should have a module for management of digital signature including issuance, renewal and suspension of digital signatures based on the administrative decisions taken by the State.

f. MSI shall ensure using Digital signatures/eAuthentication(Aadhar Based) to authenticate approvals of service requests etc.

i. e-Transaction & SLA Monitoring Tools

- The MSI should be able to measure and monitor the performance of the deployed infrastructure and all SLAs set out in this RFP. More importantly, it should be possible to monitor in REALTIME, the number of citizens touched through e-Services each day, month and year, through appropriate tools and MIS reports.
- The Infrastructure management and Monitoring System shall be used by MSI to monitor the infrastructure (Both IT and Non-IT) hosted at the Data center and DR site.
- For monitoring of uptime and performance of IT and non IT infrastructure deployed, the MSI shall have to provision for monitoring and measurement tools, licenses, etc. required for this purpose.

ii. The ICCC Application should have roadmap to integrate with key initiatives of State namely Portal Services, Citizen Contact Centre, Certifying Authority etc.

iii. Complete mobile enablement of the ICCC System

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

5.5 Site Clearance obligations & other relevant permissions

5.5.1 Electrical works and power supply

The MSI shall directly interact with electricity boards for provision of mains power supply at select/permanent locations for ICCC field systems. The MSI shall be responsible to pay the

electricity bills including connection charge, meter charge, recurring charges etc. to the electricity board directly. MSI shall have to submit the challan of bill submission to LSCL.

Survey and Commencement of Works

Prior to starting the site clearance, the MSI shall carry out survey of field locations as specified in Annexure IX, for buildings, structures, fences, trees, existing installations, etc. The LSCL shall be fully informed of the results of the survey and the amount and extent of the demolition and site clearance shall then be agreed with the LSCL.

5.5.2 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 arrester shall be erected for the entrance cables of power line, video line, data transmission cables. All crates shall have firm, durable shell. Shell shall have dustproof, antifouling, waterproof function & should capable to bear certain mechanical external force. Signal separation of low and high frequency; equipment's protective field shall be connected with its own public equal power bodies; small size/equipment signal lightning arrester shall be erected before the earthling. The Internal Surge Protection Device for Data Line Protection shall be selected as per zone of protection described in IEC 62305, 61643-11/12/21, 60364-4/5. Data line protection shall be used for security system, server data path and other communication equipment. Data line protection shall be installed as per zone defined in IEC 62305.Type 1 device shall be installed between zone 0B and zone 1. Type 2 devices shall be installed before the equipment in zone 2 and 3.

5.5.3 Earthing System

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

1. Earthing should be done for the entire power system and provisioning should be there to earth UPS systems, Power distribution units, AC units, etc. so as to avoid a ground differential. LSCL shall provide the necessary space required to prepare the earthing pits.
2. All metallic objects on the premises that are likely to be energized by electric currents should be effectively grounded.
3. 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.
4. The earth connections shall be properly made.

5. A complete copper mesh earthing grid needs to be installed for the server farm area, every rack need to be connected to this earthing grid. A separate earthing pit needs to be in place for this copper mesh.
6. Provide separate Earthing pits for Servers, & UPS as per the standards.

5.5.4 Junction Box, Poles and Cantilever

1. The MSI shall provide the Junction Boxes, poles and cantilever to mount the field sensors like the cameras, traffic sensors, traffic light aspects, active network components, controller and UPS at all field locations, as per the specifications given in the RFP.
2. The Junction Box needs to be appropriately sized in-order to accommodate the systems envisaged at the Junctions
3. The Junction Box for UPS with Battery bank needs to be considered separately
4. It should be noted that the MSI would have designed the Junction box keeping in mind the scalability requirements of ICCC project
5. The junction box should be designed in a way that, separate compartment will 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.
6. At selected traffic junctions, the infrastructure of poles and cantilevers will be provided by the client for mounting/installing the traffic light aspects. The details of such traffic junctions/locations are provided in Annexure VIII**.**

5.5.5 Cabling Infrastructure

1. The MSI shall provide standardized cabling for all devices and subsystems in the field.
2. 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.
3. 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.
4. Cabling must be carried out per relevant BIS standards. All cabling shall be documented in a cable plan by the MSI.

5.6 Design and Implementation of Integrated Command & Control Center System

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

1. Integrated Control and Command Centre

2. Data Centre
3. City Surveillance System
4. Variable Message Display
5. Environmental Sensors
6. Public Address System
7. Emergency Call Box/ Panic Button

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

5.6.1 Design, Supply, Installation & Commissioning of the Field Equipment

The Scope includes Supply, Installation, commissioning and Customization (as required) of various field systems which include Surveillance System, Variable Message Display (VMDs), Environmental Sensors, Public Address System, Emergency Call Box, etc. and other IT infrastructure required for successful operations of the ICCC project.

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

1. The implementation methodology and approach must be based on the global best practices in-order to meet the defined Service Levels during the operation.
2. Best efforts have been made to define major functionalities for each sub- system of ICCC system. However, MSI should not limit its offerings to the functionalities proposed in this RFP and is suggested to propose any functionality over and above what has already been given in this tender.
3. The MSI shall design the field level equipment architecture to ensure maximum optimization of network equipment, poles, cantilever, mounting infrastructures, power supply equipment including, electric meters and junction box.
4. Finally approved/accepted solution for each component of ICCC project shall be accompanied with "System Configuration" document and the same should be referenced for installation of ICCC systems at Junctions/Locations that are identified within the scope of this project.
5. The MSI shall be required to submit a detailed installation report post installation of all the equipment at approved locations. The report shall be utilized during the acceptance testing period of the project to verify the actual quantity of the equipment supplied and commissioned under the project.
6. The MSI shall be responsible for obtaining all permits and approvals necessary to install the ICCC systems components as per the approved design.

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

5.6.1.1 Surveillance System

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

1. The MSI shall install Surveillance System Cameras for CCTV monitoring and management at different locations across Ludhiana city.
2. Provision for Emergency Call Box and Public Address/Hooter System at identified locations
3. The MSI shall undertake due diligence for selection and placement of surveillance cameras to ensure the optimized coverage of the traffic junction and other locations along with all

associated junction arms, accuracy of the information captured on the field and for rugged operations.

4. The MSI shall design, supply, and install the surveillance cameras as defined in the RFP; all wiring connections for the system shall be installed by the MSI. The MSI shall supply all of the necessary equipment for the camera operations including camera housings and mountings, camera poles, switches, cabling, and shall make the final connections to the junction box.
5. The MSI shall be responsible for providing the entire necessary IT infrastructure for monitoring, recording, storage & retrieval of the video streams at ICCC or any other location as specified in the RFP.
6. For more details on technical and functional specifications of Surveillance Cameras, MSI should refer to Annexure I for Functional and Technical specifications.

5.6.1.2 Variable Message Display (VMD) Boards

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

1. The MSI shall install 10 digital VMD boards at identified locations across city of Ludhiana. These VMD boards shall have different characteristics depending upon the location and purpose of installation. VMD board displays are to be controlled through ICCC. The purpose of the VMD boards is to provide the commuters with information about traffic/congestion conditions and alternate routes/diversions in case of high traffic on roads.
2. The MSI, in consultation with LSCL can propose alternate locations apart from the locations mentioned in this RFP for installing the VMD boards where their effectiveness in communicating information about traffic conditions/other informations in Ludhiana will be maximized.
3. LSCL shall review and approve the proposed locations. The MSI shall install the VMD boards on the approved locations.
4. For more details on technical and functional specifications of VMD boards, the MSI should refer to Annexure I for functional requirements and technical specifications.

5.6.1.3 Environmental Sensors

MSI shall require to design and install the environmental sensors at 10 strategic locations to display environment related information through Variable Message Display Boards. The environment sensors shall be integrated with the central control system at ICCC to capture and display/ provide feed on Temperature, Humidity, and Pollutants etc. The data collected shall be location-marked. Each environmental Sensor should be able to measure following parameters:

- Temperature
- Humidity

- CO
- CO2
- NO2
- SO2
- PM 2.5
- PM 10

For more details on technical and functional specifications of Environemntal Sensors, the MSI should refer to Annexure I for functional requirements and technical specifications.

5.6.1.4 Public Address System

The scope of work for the MSI will include installation of Public Address System at identified location across the city.

The MSI will be responsible for design and implementation and maintenance of Public Adress System as per below requirements and should not be limited to:

a. The MSI will have to conduct a survey and finalize the location with LMC/LSCL

b. The MSI will be responsible for replacement, repair and periodic updation of PAS

c. During warranty period besides service/maintenance of Hardware, System Software and its Peripherals, all software up-gradation, bugs/patches and services shall be provided free of cost by the vendor

d. The MSI must not bid/supply any equipment that is likely to be declared end of sale within the 5 years from the Bid Date. The bidder would be required to replace all such equipments/faulty spares/peripherals with latest and at least of equivalent configuration if not better in such case.

e. The PAS will be used to disseminate information emergency information the citizens. Emergency situation shall include (but not limited to) Fire, Flood, Fog, Riots, Political Possessions etc.

f. PAS will also be used to provide traffic alerts, accidents, etc. to the commutters. This will help citizens to avoid such road.

g. Public Address System at junctions will be used by traffic control room to inform commuter about red light violation, zebra crossing encroachment etc.

h. MSI to make such provision that faulty PAS is noticed in the ICCC and respective authority is immediately informed to recity/replace the non functional equipments

For more details on technical and functional specifications of Public Address System, the MSI should refer to Annexure I for functional requirements and technical specifications.

5.6.1.5 Emergency Call Box/ Panic Button

Emergency Call Box/ Panic Button is an important component as far as safety aspect in the city is concerned. ECB will be installed at 50 locations across the city.

The MSI will be responsible for design and implementation and maintenance of Emergency Call Box/Panic Button as per below requirements and should not be limited to:

a. The MSI will have to conduct a survey and finalize the location with LMC/LSCL

b. The MSI will be responsible for replacement, repair and periodic updation of ECB/Panic Button

c. During warranty period besides service/maintenance of Hardware, System Software and its Peripherals, all software up-gradation, bugs/patches and services shall be provided free of cost by the vendor

d. The MSI must not bid/supply any equipment that is likely to be declared end of sale within the 5 years from the Bid Date. The bidder would be required to replace all such equipments/faulty spares/peripherals with latest and at least of equivalent configuration if not better in such case.

e. Emergency Call Box/Panic Button should be used by citizens to connect with authority at the time need or emergency

f. ECB/Panic Button shall be integrated with ICCC and control and command centre will convey message to local police to act immediately

g. ECBs should be vandal free and MSI to make sure that ECB/Panic Button should not be removed from where installed. Also MSI to make sure that ECB/Panic Button are not vandalized by miscreants

h. MSI to consult with Ludhiana Police/Traffic Department and LMC/LSCL and install ECBs/Panic Button in locations where there is provisioning of CCTV camera. This will help authority and ICCC to check and identify the individual pressing the panic button. This way authority will also be able to recognize if the panic button is pressed by some one in need or by some miscreant.

i. MSI to make such provision that faulty ECB/Panic Button is noticed in the ICCC and respective authority is immediately informed to recity/replace the non functional equipments

j. For more details on technical and functional specifications of Laying of OFC, the MSI should refer to Annexure I for functional requirements and technical specifications.

5.6.2 Design & Implementation of Artificial Intelligence System with Edge Analytics

The MSI shall be responsible for designing and implementing Advanced Video Analytics with supportive Artificial Intelligence System. This can implemented through either edge / hybrid/ DC

based advanced analytical solution. Decision on use cases to be implemented using edge devices would be taken during the design phase after finalisation on locations and approval from client. This advanced analytics system should be supported by continuous learning capabilities. **ICCC hence established by MSI shall have provision to displayof feed / analytics for the temporarily installed cameras. The number of cameras cannot be anticipated now.**

Following listed are the categories along with their associated use cases should be part of implementation and should be not be limited to:

A. Solid Waste Management/Vandalism use cases (Number of locations to be finalized by Client)

1. Graffiti and Vandalism detection
2. Debris and Garbage detection
3. Attendance of sanitation workers on site by face recognition
4. Sweeping and cleaning of streets/bins before and after
5. Garbage bin, cleaned or not
6. Litter detection
7. Tracking of garbage truck movement and Quantity of garbage dumped at dumpsite

B. Traffic Management use cases (Number of locations to be finalized by Client)

1. Parking violation
2. Speeding vehicle
3. Accident detection
4. 'Vehicle of interest' tracking by color, speed, number plate
5. Helmet detection on two wheeler
6. Unwanted/ banned vehicle detection
7. Wrong way or illegal turn detection

C. Citizens Safety use cases (Number of locations to be finalized by Client)

1. Detection and classification of human, animal and vehicle
2. Loitering detection
3. Person climbing barricade
4. Person collapsing
5. Person/Face recognition
6. Detection and Recognize the pattern of demonstration and conflicts in crowd
7. Gesture recognition : Identification through gesture change

8. Behavioral Biometry : Identification through multiple behavior

The MSI shall be responsible for implementing the above mentioned (but not limited to) analytics based use cases for Fixed Box/Fixed Bullet IR Cameras as per city requirements in below mentioned indicative combinations:

1. Any use cases of Solid Waste Management/Vandalism related as per city requirements
2. Any use cases of Traffic Management related as per city requirements
3. Any use case of Citizens Safety related as per city requirements

The MSI is expected to provide solution which can adopt to any complex form of data analytics. MSI to continously discuss with LSCL about the various use cases and implement them as part of their solution.

The MSI is expected to propose Edge / Hybrid / DC based analytical solution for above mentioned use cases. The Bidder is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards & best practices adopted in the industry. The Bidder is encouraged to design an Optimized solution which is technically superior, innovative, proven, better in terms of functionality and is cost effective.

5.6.2.1 Data Analytics Capabilities

The MSI is expected to provide solution which can adopt to any complex form of data analytics. MSI to continously discuss with LSCL about the various use cases and implement them as part of their solution. Minimum data analytics capabilities (but not restricted) is mentioned below:

a. The ICCC software solutions should have inbuilt capability of data analytics/ business intelligence.

b. The Data Analytics/ BI Tool of software solution should work as single platform for analyzing data coming/input from all the IT components/initiative of all smart cities (City Specific or State Wide initiative).

c. The system should be able to generate report in the user defined manner.

d. There should be a provision for a dash board which may take input from various system like individual sensors of multiple IT components (SCADA sensor, Environment sensors etc.)

e. Apart from basic analytics system should also have provision to perform Predictive Analysis.

f. User should be able to choose any permutation and combinations of data fields to perform predictive analysis.

g. System should be able to predict the events, make scenarios which helps in decision making to city authorities.

h. The Data analytics/BI tool should have ability to analyze the useful information and sharing it with general public. For example in case of water supply effected areas and traffic situation awareness etc.

i. System should have capabilities to suggest best response options on the basis of current and historic data sets.

j. Solution should enable the department to monitor activities and operations relating to the citizen (Municipal) service being provided, feedback and grievances received

k. Solution should help department understand the level of responsiveness of the officers concerned in terms of their response to the grievances.

l. The solution should also contain abilities for forecasting and scenario analysis, this will help the department understand the trends of different concern areas.

m. Forward looking decision making – BI and analytics tool provide the predictive and forecasting capabilities which can help department in forward looking policy and decision making.

n. Analysis of citizen sentiment across topics as represented through news and social media

o. Identification of recently emerging and trending topics of interest

p. Providing analytical platform for identification of misclassified events reported by citizens and inadequacies in action taken versus relief requested

q. System shall provide an Enterprise Reporting and Visualization solution to author, manage, and deliver all types of highly formatted reports

r. The solution should have mining, analytical and querying capabilities, and should be able to interoperate with other DBMS.

s. The BI Platform should have the capability to schedule reports on the basis of a time calendar i.e. by hour, day, week, month, etc.

t. The BI Platform should have the capability to schedule reports on the basis of a trigger or an occurrence such as an email, database refresh, etc.

u. Solution should provide capability to :

- Understand issues and concerns of citizens in a quick and effective manner
- Monitor progress of grievances and quality of grievance redressal
- Understand special / specific needs for different part of cities / subject areas affecting citizens (such as water, electricity etc.)

5.6.3 Design, Supply, Installation and Commissioning of Network & Backbone Connectivity for ICCC and other Smart Components

1. Network & Backbone Connectivity is an important components of the project and needs very careful attention in assessment, planning and implementation. It is important not only

to ensure that the required 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.

2. In order to meet the project requirements and SLA requirements as defined in this RFP, it has been decided that the MSI shall provision bandwidth/connectivity requirements as below:
    a. For all locations, where field infrastructure would be operational the MSI should consider the bandwidth/network connectivity requirements from field locations to Data Center/ICCC as defined in Annexure IX for 5 years from date of Go-Live
3. The provisioning of the PoPs for the City Network Backbone at the Junction and other field locations will be mutually agreed upon by the LSCL and the MSI for the ICCC project.
4. The MSI should provide a 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 Centre, and ICCC. All the components of the technical network architecture should be of industry best standard and assist MSI in ensuring that all the connectivity SLAs are adhered to during the operational phase.
5. 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. It is necessary that at least 70% of the proposed last mile connectivity should be wired. Last Mile to be defined as “the access link from the service provider’s PoP – (as per Telco Standards) to the field device”.
6. MSIs are also required to do the estimation of bandwidth requirements considering the functional requirement mentioned in the RFP
7. The actual bandwidth requirement to cater the above mentioned bandwidth parameters and to meet SLAs would be calculated by the MSI and the same shall be clearly proposed in the technical proposal with detail calculations. LSCL 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. LSCL reserves its right to ask the Master Systems Integrator to increase the bandwidth if the provided bandwidth is not sufficient to give the functionality of the system mentioned in the RFP and adhere to the SLAs.
8. In case the Telecommunication Guidelines of Government of India require the purchaser to place Purchase Order to the Service Provider for bandwidth, LSCL shall do so. However, Master Systems Integrator shall sign a contract with Telecom Service Provider(s) and ensure the performance. LSCL shall make payments to the Systems Integrator.
9. The MSI shall be required to submit a detailed installation report post installation of all the equipment at approved locations. The report shall be utilized during the acceptance testing

period of the project to verify the actual quantity of the equipment supplied and commissioned under the project.

5.6.4 Hosting Services

1. The infrastructure of Data Center for ICCC, and other city sub system etc. shall be hosted along with ICCC at the site identified.
2. The MSI need to do the sizing of rack space required at facilities based on its capacity planning and sizing for the entire duration of the contract with adequate space for future expansion.
3. All the requisite consumables like tapes, hard disks, etc. for backup shall be provided by the MSI as per the project requirements. All the tapes, hard disks, etc. once deployed for the project will become property of LSCL including corrupted/damaged devices.

5.6.5 Design, Supply, Installation and Commissioning of IT Infrastructure at Data Centre (DC) and ICCC

1. It is proposed that the MSI shall provide the IT hardware/software and Non-IT infrastructure at the following locations:

S. No.	Location Type	Location Name	Approximate Area	Indicative IT Infrastructure
1	Integrated Command & Operation Center (ICCC)	Ludhiana Municipal Corporation	4000 SFT	a. Video Wall 55" in 4*4 matrix b. Workstation with VMS Client License: 16 Nos c. IP Phones: 16 Nos d. Simulatneous Viewing Capability: All live Cameras feeds coming at the DC/ICCC
2	Data Center	At ICCC Site	400 SFT	a. DC Infrastructure will be available at State DC b. Servers c. Storage d. Network Switches
3	Cloud DC	Cloud Hosted	NA	Cloud Hosted ICCC & other applicable applications
4	Data Recovery	Cloud Hosted	NA	Cloud Hosted DR (Details provided in next section)

2. MSI has to ensure that redundancy is provided for all the key components to ensure that no single point of failure affects the performance of the overall system. It will be MSI's responsibility to supply, install and commission of IT Infrastructure including site preparation in DC, and ICCC
3. Cloud Data Centre developed by MSI should be as per Telecommunications Infrastructure Standard for Data Centers
4. Access to the Cloud Data Centre Space where the ICCC platform is hosted should be restricted and access be given only to the authorized personnel including Networking & Security Infrastructure and other associated ICT Components.
5. The MSI shall provide system integration services to customize and integrate the applications procured through the project. The ICCC system applications proposed by the MSI should have open APIs and should be able to integrate and share the data with other third party systems already available or coming up in the near future
6. As part of preparing the final bill of material for the cloud data center, the successful MSI will be required to list all passive & active components required in the data centers.
7. The bill of material proposed by the successful MSI will be approved by LSCL for its supply and installation. Indicative IT Infrastructure to be commissioned as part of the ICCC project at Data Centre/ICCC are as under:
    a. Servers (inclusive of OS) - Application Servers, Database Server, Video Recording Server, Video Management Server, Enterprise Backup Server, Domain Controller, Failover Servers for application and Recording Servers
    b. Application & System Software (with necessary customization) – Video Management System application, Variable Message Display application, Emergency Call Box, Command & Control Centre Application, etc.
    c. RDBMS (if required)
    d. Anti-Virus Software
    e. Primary Storage Solution
    f. Storage Management Solution
    g. Core Router
    h. Switches (PoE+)
    i. NGFW Next Generation Firewall
    j. HIPS (Host intrusion prevention system)
    k. IP Phones
    l. Racks
    m. All required Passive Components

n. Any other Server required to the cater to the scope of work mentioned in this

8. The bidder is expected to calculate and design the IT Infrastructure requirements including compute, storage and video management software licences etc. required for real-time monitoring, recording and integration of IP CCTV (PTZ and Fixed Box) Cameras. The supply, installation and connectivity till ICCC of the provided cameras will be in their scope. MSI is expected to capture and propose the IT Infrastructure for successful oprations and integrations of the same. The following table provides the details of proposed cameras:

S. No.	No. of Locations	Approximate No. of Cameras	Remarks
1	To be decided in consultation with Authority during design phase.	300 nos	Permanent infrastructure for City Area

9. The above are only indicative requirements of IT & Non-IT Infrastructure requirements at DC/ICCC. The exact quantity and requirement shall be proposed as part of the technical proposal of the MSI.
10. The MSI shall prepare the overall data centers establishment & their operational plan for this project. The plan shall comprise of deployment of all the equipment required under the project. The implementation roll-out plan for setting up the data centers shall be approved by LSCL. The detailed plan shall be also comprise of the scalability, expandability and security that such data centers will implement under this project.
11. The MSI shall establish a state of the art ICCC, the key components for the same will be as follows:
    a. Video Wall system
    b. Operator workstations
    c. IP Phones
    d. Active Networking Components (Switches, Routers)
    e. Passive Networking Components
    f. Electrical Cabling and Necessary LED Illumination Devices
    g. Office Workstations
    h. UPS (as per the requirement mentioned in the Technical Specification)
12. The MSI shall be required to submit a detailed installation report post installation of all the equipment at approved locations. The report shall be utilized during the acceptance testing period of the project to verify the actual quantity of the equipment supplied and commissioned under the project.

5.6.6 Design and Implementation of Disaster Recovery Infrastructure for ICCC project

1. MSI shall propose to host Applications and storage on cloud for complete Data Recovery (DR) operations. Applications should fail-over to the cloud in case of DR. The MSI would have to Design the DR according to RTO /RPO criteria, which would be defined during the design phase.
2. DR shall be implemented based on managed cloud services and shall adhere to guideline issued by MeitY over time to time. SLA for DR shall be as per MeitY guideline.
3. MSI may propose the Cloud Service Provider from the empaneled vendors of MeitY.
4. Below are the key factors to be considered for cloud hosting -
    a. The MSI is required to prepare and submit along with their technical proposal, the details of methodologies and computations for sizing and capacity of storage, compute, backup, network and security.
    b. There should be logical separation (of space, servers, storage, network infrastructure and networks) to protect data, applications and servers on Private cloud.
    c. It is expected that bidder will make all necessary provision to ensure high availability at the Data Centre and after switch over to the DR; it gets back in to normal operations from the DC as soon as possible.
    d. One full-scale DR drill to be conducted after go-live and additional DR Drills on half yearly basis shall be conducted.
    e. The system will be hosted in the site identified by the MSI and as agreed by the LSCL for DR (backup only).
    f. There should be sufficient capacity (compute, network and storage capacity offered) available for near real time provisioning (as per the SLA requirement of the LSCL) during any unanticipated spikes in the user load.
    g. DR site will be located in India only.
    h. Ensure redundancy at each level.
    i. MSI shall provide interoperability support with regards to available APIs, data portability etc. for the LSCL to utilize in case of Change of cloud service provider, migration back to in-house infrastructure, burst to a different cloud service provider for a short duration or availing backup or DR services from a different service provider.
    j. The MSI is fully responsible for tech refreshes, patch management and other operations of infrastructure that is in the scope of the MSI.
    k. LSCL retains ownership of all virtual machines, templates, clones, and scripts/applications created for the LSCL's application. LSCL retains the right to request (or should be able to retrieve) full copies of these virtual machines at any time

l. Provide a robust, fault tolerant infrastructure with enterprise grade SLAs with an assured uptime of 99.999%, SLA measured at the VM Level & SLA measured at the Storage Levels

m. Cloud services should be accessible via internet and MPLS.

n. Required Support to be provided to the LSCL in migration of the VMs, data, content and any other assets to the new environment created by the LSCL or any Agency (on behalf of the LSCL) on alternate cloud service provider's offerings to enable successful deployment and running of the LSCL's solution on the new infrastructure.

o. The MSI should configure, schedule and manage backups of all the data including but not limited to files, folders, images, system state, databases and enterprise applications

- Perform and store data and file backups consisting of an initial full back up with daily incremental backups for files;
- For the files, perform weekly backups;
- For the databases, perform a twice weekly full database backup, with a three times daily backup of database log files
- Encryption of all backup files and data and management of encryption keys as a service that can be enabled for Government Departments that require such a service.
- Retain database backups for thirty (30) days

p. The MSI should offer dashboard to provide visibility into service via dashboard.

q. MSI shall not delete any data at the end of the agreement (for a maximum of 45 days beyond the expiry of the Agreement) without the express approval of the LSCL.

Preparation of Disaster Recovery Operational Plan

The MSI should provide detailed operating procedures for each application during the following scenarios. These will be mutually agreed upon with LSCL 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 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

Configure proposed solution for usage

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

#	Features
1	The proposed solution must offer a workflow based management & monitoring and reporting capability for the real time monitoring of a DR solution parameters like RPO (at DB level), RTO, replication status and should provide alerts(including SMS and e-mail alerts) on any deviations. The proposed solution should be able to conduct DR Drills from a centralized location
2	The proposed solution should provide a single dashboard to track DR Readiness status of all the applications under DR
3	The proposed solution should be capable of reporting important health parameters like disk space, password changes, file addition/deletion etc. to ensure DR readiness
4	The proposed solution should have inbuilt ready to use library of recovery automation action for heterogeneous databases and replication environment. This must significantly reduce custom development of scripts and speedy deployment of DR solutions
5	The proposed solution should facilitate out-of-the-box, workflow based switchover and switchback for DR drills for standard applications based on industry best practices
6	The proposed solution should facilitate workflows for bringing up the applications and all the components it depends on at DR while it is up at primary site without pausing/stopping the replication
7	The proposed solution should be able to manage hosts by either deploying agents or without deploying any agent and should not require any change in the existing environment
8	The proposed solution must support all major platforms including Linux, Windows, Solaris, HP-UX, and AIX with native high availability options. It must support both physical and virtual platforms
9	The proposed solution should facilitate workflow based, single-click recovery mechanism for single or multiple applications
10	The proposed DRM solution should integrate seamlessly with the existing setup without the need to reconfigure or remove existing application setup including clusters
11	The proposed solution should cover all the functionalities mentioned in the specifications and all the required licenses should be provisioned

Periodic Disaster Recovery Plan Update

The service provider shall be responsible for –

a. Devising and documenting the DR policy discussed and approved by Authority.

b. Providing data storage mechanism with from the Go-Live date till the date of contract expiry for the purpose of compliance and audit

5.7 Responsibility Matrix

#	Key Activities	MSI==	LSCL	PMC	Exisitng ICT Vendors at LSCL
Project Inception Phase					
1	Project Kick Off	R/A	C	C	I
2	Deployment of manpower	R/A	C	C	I
Requirement Phase					
3	Assess the requirement of IT Infrastructure and Non IT Infrastructure	R/A	C	C	C
4	Assessment of Business processes	R/A	C	C	I
5	Assessment of requirement of Software requirements	R/A	C	C	I
6	Assess the Integration requirement	R/A	C	C	C
7	Assess the connectivity requirement all locations (including Building)	R/A	C	C	I
8	Assessment the Network laying requirement	C	C	C	I
9	Assessment of training requirement	R/A	C	C	I
Design Phase					
10	Develop the Concept of Operations (CONOPS)	R/A	C	C	I
11	Formulation of Solution Architecture	R/A	C	C	I
12	Detailed Design of Smart City Solutions	R/A	C	C	I
13	Development of test cases (Unit, System Integration and User Acceptance)	R/A	C	C	I
14	Preparation of final bill of quantity and material	R/A	C	C	I
15	SoP & KPIs preparation	R/A	C	C	I
Development Phase					
16	Helpdesk setup	R/A	C	C	I
17	Physical Infrastructure setup	R/A	C	C	I

#	Key Activities	MSI==	LSCL	PMC	Exisitng ICT Vendors at LSCL
18	Procurement of Equipment , edge devices, COTS software (if any), Licenses	R/A	C	C	I
19	IT and Non IT Infrastructure Installation	R/A	C	C	I
20	Development, Testing and Production environment setup	R/A	C	C	I
21	Software Application customization (if any)	R/A	C	C	I
22	Development of Bespoke Solution (if any)	R/A	C	C	I
23	Integration with Third party services/ application (if any)	R/A	C	C	I
24	Unit Testing	R/A	C	C	I
25	Implementation of Solutions	R/A	C	C	I
26	Preparation of User Manuals , training curriculum and training materials	R/A	C	C	I
27	Role based training(s) on the Smart City Solutions	R/A	C	C	I
UAT					
28	User Acceptance Testing	A	R	C	I
Go –Live					
29	Go Live	R/A	C	C	I
Operation and Maintenance					
30	Operation and Maintenance of IT, Non IT infrastructure and Applications	R/A	C	C	I
31	SLA and Performance Monitoring	R/A	C	C	I
32	Logging, tracking and resolution of issues.	R/A	C	C	I
33	Application enhancement	R/A	C	C	I
34	Patch & Version Updates	R/A	C	C	I
35	Helpdesk services	R/A	C	C	I

Note: All decisions will be taken by LSCL which will be abided by all the stakeholders in the above matrix.

R/A = Responsible/Accountable

C = Consulted

I = Informed

5.8 Project Deliverables

#	Key Activities	Deliverables
Project Inception Phase		
1	Project Kick Off	1. Project Development Plan 2. Risk Management and Mitigation Plan 3. Project tracebility matrix
2	Deployment of manpower	
Requirement Phase		
3	Assess the requirement of IT Infrastructure and Non IT Infrastructure	1. Functional Requirement Specification Document 2. System Requirement Specification document (SyRS) 3. System Architecture document 4. Test strategy 5. Site Survey Report 6. Final Bill of Quantity 7. Updated tracebility matrix
4	Assessment of Business processes	
5	Assessment of requirement of Software requirements	
6	Assess the Integration requirement	
7	Assess the connectivity requirement for field locations (including Building)	
8	Assessment the Network laying requirement	
9	Assessment of training requirement	
Design Phase		
10	Develop the Concept of Operations (CONOPS)	1. HLD documents 2. LLD documents 3. Application architecture documents 4. Technical Architecture documents 5. Network Architecture documents 6. Interface specification (for all the integeration modules) 7. GUI design (screen design, navigation, etc.) 8. Test Plans 9. Security Plan 10. Training Plan 11. SoPs and KPIs 12. Change management Plan 13. Updated tracebility matrix
11	Formulation of Solution Architecture	
12	Detailed Design of Smart City Solutions.	
13	Development of test cases (Unit, System Integration and User Acceptance)	
14	Preparation of final bill of quantity and material	
15	SoP and KPI preparation	
16	Helpdesk setup	
17	Procurement of Equipment , edge devices, COTS software (if any), Licenses	1. IT and Non IT Infrastructure Installation Report 2. Integration Testing Report 3. Training Completion report
18	IT and Non IT Infrastructure Installation	

#	Key Activities	Deliverables
19	Development, Testing and Production environment setup	4. Application deployment and configuration report 5. Project tracebility matrix
20	Network connectivity (All activities other that bandwidth provisioning)	
21	Software Application customization	
22	Development of Bespoke Solution (if any)	
23	SoP and KPI implementation	
24	Integration with Third party services/application (if any)	
25	Unit and integration Testing	
26	Preparation of User Manuals , training curriculum and training materials	
27	Role based training(s) on the Smart City Solutions	
UAT		
28	User Acceptance Testing	1. Completion of UAT and closure of observations report 2. Project tracebility matrix
Go –Live		
29	Go Live	1. Go-Live Report 2. Project tracebility matrix
Operation and Maintenance		
30	Operation and Maintenance of IT, Non IT infrastructure and Applications	1. Detailed plan for monitoring of SLAs and performance of the overall system 2. Fortnightly Progress Report 3. Monthly SLA Monitoring 4. Report and Exception Report 5. Quarterly security Report 6. Issues logging and resolution report 7. Project tracebility matrix
31	SLA and Performance Monitoring	
32	Logging, tracking and resolution of issues.	
33	Application enhancement	
34	Patch Updates	
35	Helpdesk services	

5.9 Project Timelines

The project is envisaged to be implemented within **09 months** upon issue of the Work Order.

Operations and management of the entire system including its sub systems, customer support and responsibility as per SLAs for the duration of **4 years post successful implementation**.

List of the broad activities to be carried out by the Systems Integrator and the timelines from the date of Work Order are given in the table below. “D” stands for the date of issue of the Work Order.

Sr. No.	Deliverables	Time Schedule
1	Completion of Scoping and feasibility study (Inception Phase)	D+ 1 Month
2	Installation, Integration, Commissioning and Go-Live of ICCC (Phase I) 1. ICCC - IT hardware 2. ICCC - Non-IT equipment 3. ICCC – software 4. Data Center Cloud – Hardware 5. Data Center Cloud- Software 6. Data Center (DC) – Hardware 7. Data Center (DC) – Software 8. Data Center (DC) – Non-IT equipment 9. DR – Hardware 10. DR – Software 11. DC-DR link 12. Implementation and Integration of City Surveillance System – 300 Cameras 13. Implementation and Integration of 10 Variable Message Display (VMD) Boards at different identified Locations 14. Implementation and integraton of 50 ECB/Panic Button 15. Implementation and integration of 50 Public Address System 16. Implementation and Integration of 10 Environmental Sensors 17. DR Services 18. Integeration with other phase I components such as city surveillance, smart governance, smart LED light, smart traffic and SWM	D+ 6 Months
3	Integration of Smart elements of Phase II	D + 9 Months

6. Annexure I- Functional Requirements & Technical Specifications

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

6.1 Integrated Command and Control Centre (ICCC) - Technical Specifications & Functional specifications

6.1.1 Integrated Command and Control Center Application

#	Parameters	Minimum Specifications	Bidder Compliance	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	Solution & Platform	The Command & Control solution should be implemented and complied to the industry open standards based Commercial-of-the-shelf (COTS) products. The platform will be hosted at cloud and will operate on SaaS or PaaS model.		
4.		Must have built-in fault tolerance, load balancing and high availability & must be certified by the OEM.		
5.		Software (Application, Database and any other) must not be restricted by the license terms of the OEM from scaling out on unlimited number of cores and servers during future expansion.		
6.		System must provide a comprehensive API (Application Program Interface) or SDK (Software Development's Kit) to allow interfacing and integration		

#	Parameters	Minimum Specifications	Bidder Compliance	Product Documentation Reference
		with existing systems, and future application and sensors which will be deployed on the field.		
7.		The solution should be network and protocol agonistic and provide option to connect legacy system through API's with either read, write or both options. It should connect diverse on premise and/or cloud platform's and make it easy to exchange data and services between them.		
8.		The system shall allow seamless integration with all of the department's existing and future initiatives (as mentioned in Section 7.1.5)		
9.		The platform should be able to integrate with any type of sensor platform being used for the urban services irrespective of the technology used.		
10.		The platform should be able to normalize the data coming from different devices of same type (i.e. Different lighting sensor from different OEMs, different energy meters from different OEMs etc.) and provide secure access to that data using data API(s) to application developers		
11.	Convergence of Multiple feeds / services	System need to have provision that integrates various services and be able to monitor them and operate them. The solution should provide option to integrate existing deployed solution by City and also need to provide scalability option to implement new use cases.		

#	Parameters	Minimum Specifications	Bidder Compliance	Product Documentation Reference
		System should support DDE and OLE for integration with Process control systems and sensors System should have capability to source data from various systems implemented in Ludhiana City to create actionable intelligence		
12.	Industry Standards for the Command & Control Center	The solution should adhere to the Industry standards for interoperability, data representation & exchange, aggregation, virtualization and flexibility		
13.		IT Infrastructure Library (ITIL) standards for Standard Operations Plan & Resource Management		
14.		Geo Spatial Standards like GML & KML etc.		
15.		Business Process Model and Notation (BPMN) or equivalent for KPI Monitoring.		
16.	Command & Control Center Components	• Web server to manage client requests. Client should provide web-based, one-stop portals to event information, overall status, and details. The user interface (UI) to present customized information in various preconfigured views in common formats. All information to be displayed through easy-to-use dashboards.		

#	Parameters	Minimum Specifications	Bidder Compliance	Product Documentation Reference
17.		• Application server to provide a set of services for accessing and visualizing data. Should be able to import data from disparate external sources, such as databases and files. It should provide the contacts and instant messaging service to enable effective, real-time communication. It should provide business monitoring service to monitor incoming data records to generate key performance indicators. It should also provide the users to view key performance indicators, standard operating procedures, notifications, and reports, spatial-temporal data on a geospatial map, or view specific details that represent a city road, building or an area either on a location map, or in a list view. The application server should provide security services that ensure only authorized users and groups can access data. • System Platform – The platform should provide a common data integration layer which can collect and contextualize information from disparate data sources regardless of protocol. The platform should support templatization to allow "build once-deploy everywhere" functionality. • Workflow and Incidents		

#	Parameters	Minimum Specifications	Bidder Compliance	Product Documentation Reference
		Lifecycle engine – This function should allow users to define and modify new worflows. The workflow could cut across multiple systems via the interfacing modules. Workflow for operational alerts and escalations should be triggered automatically without human intervention. Workflow approvals should have facility to approve from any device with e-signature. This function should provide facility to trigger a corrective action workflow and define the stakeholders for the same. Should manage the life cycle of incidents and related entities via pre-define workflows. The workflow could cut across multiple systems via the interfacing modules. Workflow for operational alerts and escalations should be triggered automatically without human intervention. • Incidents Planning – should manage the planning preparations of an incident including resource allocation, tasks management etc. • Analytics and MIS – should provide users with business analytics reporting and tools to organize, evaluate and efficiently perform day to day operations • Security & Roles – should		

#	Parameters	Minimum Specifications	Bidder Compliance	Product Documentation Reference
		manage roles definition for internal as well as external access • Centralized data archiving for operational data : Should provide facility for centralized storage of operational data (time-series or transactional) with high granularity and data compression capability • Mobility: should enable app-based access to monitor alerts, KPI ,KOPs, SOPs and reports to mobile users. Should support popularly user's smartphone /tablets. App content should be presented in context to the user role.		
18.	Incident Management Requirements	The system must provide Incident Management Services to facilitate the management of response and recovery operations:		
19.		Should support comprehensive reporting on event status in real time manually or automatically by a sensor/CCTV video feeds.		
20.		Should support for sudden critical events and linkage to standard operating procedures automatically without human intervention.		
21.		Should support for multiple incidents with both segregated and/or overlapping management and response teams.		
22.		Should support Geospatial rendering of event and incident information.		
23.		Should support plotting of area of impact using polynomial lines to		

#	Parameters	Minimum Specifications	Bidder Compliance	Product Documentation Reference
		divide the area into multiple zones on the GIS maps.		
24.		Should support incorporation of resource database for mobilizing the resources for response.		
25.		Should provide facility to capture critical information such as location, name, status, time of the incident and be modifiable in real time by multiple authors with role associated permissions (read, write). Incidents should be captured in standard formats to facilitate incident correlation and reporting.		
26.		The system must identify and track status of critical infrastructure / resources and provide a status overview of facilities and systems		
27.		Should provide detailed reports and summary views to multiple users based on their roles.		
28.		A Reference Section in the tool must be provided for posting, updating and disseminating plans, procedures, checklists and other related information.		
29.		Provide User-defined forms as well as Standard Incident Command Forms for incident management.		
30.	Integrated User Specific & Customizable Dashboard	Should provide integrated dashboard with an easy to navigate user interface for managing profiles, groups, message templates, communications, tracking receipts and compliance		

#	Parameters	Minimum Specifications	Bidder Compliance	Product Documentation Reference
31.		• Collects major information from other integrated City sensors/platforms. • Should allow different inputs beyond cameras, such as, PC screen, web page, and other external devices for rich screen layout • Multi-displays configurations • Use of, GIS tool which allows easy map editing for wide area monitoring (Google map, Bing map, ESRI Arc GIS map, etc.).		
32.		Should provide tools to assemble personalized dashboard views of information pertinent to incidents, emergencies & operations of command center		
33.		Should provide historical reports, event data & activity log. The reports can be exported to pdf or html formats.		
34.		Should provide dashboard filtering capabilities that enable end-users to dynamically filter the data in their dashboard based upon criteria, such as region, dates, product, brands, etc. and capability to drill down to the details		
35.	Integration with Social Media & Open Source Intelligence	Should provide integration of the Incident Management application with the social media. Should Provide analytics based on the social media feed collected from the open source intelligence and collate with the surveillance inputs to alert the responders for immediate action on the ground.		
36.		Should extract messages and		

#	Parameters	Minimum Specifications	Bidder Compliance	Product Documentation Reference
		display it in an operational dashboard.		
37.		Should be able to correlate the extracted message from the social media with existing other events and then should be able to initiate an SOP.		
38.		Should be able to identify the critical information and should be able to link it to an existing SOP or a new SOP should be started.		
39.		Should provide notifications to multiple agencies and departments (on mobile) that a new intelligence has been gathered through open source/social media.		
40.	Device Status, Obstruction Detection and Availability Notification	Should provide icon based user interface on the GIS map to report non-functional device.		
41.		Should also provide a single tabular view to list all devices along with their availability status in real time.		
42.		Should provide User Interface to publish messages to multiple devices at the same time.		
43.	Event Correlation	Command & Control Center should be able to correlate two or more events coming from different subsystems (incoming sensors) based on time, place, custom attribute and provide correlation notifications to the operators based on predefined business and operational rules in the configurable and customizable rule engine.		

#	Parameters	Minimum Specifications	Bidder Compliance	Product Documentation Reference
44.	Standard Operations Procedures (SOP)	Command & Control Center should provide for authoring and invoking un-limited number of configurable and customizable standard operating procedures through graphical, easy to use tooling interface.		
45.		Standard Operating Procedures should be established, approved sets of actions considered to be the best practices for responding to a situation or carrying out an operation.		
46.		The users should be able to edit the SOP, including adding, editing, or deleting the activities.		
47.		The users should be able to also add comments to or stop the SOP (prior to completion).		
48.		There should be provision for automatically logging the actions, changes, and commentary for the SOP and its activities, so that an electronic record is available for after-action review.		
49.		The SOP Tool should have capability to define the following activity types:		
50.		**Manual Activity** - An activity that is done manually by the owner and provide details in the description field.		
51.		**Automation Activity** - An activity that initiates and tracks a particular work order and select a predefined work order from the list.		
52.		**If-Then-Else Activity** - A conditional activity that allows branching based on specific criteria.		

#	Parameters	Minimum Specifications	Bidder Compliance	Product Documentation Reference
		Either enter or select values for Then and Else.		
53.		**Notification Activity** - An activity that displays a notification window that contains an email template for the activity owner to complete, and then sends an email notification.		
54.		**SOP Activity** - An activity that launches another standard operating procedure.		
55.	Key Performance Indicator	Command & Control Center should be able to facilitate measurement or criteria to assay the condition or performance of departmental processes & policies.		
56.		**Green** indicates that the status is acceptable, based on the parameters for that KPI, no action is required.		
57.		**Yellow** indicates that caution or monitoring is required, action may be required.		
58.		**Red** indicates that the status is critical and action is recommended.		
59.	Reporting Requirements	Command & Control Center should provide easy to use user interfaces for operators such as Click to Action, Charting, Hover and Pop Ups, KPIs, Event Filtering, Drill down capability, Event Capture and User Specific Setup		
60.		The solution should generate Customized reports based on the area, sensor type or periodic or any other customer reports as per choice of the administrators		

#	Parameters	Minimum Specifications	Bidder Compliance	Product Documentation Reference
61.	Collaboration Tools	Should provide tools for users to collaborate & communicate in real-time using instant messaging features.		
62.	Communication Requirements	The solution should adhere to the below mentioned communication requirements.		
63.		Provide the ability to search/locate resources based on name, department, role, geography, skill etc. for rapidly assembling a team, across department, divisions and agency boundaries, during emergency		
64.		Provide the capability to Invite - Using information provided during the location of those individuals or roles, invite them to collaborate and to share valuable information.		
65.		Provide a single web based dashboard to send notifications to target audiences using multiple communication methods including voice-based notification on PSTN/Cellular, SMS, Voice mail, E-mail and Social Media		
66.		The solution should provide Dispatch Console integrates with various communication channels. It should provide rich media support for incidents, giving dispatchers the power to consolidate information relating to an incident and instantly share that information among responder teams. It should assess the common operating picture, identify & dispatch mobile resources available nearby the incident location. Augment		

#	Parameters	Minimum Specifications	Bidder Compliance	Product Documentation Reference
		resources from multiple agencies for coordinated response.		
67.	Authentication	Use authentication information to authenticate individuals and/or assign roles.		
68.	Instant messaging	Provide ability to converse virtually through the exchange of text, audio, and/or video based information in real time with one or more individuals within the emergency management community.		
69.	Events and Directives control	Should provide the capability for the events that are produced from a sub- system and are forwarded to the Command & Control Center. Events could be a single system occurrence or complex events that are correlated from multiple systems. Events could be ad hoc, real-time, or predicted and could range in severity from informational to critical. At the Command & Control Center, the event should be displayed on an operations dashboard and analysed to determine a proper directive.		
70.		Directives issued by the Command & Control Center should depend on the severity of the monitored event. Directives will be designed and modified based on standard operating procedures, as well as state legislation. A directive could be issued automatically via rules, or it could be created by the operations team manually.		
71.	Resource & Route	The system should provide the software component for the		

#	Parameters	Minimum Specifications	Bidder Compliance	Product Documentation Reference
	Optimization	message broadcast and notification solution that allows authorized personal and/or business processes to send large number of messages to target audience (select-call or global or activation of pre-programmed list) using multiple communication methods including SMS, Voice (PSTN/Cellular), Email and Social Media.		
72.	Alert & Mass Notification Requirements	Provide a single web based dashboard to send notifications to target audiences using multiple communication methods including voice-based notification on PSTN/Cellular, SMS, Pager, Voice mail, E-mail and Social Media		
73.		Provide function for creating the alert content and disseminating to end users. Provision of alerting external broadcasting organizations like Radio, TV, Cellular, etc., as web-service.		
74.		Provide Role based security model with Single-Sign-On to allow only authorized users to access and administer the alert and notification system.		
75.	Security & Access Control	Provide comprehensive protection of web content and applications on back-end application servers, by performing authentication, credential creation and authorization.		
76.	Internet Security	Comprehensive policy-based security administration to provide all users specific access based on user's responsibilities. Maintenance of authorization policy in a central		

#	Parameters	Minimum Specifications	Bidder Compliance	Product Documentation Reference
		repository for administration purposes.		
77.	Authorization	Should support to enable assignment of permissions to groups, and administration of access control across multiple applications and resources. Secure, web-based administration tools to manage users, groups, permissions and policies remotely		
78.	User group	Provide policies using separate dimensions of authorization criteria like Traditional static Access Control Lists that describe the principals (users and groups) access to resource and the permissions each of these principals possess.		
79.	Provide multi-dimensional access control	SSO to Web-based applications that can span multiple sites or domains with a range of SSO options.		
80.	Flexible single sign-on (SSO)	Support LDAP authentication mechanism		
81.	Authentication	Should have ability to respond to real-time data with intelligent & automated decisions		
82.	Rule Engine & Optimization	Should provide an environment for designing, developing, and deploying business rule applications and event applications.		
83.		The ability to deal with change in operational systems is directly related to the decisions that operators are able to make		
84.		Should have at-least two complementary decision		

#	Parameters	Minimum Specifications	Bidder Compliance	Product Documentation Reference
		management strategies: business rules and event rules.		
85.	Situational Awareness COP (Common Operational Picture)	• The CCA should be able to combine data from various sources and present it as different views tailored to different operator's needs. • The CCA should automatically update the information based on alarms and incidents that are presented to it via the business rules engine. The polling and CCA database refresh cycle shall be configurable to match the status of the situation (whether there is an emergency or crisis or just monitoring only). • Common Operational Picture 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 e.g. household affected by a transformer shut down o Timeline view of the situation Suggested actions from the system with their status		

#	Parameters	Minimum Specifications	Bidder Compliance	Product Documentation Reference

86.	Task Management	• The system should be able to create, assign, track and report on the lifecycle of tasks during a particular incident.
		• The system should allow a particular task to be decomposed into sub-tasks.
		• The system should provide an easy to interpret management dashboard view of the progress of all tasks during an incident.
		• The system should be able to organise the visual representation of tasks into prioritized list, filtered list, as well as colour coded representation for ease of understanding.
		• The system should be able to perform the following functions around task management:
		  ○ Create a task with unique ID. (Subtasks shall follow parent ID with second level numbering).
		  ○ Assign a target completion date and time for the task, either directly or as a time-span from the task's creation.
		  ○ Date and time stamp of the creation of the task.
		  ○ Log and track status of tasks. System should provide capability to define status of tasks during its lifecycle. These status definitions could be		

#	Parameters	Minimum Specifications	Bidder Compliance	Product Documentation Reference
		mapped to other task attributes such as the task type. ○ Key-word search against task list. • The above attributes shall be colour coded. • The system shall allow the tasks to be filtered on the real-time dashboard by agency then by task status. This filtering should allow an operator to filter for all tasks of a particular state or a combination of state; and by the time remaining until (or time elapsed since) the target completion time. • The system should allow multiple individual workstations to select specific agencies of interest on each workstation simultaneously. • The system should allow the LSCL to display all agencies' tasks simultaneously as well. • The tasks should be displayed on a real-time timeline. **The criticality of tasks should be dynamically changed depending on the performance of the incident response.**		
87.	Timeline and Charting	• The system should provide a facility to see incidents and actions (tasks) added to the CCA in a tabular list form as well as GANTT chart format filtered by day, week, month, year or any specific date range. • The system should provide a		

#	Parameters	Minimum Specifications	Bidder Compliance	Product Documentation Reference

		facility to see incidents, actions and interdependencies between actions in a clear visual graphical manner.
		• The system should be able to filter the information based on at least the following parameters:
		  ○ Incident information
		  ○ Resources information
		  ○ Agency type
		  ○ Tasks
		  ○ Criticality or priority		

88.	GIS Display	• Shall view the environment through geospatial or fixed composite computer-generated (JPEG, BMP, AutoCAD, etc.) map • Should allow user to view sensor and related name from the displayed map • Should allow all resources, objects, sensors and elements on the map to be geo-referenced such that they have a real world coordinate. • Should visually display a camera sensor with related camera orientation, camera range and camera field of view angle. • Should visually display an alarming sensor on map • Should visually differentiate sensor alarm severities on map through different color and icon identifiers • Should immediately view alarm details (including description, video, etc.) and investigate the alarm from the map		

#	Parameters	Minimum Specifications	Bidder Compliance	Product Documentation Reference
		• Should allow user to choose camera and other sensors from map to view live video and the data • Should allow user to choose camera and take live video image snapshot and save to file from any camera • Should allow user to choose camera from map to move PTZ cameras • Should allow user to choose camera to play, pause, stop, fast-forward, rewind, and play recorded video from preset time • Should allow user to choose camera and take recorded video image snapshot and save to file or print from any live or recorded video • Should allow user to jump from one map to the next with a single click of a mouse with map links • Should allow map information "layers" to be displayed/hidden on items such as – o Sensor names o Sensors o Sensor range (e,g. camera – orientation, range, field of view angle) o Locations and zones o Perimeter ranges o Resource tracks Allow user to zoom in/out on different regions of map graphic		
89.	Video Display	• Shall view live or recorded video from resizable and		

#	Parameters	Minimum Specifications	Bidder Compliance	Product Documentation Reference
		movable windows • Should have an ability to perform video controls for video systems from workstation • Shall play, fast-forward, rewind, pause, and specify time to play recorded video • Shall take a video still image (snapshot) from live or recorded video • Shall export video for user specified time and duration • Shall have the capability to move PTZ cameras • Shall view Video in Video Matrix • Shall display in 1x1, 2x2, 3x3 and 4x4 window formats • Shall enable operator to specify video windows to be displayed in matrix • Shall enable matrix settings to be saved per user • Shall view either live or recorded video can be displayed in the video matrix window. • Shall enable video snapshot to be taken and saved from any window pane in the matrix view • Shall rotate video in “virtual” video guard tour • Shall rotate through multiple video views based on predefined video camera sequence and duration. • Shall enable the user to pause the rotation of video and resume the video rotation again • Shall enable times between new		

#	Parameters	Minimum Specifications	Bidder Compliance	Product Documentation Reference
		video to be adjusted • Shall enable both live video and recorded video to be played through the video guard tour. • Shall enable alarms to be generated from any video pane • Shall enable user to only view and control video for which they have been assigned permissions by the administrator • Shall manually create an alarm from the live or recorded video with specified severity and description		
90.	Alarm Display	• Should have an ability to display alarm condition through visual display and audible tone • Should have an ability to simultaneously handle multiple alarms from multiple workstations • Should have an ability to automatically prioritize and display multiple alarms and status conditions according to pre-defined parameters such as alarm type, location, sensor, severity, etc. • Should display the highest priority alarm and associated data / video in the queue as default, regardless of the arrival sequence		
91.	Historical Alarm Handling	• Should have an ability to view historical alarms details even after the alarm has been acknowledged or closed.		

#	Parameters	Minimum Specifications	Bidder Compliance	Product Documentation Reference
		• Should have an ability to sort alarms according to date/time, severity, type, and sensor ID or location.		
92.	Alarm Reporting	• Should have an ability to generate a full incident report of the alarm being generated. • Should have an ability to display report on monitor and print report • Should have details of alarm including • severity, time/date, description and location • Captured video image snapshots • Relevant sensor data such as SCADA sensors • Response instructions • Alarm activities (audit trail) • Should have an ability to export alarm report in various formats including pdf, jpeg, html, txt, and mht formats • Should have an ability to generate an alarm incident package including the full incident report and exported sensor data from the incident in a specific folder location.		
93.	Alarm Policies and Business Logic Administration	• The CCA solution should have the following ability to handle the workflow alarms through graphical user interface. • Should have an ability to match keywords or text from the alarming subsystem's incident description to raise an alarm using criteria including exact		

#	Parameters	Minimum Specifications	Bidder Compliance	Product Documentation Reference
		match, exact NOT match, contains match, wildcard match and regularly expression match (such as forced door alarm, denied access, door open too long, etc.) • Should have an ability to optionally match alarming subsystem's incident status, incident severity, and sensor type • Should have an ability to apply any alarm policy to one or more monitoring area(s) or zone(s) without having to reapplying the policy multiple times. • Should have an ability to apply any alarm policy to one or more sensors without having to reapply the policy multiple times. • Should have an ability to assign specific actions for each alarm • Should have an ability to activate or deactivate alarms as required • Should have an ability to create exceptions • Should Create batch-wise rules and process them • Should Check and rectify logical errors and contradictory rules • Should have an ability to schedule execution of rules • Should Suspend or Terminate the application of rule • Should archive unused or deactivated rules		

#	Parameters	Minimum Specifications	Bidder Compliance	Product Documentation Reference
94.	Security compliance	The platform hosted at the cloud shoud have following security components (but not limited to): 1. Multi-factor authenticaton 2. SIEM 3. IDAM 4. Anti Advance Persistent Threat 5. DDoS 6. Network access control Few of the above mentioned security components like SIEM, IDAM etc. should also cater to security requirements of DC applications. Apart from above mentioned components, MSI shall adhere to the latest cyber security guidelines as mentioned in Annexure VII to provide safe and secure cloud platform environment.		

6.1.2 Video Wall

The Video Wall for CCC shall be configured with 4x4 formation of the following Professional Display (DLP LED Display Cube) Screens.

#	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Technology	DLP LED Suitable for Video Wall Display		
5.	Screen Size	55”		
6.	Panel Technology	Vertical Alignment (VA)		
7.	Native Resolution	1920 x 1080 (Full HD) Pixels		
8.	Aspect Ratio	16:9		
9.	Pixel Pitch	0.53025 (H) X 0.53025		

#	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		(W)		
10.	Static Contrast Ratio (Minimum)	1800:1 or better		
11.	Dynamic Contrast Ratio (Minimum)	1000000:1 or more		
12.	Brightness	700 (or above) nit		
13.	Brightness of projection engines	Minimum 2000 lumens		
14.	Brightness uniformity	>= 98%		
15.	Viewing angle	178 degree/178 degree (H/V)		
16.	Response time	8ms		
17.	Bezel Width	3.4 mm or less		
18.	Screen to Screen Gap	<= 1 mm		
19.	Input	HDMI,VGA, Digital DVI, Display Port, HDBase T & other inputs as per Video Wall solution offered		
20.	Operations	365 X 7 X 24		
21.	Accessories	All Included (AC Power Cord, Remote Control, Adjustable Wall Mount Bracket, Necessary Cables And Connectors etc.)		
22.	Monitoring of critical parameters to ensure stable operation of the system 24 x 7	Internal temperature, Ambient temperature, humidity, Brightness, Cooling, Light source status		
23.	Cube control & monitoring	Videowall should be equipped with a cube control & monitoring system, Should be able to control & monitor individual cube , multiple cubes and multiple video walls, Provide videowall status including Source , light source ,temperature, fan and power		

#	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		information, Should provide a virtual remote on the screen to control the videowall, System should have a quick monitor area to access critical functions of the videowall		
24.	Dust prevention	Should meet or exceed IP6X standard. Certificate to this effect to be furnished from 3rd party Laboratory		
25.	Control	IP based control to be provided		
26.	Remote	IR remote control should also be provided for quick access		

6.1.3 Video Wall Controller

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Controller	Controller to control Video wall in a matrix form as per requirement		
5.	Chassis	19" Rack mount		
6.	Processor	Latest Generation 64 bit x86 Quad Core processor (3.4 Ghz) or better		
7.	Operating System	Pre-loaded latest 64-bit Operating System Windows / Linux / Equivalent, with recovery disc		
8.	RAM	16 GB DDR3 RAM or higher		
9.	HDD	500 GB or higher Solid State Disk		
10.	Networking	Dual-port Gigabit Ethernet Controller with RJ-45 ports		
11.	RAID	Should support all RAID levels		
12.	Power Supply	(1+1) Redundant hot swappable		
13.	Input/ Output support	DVI/HDMI/USB/ LAN/ VGA/SATA port		
14.	Accessories	104 key Keyboard and Optical USB mouse		
15.	USB Ports	Minimum 4 USB Ports		
16.	Redundancy support	Power Supply, HDD, LAN port & Controller		
17.	Scalability	Display multiple source windows in any size, anywhere on the wall		
18.	Control functions	Brightness/		
19.	Inputs	To connect to minimum 2 sources through HDMI		
20.	Output	To connect Displays through HDMI/DVI as per requirements		
21.	Operating Temperature	10°C to 35°C, 80 % humidity		
22.	Cable & Connections	Successful bidder should provide all the necessary cables		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		and connectors, so as to connect Controller with LED Display units		

6.1.4 Video Wall Management Software

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Display & Scaling	Display multiple sources anywhere on display up to any size		
5.	Input Management	All input sources can be displayed on the video wall in freely resizable and movable windows		
6.	Scenarios management	Save and Load desktop layouts from Local or remote machines		
7.	Layout Management	Support all Layout from Input Sources, Internet Explorer, Desktop and Remote Desktop Application		
8.	Multi View Option	Multiple view of portions or regions of Desktop, Multiple Application Can view from single desktop		
9.	Other features	SMTP support Remote Control over LAN Alarm management Remote management Multiple concurrent client KVM support		
10.	Cube Management	Cube Health Monitoring Pop-Up Alert Service Graphical User Interface		
11.	General requirement	The wall management software shall be having interoperability with Video management system The wall management software		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		may be centrally Server based or local controller based architecture		
12.	General Requirement	Key features of Wall management Software a. Central configuration database The Wall Control software shall perform health monitoring that allows timely detection of faults. a. Wall health b. Cube health c. Cube IP-address Brightness		

6.1.5 Audio Mixer & Speaker system

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Audio Mixer	Input Power 6W RMS		
5.	Frequency Response (-3dB)	80Hz - 20kHz		
6.	Frequency Range (-10dB)	74Hz - 54kHz		
7.	System Sensitivity (1W @1m)	89dB (1W = 4V for 16 Ohms)		
8.	Nominal Impedance	16 Ohms		
9.	Speaker Mounting	Ceiling Speaker		
10.	SNR	>= 70 dB		
11.	Speaker Outout	100 V AB 6 Zone Speaker Output		
12.	Rated Power Outout	240W		
13.	Fireman Microphone	500 Mv, 600Ω		
14.	Line 1-2 inputs	385mV, 10kΩ balanced Combo		
15.	Line 3-6 inputs	350mV, 10kΩ, RCA		
16.	Operation Environment	Operation Temp: +5 °C ~ +40 °C		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		Store Temp:-20 °C ~ +70 °C Operation Humidity: <95%		
17.	Power Consumption	600		

6.1.6 Network Colour Multi-Function Laser Printer

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Print Speed	Black : 16 ppm or above on A3, 24 ppm or above on A4 Color : 8 ppm or above on A3, 12 ppm or above on A4		
5.	Copy Speed	12 ppm or better		
6.	Scanner	Flatbed type with ADF		
7.	Resolution	600 X 1200 DPI		
8.	Memory	1 GB or more		
9.	Paper Size	A3, A4, Legal, Letter, Executive, custom sizes		
10.	Paper Capacity	250 sheets or above on standard input tray, 100 Sheet or above on Output Tray		
11.	Duty Cycle	25,000 sheets or better per month		
12.	OS Support	Latest version of Linux, Windows 10, 7, 8, 8.1		
13.	Interface	Fast Ethernet (100Base-T),Hi-Speed USB 2.0 , Wi-Fi		
14.	General	Full toner Cartridge shall be supplied with the printer		

6.1.7 Work Station for City Management Room with Joy Stick and Dual Monitor

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Processor	Latest Quad Core i7 with 3 GHz or higher		
5.	Chipset	Compatible 64 bit Chipset		
6.	Motherboard	OEM Motherboard		
7.	RAM	Minimum 8 GB DDR3 or higher expandable up to 32 GB or more		
8.	Graphics card	Minimum Graphics card with 2 GB video memory (non-shared)		
9.	HDD	2 TB SATA-3 Hard drive @7200 rpm with Flash Cache of 64GB SSD. Provision for installing 4 more drives.		
10.	Media Drive	NO CD / DVD Drive		
11.	Network interface	10/100/1000 Mbps autosensing on board integrated RJ-45 Ethernet port.		
12.	Audio	Line/Mic IN, Line-out/Spr Out (3.5 mm)		
13.	Ports	1 HDMI port (Preferable), 2x USB 2.0 and 2 x USB 3.0 (Preferable), 10 USB ports external - with minimum 4 ports USB 3.0 Front I /O includes (2 or more) USB 2.0 ports Rear I / O includes (2 or more) USB 3.0 ports, (2 or more) USB 2.0 ports, serial port, Parallel port, PS 2 mouse and keyboard ports, RJ-45 network interface, Display Port 1 VGA and		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		3.5mm audio in /out jacks; 4 in 1 Media Card Reader (Preferable)		
14.	Keyboard	107 or more English + Punjabi and Rupee symbol Keys keyboard		
15.	Mouse	2 Or 3 button USB Optical Scroll Mouse with antistatic mouse pad resolution of Optical 1000 CPI, Complying to CE and FCC norms		
16.	PTZ joystick controller (with 2 of the workstations in SCOC)	• PTZ speed dome control for IP cameras • Minimum 10 programmable buttons • Multi-camera operations • Compatible with all the camera models offered in the solution Compatible with VMS /Monitoring software offered		
17.	Monitor	Two monitors of 22" TFT LED monitor, Minimum 1920 x1080 resolution, 5 ms or better response time		
18.	Certification	Energy star /BEE certified/EPEAT		
19.	Operating System	Pre-Loaded Windows 10 with recovery disc, Linux etc.		
20.	Security	BIOS controlled electro-mechanical internal chassis lock for the system.		
21.	Power Input	100 -240V AC		

6.1.8 Manager workstation with touch screen monitor

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Processor	Latest Quad Core i7 with 3		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		GHz or higher		
5.	Chipset	Compatible 64 bit Chipset		
6.	Motherboard	OEM Motherboard		
7.	RAM	Minimum 8 GB DDR3 or higher expandable up to 32 GB or more		
8.	Graphics card	Minimum Graphics card with 2 GB video memory (non-shared)		
9.	HDD	2 TB SATA-3 Hard drive @7200 rpm with Flash Cache of 64GB SSD. Provision for installing 4 more drives.		
10.	Media Drive	NO CD / DVD Drive		
11.	Network interface	10/100/1000 Mbps autosensing on board integrated RJ-45 Ethernet port.		
12.	Audio	Line/Mic IN, Line-out/Spr Out (3.5 mm)		
13.	Ports	1 HDMI port (Preferable), 2x USB 2.0 and 2 x USB 3.0 (Preferable), 10 USB ports external - with minimum 4 ports USB 3.0 Front I /O includes (2 or more) USB 2.0 ports Rear I / O includes (2 or more) USB 3.0 ports, (2 or more) USB 2.0 ports, serial port, Parallel port, PS 2 mouse and keyboard ports, RJ-45 network interface, Display Port 1 VGA and 3.5mm audio in /out jacks; 4 in 1 Media Card Reader (Preferable)		
14.	Keyboard	107 or more English + Punjabi and Rupee symbol Keys keyboard		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
15.	Mouse	2 Or 3 button USB Optical Scroll Mouse with antistatic mouse pad resolution of Optical 1000 CPI, Complying to CE and FCC norms		
16.	Monitor	Touchscreen monitor with 27 Inches screen , Wide LED, Resolution- 1920x1080, Aspect Ratio-16:9 , refresh rate 5ms or better		
17.	Certification	Energy star /BEE certified/EPEAT		
18.	Operating System	Pre-Loaded Windows 10 with recovery disc, Linux etc.		
19.	Security	BIOS controlled electro-mechanical internal chassis lock for the system.		
20.	Power Input	100 -240V AC		

6.1.9 Help Desk Team/ Contact Centre/ War Room/ Security/ Technical Support Team Work Stations

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Processor	Latest Quad Core i7 with 3 GHz or higher		
5.	Chipset	Compatible 64 bit Chipset		
6.	Motherboard	OEM Motherboard		
7.	RAM	Minimum 8 GB DDR3 or higher expandable up to 32 GB or more		
8.	Graphics card	Minimum Graphics card with 2 GB video memory (non-shared)		
9.	HDD	2 TB SATA-3 Hard drive @7200 rpm with Flash Cache of 64GB SSD. Provision for installing 4 more drives.		
10.	Media Drive	NO CD / DVD Drive		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
11.	Network interface	10/100/1000 Mbps autosensing on board integrated RJ-45 Ethernet port.		
12.	Audio	Line/Mic IN, Line-out/Spr Out (3.5 mm)		
13.	Ports	1 HDMI port (Preferable), 2x USB 2.0 and 2 x USB 3.0 (Preferable), 10 USB ports external - with minimum 4 ports USB 3.0 Front I /O includes (2 or more) USB 2.0 ports Rear I / O includes (2 or more) USB 3.0 ports, (2 or more) USB 2.0 ports, serial port, Parallel port, PS 2 mouse and keyboard ports, RJ-45 network interface, Display Port 1 VGA and 3.5mm audio in /out jacks; 4 in 1 Media Card Reader (Preferable)		
14.	Keyboard	107 or more English + Punjabi and Rupee symbol Keys keyboard		
15.	Mouse	2 Or 3 button USB Optical Scroll Mouse with antistatic mouse pad resolution of Optical 1000 CPI, Complying to CE and FCC norms		
16.	Monitor	22" TFT LED monitor, Minimum 1920 x1080 resolution, 5 ms or better response time		
17.	Certification	Energy star /BEE certified/ EPEAT		
18.	Operating System	Pre-Loaded Windows 10 with recovery disc, Linux etc.		
19.	Security	BIOS controlled electro-mechanical internal chassis lock for the system.		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
20.	Power Input	100 -240V AC		

6.1.10 IP Phone

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Display	2 line or more, Monochrome display for viewing features like messages, directory		
5.	Integral switch	10/100 mbps for a direct connection to a 10/100BASE-T Ethernet network through an RJ-45 interface		
6.	Speaker Phone	Yes		
7.	Headset	Wired, Cushion Padded Dual Ear-Speaker, Noise Cancelling headset with mouthpiece microphone, port compatibility with IP Phone		
8.	VoIP Protocol	SIP V2		
9.	POE	IEEE 802.3af or better		
10.	Supported Protocols	SNMP, DHCP, DNS		
11.	Codecs	G.711, G.722 including handset and speakerphone		
12.	Speaker Phone	Full duplex speaker phone with echo cancellation Speaker on/off button, microphone mute		
13.	Volume control	Easy decibel level adjustment for speaker phone, handset and ringer		
14.	Phonebook/Address book	Minimum 100 contacts		
15.	Call Logs	Access to missed, received, and placed calls. (Minimum 20 overall)		
16.	Clock	Time and Date on display		
17.	Ringer	Selectable Ringer tone		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
18.	Directory Access	LDAP standard directory		
19.	QoS	QoS mechanism through 802.1 p/q		

6.1.11 Digital Set Top Box

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	Equipment must confirm to standards and specifications laid down by Government of India.			

6.1.12 Television set for Meeting Room

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
4.	**Make**		<to be provided by the bidder>	
5.	**Model**		<to be provided by the bidder>	
6.	**Key Features:**			
7.	Technology	LED Backlit Full HD TV		
8.	Screen Size	55" or higher		
9.	Native Resolution	Full HD(1920 x 1080 progressive signal)		
10.	Aspect Ratio	16:9		
11.	Static Contrast Ratio (Minimum)	4500:1 or better		
12.	Dynamic Contrast Ratio (Minimum)	Up to 50000		
13.	Brightness	350 nit or better		
14.	Response time	8ms		
15.	Input	2 HDMI , 1 DVI and USB		
16.	Output Port	Audio		

6.1.13 Technical requirement for Contact Center Application

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	For up to 50 agents			
5.	Automatic Call Distribution			
6.	Automatic identification of incoming number based on landline and mobile number mapping			
7.	Call recording mapped to incident tickets			
8.	Customizable agent and supervisor desktop layout			
9.	Inbound and outbound capability			
10.	Call control			
11.	Multisession web chat			
12.	Email			
13.	Live data reporting gadgets			
14.	Phonebook			
15.	Multiline support			
16.	Speed dial in IP phones			
17.	ACD Should be highly available with hot standby and seamless failover in case of main server failure. There should not be any downtime of Contact Center in case of single server failure.			
18.	ACD should support skill based routing and it should be possible to put all the agents in to a single skill group and different skill groups			
19.	ACD should support routing of incoming calls based upon caller input to menus, real-time queue statistics, time of day, day of week, ANI, dialled number etc.			
20.	ACD should support call routing based on longest available agent, circular agent selection algorithms.			
21.	ACD should support the playing of customizable queuing announcements based upon the skill group that the call is being queued to, including announcements related to position in queue and expected delay.			
22.	ACD should enable agents to chat with other Agents or supervisor from the Agent desktop software			
23.	ACD should enable supervisor to see the real-time status of agents, supervisors should be able to make agent ready or logout from the supervisor desktop			

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
24.	ACD should support Queuing of calls and playing different prompts depending on the type of call and time in the queue.			
25.	In future if required, the ACD should support active and standby server mode, where the server can be put in DC and DR. In case of Main server in the Data center fail the standby server in DR should take over seamlessly. ACD solution should support placing of Main and Stand by server in DC and DR respectively.			
26.	IVR should play welcome messages to callers Prompts to press and collect DTMF digits			
27.	IVR should be able to integrate with backend database for self-service, as and when required.			
28.	GUI based tool to be provided for designing the IVR and ACD call flow.			
29.	IVR should support VoiceXML for ASR, TTS, and DTMF call flows			
30.	IVR should be able to Read data from HTTP and XML Pages			
31.	IVR should be able to run outbound campaigns.			
32.	IVR should be able to record calls.			
33.	System to provide report of IVR Application Performance Analysis, Call by Call details for all the calls, Traffic analysis reports etc			
34.	Reporting platform to support Agent level reports, Agent login, logout report, report on agent state changes			
35.	Queue reports, Abandon call reports all the reports should be summary, tabular and detailed report format to be available for the agents.			
36.	Reporting platform to support custom reports using a combination of the Crystal Reports Developer's Toolkit and SQL stored procedures.			
37.	Users of the Historical Reports should be able to perform the following functions View, print, and save reports. Sort and filter reports, Send scheduled reports to a file or to a printer. Export reports in a variety of formats, including PDF, RTF, XML, and CSV.			
38.	Administrator should be able to assign one or more email addresses to a single Queue.			
39.	Email routing support integration with Microsoft Exchange 2003 or Microsoft Exchange 2007 or 2010.			

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
40.	Agents should be able to automatically resume of e-mail processing on voice disconnect.			
41.	Agent should be able to save email draft response and resume at a later time.			
42.	Agent should be able to re-queue email.			
43.	Supervisor should be able to access real-time reporting for Agent E-Mail mail volume by Queue			

6.1.14 War Room

6.1.14.1 LED display to present critical information display

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.			<to be provided by the bidder>	
3.	**Key Features:**			
4.	Technology	LED Backlit Full HD TV		
5.	Screen Size	55” or higher		
6.	Native Resolution	Full HD(1920 x 1080 progressive signal)		
7.	Aspect Ratio	16:9		
8.	Static Contrast Ratio (Minimum)	4500:1 or better		
9.	Dynamic Contrast Ratio (Minimum)	Up to 50000		
10.	Brightness	350 nit or better		
11.	Response time	8ms		
12.	Input	2 HDMI , 1 DVI and USB		
13.	Output Port	Audio		

6.1.14.2 Over Head Projector

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Display Technology	Poly-silicon TFT 3LCD		
5.	Resolution	WXGA, 1280x800, 16:10		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
6.	Colours	1.07 billion Colours		
7.	Brightness	4000 or more ANSI lumens (in Normal Mode)		
8.	Contrast Ratio	2200:1 / 10000:1 (dynamic)		
9.	Video Input	One computer (D-Sub, Standard 15 pin VGA connector) One HDMI		
10.	Keystone Correction	Horizontal and vertical		
11.	Zoom and Focus	Manual Zoom and Focus		
12.	Audio	Internal speaker		
13.	Remote Operations	Full function Infrared Remote Control		
14.	Other features	Auto source detect, Auto-synchronisation, Keystone Correction		
15.	Mounting	Ceiling mount with fixed structure, with all accessories and cables		
16.	Lamp Life	Up to 3000 hour(s) / up to 5000 hour(s) (economic mode)		
17.	Lamp Type	260 Watt		
18.	Lens aperture	F/2.4-2.66		
19.	Power	AC 230 V (50 Hz) Projection Distance: 4 ft. - 33 ft.		
20.	General	✓ 3D Capable – Yes ✓ Device Type: Projector with High Definition 720p or better display ✓ Min. Operating Temp : 2°C ✓ Max. Operating Temp: 48°C ✓ Security Lockup Slot – Yes ✓ Sound Emission : 37dB ✓ Sound Emission (Economic mode): 32dB ✓ Integrated speakers - Yes ✓ Throw Ratio : 1.28 – 1.536 :1 ✓ Video Inputs: RGB, Component Video (PAL – B/G, PAL-N, PAL-M, PAL-I, NTSE 4.43, NTSE 3.58, PAL-D, SECAM-L,		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		PAL-H, SECAM-K1, SECAM-D/K, SECAM-B/G) ✓ Video Interfaces : HDMI & VGA ✓ Video Modes: 480p, 720p, 1080p, 480i, 576i, 576p ✓ Zoom Factor – Min. 1.2x		

6.1.14.3 IP PABX System

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	**IP PABX System**	• The IP telephony system should be a converged communication System with ability to run TDM and IP on the same platform using same software load based on server and Gateway architecture • The single IP PBX system should be scalable to support up to 500 stations (any mix/percentage of Analog/IP) to achieve the future capacity • The system should be based on server gateway architecture with external server running on Linux OS. No card based processor systems should be quoted • The voice network architecture and call control functionality should be based on SIP • The call control system should be fully redundant solution with no single point of failure & should provide 1:1 redundancy. • The communication server and gateway should support IP V6 from day one so as to be future proof • The entire solution (IP PBX, its hardware, IP Phones,		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		Voice Gateway) should be from a single OEM		
5.	**Support for call-processing and call-control**	• Should support signalling standards/ Protocols – SIP, MGCP, H.323, Q.Sig • Voice Codec support - G.711, G.729, G.729ab, g.722, ILBC • The System should have GUI support web based management console		
6.	**Security**	• The protection of signaling connections over IP by means of authentication, Integrity and encryption should be carried out using TLS • System should support MLPP feature • Proposed system should support SRTP for media encryption and signaling encryption by TLS • Secure HTTP support for Call Server Administration, Serviceability, User Pages, and Call Detail Record Analysis and Reporting Tool. Should support Secure Sockets Layer (SSL) for directory • The administrator logging on to the call control server needs to authenticate by suitable mechanism such as User Login Information and Passwords/ Radius Server • Voice gateway to be provided with 1 PRI card scalable to 3 PRI in future for PSTN (PRI) line termination.		

6.1.14.4 PRI Modem Pair

S. No.	Module	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**			<to be provided by the bidder>	
2.	**Model**			<to be provided by the bidder>	
3.	**Key Features:**				
4.	Power Device	Voltage	AC 110/220 V		

S. No.	Module	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		Required			
5.		Voltage Required Margin	± 10%		
6.		Frequency Required	50/60 Hz		
7.		Power Consumption Operational	200 Watt		
8.		Type	Internal power supply		
9.	Modem	Type	ISDN terminal adapter		
10.		Enclosure Type	integrated		
11.		Max Transfer Rate	1.5 Mbps		
12.		Digital Ports Qty	30		
13.		Digital Signaling Protocol	ISDN PRI		
14.	Networking	Type	remote access server		
15.		Connectivity Technology	wired		
16.		Data Link Protocol	EtherTalk, Ethernet, HDLC, ISDN		
17.		Network / Transport Protocol	AppleTalk, IPX/SPX, TCP/IP		
18.		Features	CHAP authentication, PAP authentication, firewall protection		
19.		Compliant Standards	IEEE 802.3		
20.		Switching Protocol	Ethernet, Frame Relay, PPP		
21.		Remote Management Protocol	SNMP		

S. No.	Module	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
22.		Line Rate	E-1		
23.		Framing Format	D4, G.703		
24.	Communication	Digital Signaling Protocol	ISDN PRI		
25.		Protocols & Specifications	V.110 (I.470), V.120 (I.464)		
26.		Digital Ports Qty	30		
27.		Digital Ports Qty	30		
28.	Interface	Gender	female		
29.		Connector Qty	1, 30		
30.		Type	modem, serial		
31.		Interface	ISDN PRI E1, V.35		
32.		Qty	1, 30		
33.		Connector Type	44 pin D-Sub (DB-44), RJ-48		
34.	Environmental Parameters	Min Operating Temperature	32 °F		
35.		Max Operating Temperature	104 °F		
36.		Humidity Range Operating	5 - 90%		

6.1.14.5 SMS Gateway

S. No.	Module	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**			<to be provided by the bidder>	
2.	**Model**			<to be provided by the bidder>	
3.	Bidder has to provide SMS Gateway of Telecom Service Provider which has ability to withstand for continued growth in A2P SMS and SVI SMSG.				
4.	The SMS Gateway PULL SMS application must have security features to ensure confidentiality of sensitive customer data.				
5.	The SMS Gateway PULL SMS application should be able to retrieve SMSs sent to one or more short codes / virtual numbers.				

S. No.	Module	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
6.	The SMS Gateway PUSH SMS application should be able to send messages at different priority levels.				
7.	The SMS Gateway PUSH SMS application must have ability to set working hours and days.				
8.	The solution should offer configurable mechanism in terms of number of retries and time duration for each retry for messages that could not be sent / delivered immediately.				
9.	Online mechanism in real time mode has to be provided for SLA enforcement with regard uptime of Push / Pull services & deliveries along with the flexibility to generate MIS on daily / weekly / fortnightly / monthly / between specified data range.				
10.	Check should be properly imposed to avoid duplicate or multiple SMS delivery to stakeholders.				

6.1.15 Furniture

6.1.15.1 Operator Console Table & Ergonomic Chair

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Physical Structure	Ergonomically designed desk to ensure 24x7 desking solution with sufficient knee space (min 450mm) and foot space (min 600 mm) and minimum width of 1800 mm.		
5.	Working Surface material	The Console Top / working surface should be made of minimum 25 mm thick MDF with High Pressure Laminate finish. The laminate shall be fire retardant, Insulated, Water Proof, Scratch resistant and high hardness. The Table		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		Top should be able to mount three 27 Inches Display monitors for each work station with front edge of the table top should be moulded polyurethane edge(for wrist cushion)		
6.	Console Design	Consoles must be of modular design, facilitating future equipment retrofits and full reconfigurations without requiring any major modification to the structure or exterior elements		
7.	Equipment Mounting	The workstation shall be able to house computer equipment's, Ethernet Points, Power Distribution Unit. The CPUs shall be mounted on Slide out CPU trays (mounted on Heavy duty slides) for ease in maintenance, all of these equipment's should be concealed from direct human view		
8.	Frame material	Made of heavy duty Aluminium. The Extrusions shall be duly powder coated with 40+ micron over all surfaces.		
9.	Monitor Arms and Rear Walls	Die cast mounted Aluminium articulated arm; fixed firmly on MS Pole with powder coating mounted on its rear wall also made of aluminium Monitor and Functional holder shall guarantee optimum viewing distance. All ergonomic aspects shall be taken in to account. It shall be capable for		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		mounting all type of LCD/LED display with Dimensions between 17" to 27" using suitable brackets/additional base plate For configuration of working position, it shall allow the technical staff to rotate/ tilt/ raise/the monitors as well as fix their adjustment in a quick and easy manner		
10.	Warranty/Guarante e	10 years replaceable		
11.	Certifications/compl ia nt	ISO 11064 latest revision, BIFMA X5.5, RoHS (UL certificate), Seismic zone IV compliant		

6.1.15.2 Chairs

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	General	Ergonomic Chair with Arm Rest and castor wheels designed for 24/7 usage		
5.	Backrest support	Tilt adjustable, polystyrene support frame with 100% polyester fiber		
6.	Seat Support	Height adjustable, Molded wood, 10 mm. thick with polyurethane foam, density minimum 70 kg/m3		
7.	Seat Adjustment Mechanism	Self-adjustable synchronous mechanism with soft resort. Multi-locking with safe anti-return system.		
8.	Armrests	Height adjustable via button, Front/back adjustable with PU pads (50 mm)		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
9.	Column	Class 3 built-in cartridge cylinder steel tube		
10.	Base	Swivel on castor with 5 polyamide double-wheel castors (made of polyamide and fiber glass)		
11.	Colour	Black		
12.	Warranty	Minimum 5 replaceable years		

6.1.16 Building Utilities

6.1.16.1 DG Set

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Rating (KVA)	250		
5.	Rated (KWe)	40		
6.	No of Cylinders	4		
7.	Rated Speed RPM	1500		
8.	Cooling System (Air Cooled/Water Cooled)	Water		
9.	Door Type	DD		
10.	Side lifting DG set dimensions with top hood, if any (mm)	LxWxH (2770x1150x1800)		
11.	Intergrated Fuel Tank Capacity (liters)	150		
12.	Approximate Dry Weight of DG set (Kg)	1250		
13.	Centre lifting DG set dimensions with top hood, if any (mm)	LxWxH (2800x1150x1540)		
14.	BHP	84		
15.	Power Factor	0.8		
16.	Voltage	230 (1Ø) & 415 (3Ø)		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
17.	Noise Level	<75 dB		
18.	Fuel Tank Capcity	65 Ltrs. Or More		
19.	Electrical Battery starting voltage	12 V		
20.	Lube Oil Change Period	500 Hrs or more		
21.	Overload Capacity	10% for one hour in any 12 hours of continuous operations		
22.	Redundancy configuration	Should be able to be configured for redundancy from two phases		
23.	Control	Automatic Stop device if any parameters are varied beyond upper / lower limits. Integral mounting of instrument panel complete with wiring (for engine) and connections.		
24.	Fuel Tank & Piping	Fuel tank to be located within 10 meter periphery of the DG set.		
25.	Lubrication	Lube Oil		
26.	Heat Exchanger	Yes required		
27.	Enclosure	Sound proof, drip proof and Screen protected (min.as per IP 23). The alternator terminal box shall be amended and made suitable for bus duct arrangement.		
28.	Alternator	Alternator shall be self-excited, self-regulated, self-ventilated in brush less for suitable automatic voltage regulator and shall conform to BS:2613 or equivalent standard. It should give rated output at NTP condition. Alternator shall have space neater which shall be connected with		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		breaker NO/NC contacts and this should be able to cut off with thermostat. Alternator shall have RTD and BTD.		
29.	Acoustics	Acoustic treatment shall ensure a maximum sound pressure not more than 68 dB at 1 meter during the day and 45 dB at neighbor's premises during night while running on partial or full load. The condition shall apply to the engine exhaust noise levels also. A vertical type "Critical" silencer shall be fitted on the exhaust pine.		
30.	Insulation Class	Class H		
31.	Bearings	Heavy duty pre-lubricated		
32.	Ventilation	Centrifugal Fan		
33.	Space Heater	Yes to be provided		
34.	Total losses as % of rated KW	Not more than 4		

6.1.16.2 IBMS

The MSI shall supply, install and commission BAS, Access control and Physical security system for ICCC Building Office. MSI has to also provide all necessary hardware and all operating and applications software necessary to perform the control sequences of operation as called for in this specification. All components of the system –, application controllers, unitary controllers, etc. shall communicate using the BACnet protocol, as defined by ASHRAE Standard 135-2007, or EIA standard 709.1, the LonTalk™ protocol, or Modbus protocol. At a minimum, provide controls for the following:

1. Air handling units
2. Return air fans
3. Exhaust and supply fans
4. Chilled water system including pumps, chillers, and cooling towers
5. Boilers including hot water pumps
6. Computer room air handling units
7. Refrigerant leak detection system

8. Smoke evacuation sequence of AHUs and return fans including smoke control dampers and fire command override panel.
9. Finned tube radiation control
10. Variable volume and constant volume box control including interlocks with finned tube radiation.
11. Cabinet unit heater controls
12. Monitoring points for packaged equipment such as emergency generators,
13. Power wiring to DDC devices, smoke control dampers and BAS panels except as otherwise specified.

Access Control System

- The Access Controller's should be designed for both critical government & private sector security applications. Below input & output modules should be onboard with the Controllers.
    - Universal Inputs : 12
    - Reader Inputs : 8
    - Tamper Input : 1
    - Digital Lock Output : 4
- The Access Controller's should be designed to support both entry & egress readers while supplying +5 or +12 VDC to each reader.
- The controller should support the data transfer rates upto 100 Mbps and should have IPSec/IKE encryption and authentication. Encryption (up to 192-bit) and authentication may be enabled for communication to and from workstations and controllers. Controller should utilizes Internet Protocol Security (IPSec) and Internet Key Exchange (IKE) for its encryption to assure tamperproof communications over the Ethernet.
- The Controller should be perfect for large systems. A controller servicing up to 8 areas can hold 480,000 personnel records. With such a large local storage capacity, access decisions can be made swiftly without waiting for validation by a remote server.
- Controller should have inbuilt 32 MB of flash memory and 128 MB of DDR SDRAM. The flash memory is used to preserve 12 MB of application and run-time data. The dynamic RAM is partitioned for dedicated functions: a full 12 MB for applications, 48 MB for personnel records and 8 MB for the operating system. The unused memory should be available for future enhancements. Personnel record data should be preserved using onboard batteries that can hold the data for at least 7 days without the use of an external UPS. If the controller has its application stored in flash and power loss lasts longer than what the battery can supply for RAM, the controller will send a message to Cyber Station and request that the personnel records automatically be reloaded when the power returns.
- The reader inputs should be powered by a dedicated processor allowing the controllers to support current and future devices for advanced applications. The hardware should be ready to support 260-bit encrypted data messages from the reader.

- It is important for controller to be able to contain potential threats when they are detected. The Controller should respond to Area Lockdown commands set from Access control software providing a quick method of sealing off areas. A simple click of a graphic or an automatic program response is all that is needed to disable card readers and exit requests in any given area. First responder personnel can still gain access to the area if their record is marked with "executive privilege".
- The Controller should be able to adapt access rights to a change in condition or "threat" levels. Each personnel record should be assigned a clearance level for each area to which they have access. When the condition is more severe than the person's clearance level then access is automatically denied. The Condition Level may be set manually through workstation or automatically through a program. A program can even be used to monitor national threat levels and adjust Condition Levels accordingly.
- Each controller should support the use of two expansion modules plus an Display unit. The expansion module is used for expanding the controller for special or access to doors. Modules can also be used to provide a cost effective entry reader only solution.
- The Access controller should support up to 32 Infinet nodes. The RS-485 programmable port can be set to support a wired or wireless Infinet field bus.
- The Controllers should be ready to support a wide range of card formats. Ideal for retrofits, The Controller lets you preserve existing cards by accepting standard formats (Weigand, ABA, HID Corporate-1000, CardKey) as well as custom formats (Custom Weigand, Custom ABA). The Controller should support formats up to 260-bits making the controllers ready for government installations that must meet HSPD-12 and FIPS 201 standards.
- SNMP (Simple Network Messaging Protocol) messages may be sent to network monitoring software to inform IT managers as to the health and presence of the access controller on the corporate network. The Access Controller should also support the SNMP alarming option.

6.1.16.3 Fire & Smoke Detection System

Fire can have disastrous consequences and affect operations of a Control Room. It is required that there is early-detection of fire for effective functioning of the Control Room.

A. System Description

The Fire alarm system shall be an automatic 1 ton (e.g. 8) zone single loop addressable fire detection and alarm system, utilizing conventional detection and alarm sounders.

Detection shall be by means of automatic heat and smoke detectors located throughout the Control Room (ceiling, false floor and other appropriate areas where fire can take place) with break glass units on escape routes and exits.

B. Control and Indicating Component

- The control panel shall be a microprocessor based single loop addressable unit, designed and manufactured to the requirements of EN54 Part 2 for the control and indicating component and EN54 Part 4 for the internal power supply.
- All controls of the system shall be via the control panel only.
- The system status shall be made available via panel mounted LEDs and a backlit 8 line x 40-character alphanumeric liquid crystal display.
- All system controls and programming will be accessed via an alphanumeric keypad. The control panel will incorporate form fill menu driven fields for data entry and retrieval.
- The system will include a detection verification feature. The user shall have the option to action a time response to a fire condition. This time shall be programmable up to 10 minutes to allow for investigation of the fire condition before activating alarm outputs. The operation of a manual call point shall override any verify command.

C. Manual Controls

- Start sounders
- Silence sounders
- Reset system
- Cancel fault buzzer
- Display test
- Delay sounder operation
- Verify fire condition
- Disable loop

D. Smoke detectors

Smoke detectors shall be of the optical or ionisation type. Devices shall be compatible with the CIE conforming to the requirements of EN54 Part 7 and be LPCB approved. The detectors shall have twin LEDs to indicate the device has operated and shall fit a common addressable base.

E. Heat detectors

- Heat detectors shall be of the fixed temperature (58° C) or rate of temperature rise type with a fixed temperature operating point.
- Devices shall be compatible with the CIE conforming to the requirements of EN54 Part 5 and be LPCB approved
- The detectors shall have a single LED to indicate the device has operated and shall fit a common addressable base.

F. Addressable detector bases

- All bases shall be compatible with the type of detector heads fitted and the control system component used. Each base shall comprise all necessary electronics including a short circuit isolator.
- The device shall be automatically addressed by the CIE on power up of the loop without the need of the insertion of a pre-programmed EPROM or setting of DIL switches.
- Detector bases shall fit onto an industry standard conduit box.

G. Audible Alarms

Electronic sounders shall be coloured red with adjustable sound outputs and at least 3 sound signals. The sounders should be suitable for operation with a 24V DC supply providing a sound output of at least 100dBA at 1 meter and 75 dBA min, for a bed head or sounder base type device. The sounder frequency shall be in the range of 500Hz to 1000Hz.

H. Commissioning

The fire detection and alarm system will be programmable and configurable via an alpha numeric keypad on the control panel.

I. High Sensitivity Smoke Detection System

General – The HSSD system shall provide an early warning of fire in its incipient stage, analyse the risk and provide alarm and actions appropriate to the risk. The system shall include, but not be limited to, a Display Control Panel, Detector Assembly and the properly designed sampling pipe network. The system component shall be supplied by the manufacturer or by its authorized distributor.

J. Regulatory Requirements

- National Electrical Code (NEC)
- Factory Mutual
- Local Authority having Jurisdiction

6.1.16.4 Precision Air Conditioner

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Capacity	2 Ton		
5.	Type	Precision		
6.	Star Rating	5 star		
7.	Energy Saving	Yes		
8.	Temperature	Yes		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
	Control			
9.	Cooling Capacity	above 5000 W		
10.	Compressor Type	Rotary/ Scroll		
11.	Compressor Warrantee	5 Years		
12.	Air Circulation CFM (H/M/L)	above 500/450/300		
13.	Moisture Removal L/Hr	above 1.8		
14.	IDU Noise Level(DBA)	<=55/50/45		
15.	Control	Microprocessor controlled cordless remote		
16.	Power Source (V/Hz/ Φ)	230/50/1		
17.	Display	LED/LCD		
18.	Remote Control Distance	min. 10 meter		
19.	Input Voltage	130-300 V		
20.	Output Voltage	240 +/- 5 percent		
21.	High Voltage Cutoff	240V		
22.	Efficiency	>95 percentage		
23.	Frequency	50 Hz		
24.	Operations Design	24 x 7		
25.	Air Discharge	Through EC Plug Fan		
26.	Blower	Dual Blower for flexibility of operations and better redundancy		
27.	Coolant	R410A / R407C Refrigerant		
28.	Thermostat	Safety thermostat with manual reset feature must be provided		
29.	Humidifier	Electrode Type / Infrared		

6.1.16.5 Air Conditioner for City Management Room (17 TR)

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Product Type	Ceiling Concealed Duct		
5.	Indoor Unit Noise Level (H/M/L)	67 / -- / -- dB(A)		
6.	Operation Range	Up to 53°C		
7.	Energy saving (zero power consumption, standby mode)	Yes		
8.	Refrigerant Type	R22		
9.	E.S.P (External Static Pressure) Control	Yes		
10.	Two Thermistors Control	Yes		
11.	Cooling Capacity in TR	17		
12.	Air Flow Rate (H/M/L) (CFM) - Indoor Unit	6900		
13.	External Static Pressure	12 mmAq		
	Outdoor Unit			
14.	Compressor Type	Scroll		
15.	Sound Level (H)	71 dB(A)		
16.	Piping Connections (Liquid)	Ø 15.88 mm		
17.	Piping Connections (Gas)	Ø 34.93 mm		
18.	Drain(Outdoor/Indoor)	Ø 25.4 / 22.6 mm		
19.	Max. Piping Length (Main Piping)	30M		

6.1.16.6 Comfort Air Conditioner

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Capacity	2 TON		
5.	Energy Efficiency	5 Star		
6.	Energy Efficiency (EER (Cooling, W/W))	3.51		
7.	Noise Level (Indoor, High/Low, dBA)	45/28		
8.	Noise Level (Outdoor,High/Low dBA)	54		
9.	Power Source(Φ/V/Hz)	1/230/50		
10.	Power Consumption(Cooling, W)	Avg. 2000		
11.	Operating Current(Cooling, A)	8		
12.	Piping Length (Max, m)	30		
13.	Piping Height (Max, m)	15		
14.	SVC Valve (Liquid (ODxL))	6.35		
15.	SVC Valve (Gas (ODxL))	15.88		
16.	Moisture Removal (l/hr)	2.5		
17.	Air Circulation (Cooling, m^3/min)	21		
18.	Refrigerant (Type)	R410A		
19.	Low Ambient (Cooling, ℃)	16 ~ 52		
20.	Outdoor Unit (Compressor Type)	BLDC		
21.	Outdoor Unit (Anti-Corrosion Fin)	Yes		
22.	Outdoor Unit (Multi-Channel Condensor)	Yes		
23.	Air Direction Control (Up/Down)	Auto		

6.1.16.7 UPS for CCC with 30 Minutes Backup

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Capacity	Adequate capacity to cover all above IT Components at respective location (20 KVA or more)		
5.	Output Wave Form	Pure Sine wave		
6.	Input Power Factor at Full Load	>0.90		
7.	Input	Three Phase 3 Wire for over 5 KVA		
8.	Input Voltage Range	305-475VAC at Full Load		
9.	Input Frequency	50Hz +/- 3 Hz		
10.	Output Voltage	400V AC, Three Phase for over 20 KVA UPS		
11.	Output Frequency	50Hz+/- 0.5% (Free running); +/- 3% (Sync. Mode)		
12.	Inverter efficiency	>90%		
13.	Over All AC-AC Efficiency	>85%		
14.	Crest factor	Min. 3:1 at full load		
15.	Noise level	< 55 db @ 1 Meter		
16.	UPS shutdown	UPS should shutdown with an alarm and indication on following conditions 1)Output over voltage 2)Output under voltage 3)Battery low 4)Inverter overload 5)Over temperature 6)Output short		
17.	Battery Backup	60 minutes in full		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		load		
18.	Battery	VRLA (Valve Regulated Lead Acid)		
19.	Indicators & Metering	Indicators for AC Mains, Load on Battery, Fault, Load Level, Battery Low Warning, Inverter On, UPS on Bypass, Overload, etc. Metering for Input Voltage, Output Voltage and frequency, battery voltage, output current etc.		
20.	Audio Alarm	Battery low, Mains Failure, Over temperature, Inverter overload, Fault etc.		
21.	Cabinet	Rack / Tower type		
22.	Operating Temp	0 to 65 degrees centigrade		
23.	Management Protocol	SNMP Support through TCP/IP		
24.	Protection	To be provided for overload/ short circuit; overheating; input over/ under voltage; output over/ under voltage.		
25.	Certification	ISO 9001:2008 & ISO 14001 certified		
26.	Compatibility	UPS to be compatible with DG Set supply and mains supply		
27.	Safety Certificate	IEC 62040-1		

6.1.16.8 Lighting

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Overhead Lighting	All overhead lighting shall be LEDs both recessed direct and indirect lighting including pot-lights.		
5.	Aesthetics	The overhead lighting treatment shall be incorporated into the other ceiling elements to create an aesthetic specialty ceiling design in combination with the rooms.		
6.	Lighting Intensity	Overhead lighting intensity shall be ✓ Command & Control Centre – at least 400 lux ✓ City Operations Center – at least 400 lux ✓ War Room – at least 500 lux ✓ Server Farm Area – at least 500 lux ✓ UPS Room – at least 5090 lux ✓ IBMS Room / Enclosure –		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		at least 5900 lux NOC Room – at least 500 lux		
7.	Dimming Control	✓ Dimming Control shall be continuous (all lights dimmable) and zone based (with minimum of 4 lighting zones on separate circuits. ✓ Dimming Control shall have various configurations preset for ideal operations lighting environment, based upon the perimeter glass wall natural lighting conditions (e.g. sunny, cloudy, partly cloudy night, etc.)		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		Dimmers shall not be ganged in one box.		
8.	Switching	✓ Manual switches shall be used for on / off lighting control and for overriding any preset lighting configurations • Cover plates for switches shall match the colour of the switches, receptacles and receptacle cover plates.		
9.	Quality	✓ All lighting fixtures shall be of high-grade quality over and above the standard level of quality for		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		office lighting. • Lighting shall be configured in order to reduce glares and reflection on console monitors and on the video wall, as well as accommodate any other lighting needs the monitors and video wall may have.		
10.	Arrangement	• Lighting arrangement shall accommodate console locations		

6.1.16.9 CAT 6 Cable

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
11.	**Make**		<to be provided by the bidder>	
12.	**Model**		<to be provided by the bidder>	
13.	**Key Features:**			
14.	Environmental Space	Plenum		
15.	Suitable Applications	Networking Horizontal Cable, 1000Base-T (Gigabit Ethernet), 100Base-T (Fast Ethernet), 10Base-T (Ethernet), 100BaseVG, ANYLAN, 155ATM, 622ATM, ANSI.X3.263 FDDI TP-PMD, NTSC / PAL Component or Composite Video, AEX / EBU, Digital Video, RS-422, Noisy Environments, 250 MHz Category 6		
16.	AWG Size	23		
17.	Material	FEP – Fluorinated Ethylene Propylene		
18.	Outer Shield Material	Aluminium Foil Polyester		
19.	Drain Wire Material	TC – Tinned Copper		
20.	Outer Jacket Material	LS PVC – Low Smoke Polyvinyl Chloride		
21.	Cabling	Patented Central X-spline		
22.	Conductor DCR	9.38 Ohm/100m		
23.	Capacitance	160 pF/100m		
24.	Installation Temp. Range	0°C to +50°C		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
25.	UL Temp. Rating	75°C		
26.	Storage Temp. Range	-20°C to +75°C		
27.	Operating Temp. Range	-20°C to +75°C		
28.	Bulk Cable Weight	44 lbs./1000 ft.		
29.	Max. Recommended Pulling Tension	25 lbs.		
30.	Min. Bend Radius / Minor Axis	1.0 Inch		
31.	Min. Bend radius Installation	2.25 Inch		
32.	ANSI Compliance	S-116-732-2013 Category 6, ANSI/NEMA WC-66 Category 6		
33.	Telecommunication Standards	ANSI/TIA-568-C.2 Category 6		
34.	IEEE Specifications	POE per 802.3af & POE+ per 802.3at-2009		

6.1.17 City Management Center - Surveillance System

6.1.17.1 Fixed Dome Camera for Indoor Surveillance

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Video Compression	H.265		
5.	Video Resolution	1920 X 1080		
6.	Frame rate	50 FPS at all resolutions with Controllable Bit Rate/ Bandwidth and Frame Rate		
7.	Operating	50 Hz		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
	frequency			
8.	Image Sensor	1/3" Progressive Scan CCD / CMOS		
9.	Lens Type	Varifocal, C/CS Mount, IR Correction Full HD lens compatible to camera imager		
10.	Lens	5-50mm IR corrected, CS-mount lens, P-Iris		
11.	Electronic Shutter	1/28000 s to 2 s or better		
12.	Multiple Streams	The camera shall be able to setup and stream out minimum three (3) stream profiles. Each stream profile can have its own compression resolution, frame rate and quality independently up to Full HD @ 30 FPS		
13.	Minimum Illumination	Colour: 0.2 Lux @ 30 IRE B/W: 0.01 @ 30 IRE 0 Lux with Built in or External IR, IR Range 50 m		
14.	IR Cut Filter	Automatically Removable IR-cut filter		
15.	Day/Night Mode	Yes with IR Cut Filter		
16.	S/N Ratio	≥ 50 dB		
17.	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, Auto back focus		
18.	Wide Dynamic Range	True WDR 120 db or better		
19.	Privacy Masks	Minimum 20 configurable 3D zones		
20.	Audio	Full duplex, line in and line out, G.711, G.726		
21.	Local storage	microSDXC up to 64GB (Class 10) In the event of failure of connectivity to		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		the central server the camera shall record video locally on the SD card automatically. After the connectivity is restored these recordings shall be automatically merged with the server recording such that no manual intervention is required to transfer the SD card based recordings to server.		
22.	Edge Storage	SD Card Slot with minimum 64GB Support Class 10 speed		
23.	Protocol	HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, ONVIF Profile S & preferably G		
24.	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption, IEEE 802.1Xa network access control, Digest authentication, User access log		
25.	Intelligent Video	Motion Detection & Tampering alert		
26.	Alarm I/O	Minimum 1 Input & Output contact for 3rd part interface		
27.	Operating conditions	-10 degree C to 65 degree C		
28.	Interface	RJ 45, 100 Base TX		
29.	Humidity	Humidity 10–95% RH (condensing)		
30.	Casing	NEMA 4X / IP-66 rated & IK 09		
31.	Certification	UL2802 / EN, CE ,FCC, IEC		
32.	Power	802.3af PoE (Class 0) and 12VDC/24AC/ / POE+ IEEE 902.3at Compliant		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
33.	Physical security	Detection of camera tampering and Detection of Motion should be possible using either camera or VMS		
34.	Support	The system should not be an end of life / end of service product.		
35.	White Balance	Auto / Manual		
36.	Back Light Compensation	Auto		
37.	Functional	Self-cleaning / anti-dust / hydro-phobic coating features		
38.	Mounting Accessories	For pole and surface mou nt with L/C Brackets		
39.	IR Illuminator	External / build-in IR Illuminator with minimum 50 mtr.		

6.2 Data Center – Technical Specifications & Functional Specifications

6.2.1 Network Racks/ Server Racks

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Type	• 19" 42U racks mounted on the floor • Floor Standing Server Rack - 42U with Heavy Duty Extruded Aluminium Frame for rigidity. Top cover with FHU provision. Top & Bottom cover with cable entry gland plates. Heavy Duty Top and Bottom frame of MS. Two pairs of 19" mounting angles with 'U' marking. Depth support channels - 3 pairs with an overall weight carrying Capacity of 500Kgs. • All racks should have mounting hardware 2 Packs, Blanking Panel. • Stationery Shelf (2 sets per Rack) • All racks must be lockable on all sides with unique key for each rack Racks should have Rear Cable Management channels, Roof and base cable access		
5.	Wire managers	Two vertical and four horizontal		
6.	Power Distribution	• 2 per rack		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
	Units	Power Distribution Unit - Vertically Mounted, 32AMPs with 25 Power Outputs. (20 Power outs of IEC 320 C13 Sockets & 5 Power outs of 5/15 Amp Sockets), Electronically controlled circuits for Surge & Spike protection, LED readout for the total current being drawn from the channel, 32AMPS MCB, 5 KV AC isolated input to Ground & Output to Ground		
7.	Doors	• The racks must have steel (solid / grill / mesh) front / rear doors and side panels. Racks should NOT have glass doors / panels. • Front and Back doors should be perforated with at least 63% or higher perforations. Both the front and rear doors should be designed with quick release hinges allowing for quick and easy detachment without the use of tools.		
8.	Fans and Fan Tray	• Fan 90CFM 230V AC, 4" dia (4 Nos. per Rack) Fan Housing Unit 4 Fan Position (Top Mounted) (1 no. per Rack) - Monitored - Thermostat based - The Fans should switch on based on the Temperature within the rack. The temperature setting should be factory settable. This unit should also include - humidity & temperature sensor		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
9.	Metal	Aluminium extruded profile		
10.	Side Panel	Detachable side panels (set of 2 per Rack)		
11.	General	✓ Dual 32 A PDU ✓ Receptacle Power Connectors each connected to separate PDU		

6.2.2 Server

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Processor	Latest series/ generation of 64 bit x86 processor(s) with Ten or higher Cores Processor speed should be minimum 2.4 GHz Minimum 2 processors per each physical server		
5.	RAM	Min. 24 DIMM slots, should be provided with 256 GB RAM using DDR4 DIMM's operating at 2666 MT/s (depending on processor model)		
6.	Internal Storage	2 x 300 GB SAS (10k rpm) hot swap disk with extensible bays		
7.	Network interface	2 X 20GbE LAN ports for providing Ethernet connectivity Optional: 1 X Dual-port 16Gbps FC HBA for providing FC connectivity		
8.	Power supply	Dual Redundant Power Supply		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
9.	RAID support	As per requirement/solution		
10.	Operating System	Licensed version of 64 bit latest version of Linux/ Unix/Microsoft® Windows based Operating system)		
11.	Form Factor	Rack mountable/ Blade		
12.	Virtualization	Shall support Industry standard virtualization hypervisor like Hyper-V, VMWARE and Citrix.		
13.	Storage controller	SAS Raid Controller with RAID 0/1		
14.	Bus Slots	Minimum of 2 Nos of PCIe 3.0 based mezzanine slots supporting Converged Ethernet adapters		
15.	Motherboard	Intel Chipset compatible with the offered processor		
16.	Interfaces	Minimum of 1 Internal USB 3.0 port, 1 Internal SD Card Slot		
17.	Redundancy	Must have port level and card level redundancy		
18.	Operating System & Virtualization Support	✓ Microsoft Windows Server (latest version) ✓ Red Hat Enterprise Linux (RHEL) (latest version) ✓ SUSE Linux Enterprise Server (latest version) ✓ VMware / feature rich virtualization software supporting solution design &		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		stack		
19.	Warranty	5 Year OEM Warranty		

6.2.3 Blade Chassis Specifications

S. No.	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**	<to be provided by the bidder>	
2.	**Model**	<to be provided by the bidder>	
3.	**Key Features:**		
4.	Minimum 6U size, rack-mountable, capable of accommodating minimum 8 or higher hot pluggable blades		
5.	Dual network connectivity of 10 G speed for each blade server for redundancy shall be provided		
6.	Backplane shall be completely passive device. If it is active, dual backplane shall be provided for redundancy.		
7.	Have the capability for installing industry standard flavors of Microsoft Windows, and Enterprise RedHat Linux OS as well as virtualization solution such as VMware.		
8.	DVD ROM shall be available in chassis, can be internal or external, which can be shared by all the blades allowing remote installation of software		
9.	Minimum 1 USB port		
10.	Two hot-plug/hot-swap, redundant 10 Gbps Ethernet or FCoE module with minimum 16 ports (cumulative), having Layer 2/3 functionality		
11.	Two hot-plugs/hot-swap redundant 16 Gbps Fiber Channel module for connectivity to the external Fiber channel Switch and ultimately to the storage device		
12.	Hot plug/hot-swap redundant power supplies to be provided, along with power cables		
13.	Power supplies shall have N+N. All power supplies modules shall be populated in the chassis.		

S. No.	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
14.	Required number of PDUs and power cables, to connect all blades, Chassis to Data Center power outlet.		
15.	Hot pluggable/hot-swappable redundant cooling unit		
16.	Provision of systems management and deployment tools to aid in blade server configuration and OS deployment		
17.	Blade enclosure shall have provision to connect to display console/central console for local management such as troubleshooting, configuration, system status/health display.		
18.	Single console for all blades in the enclosure, built-in KVM switch or Virtual KVM features over IP		
19.	Dedicated management network port shall have separate path for remote management.		
20.	Blade chassis shall be Electronic Industries Alliance Standard width rack mountable and provide appropriate rack mount kit		
21.	Enclosure should support full height / width and half height / width blades in the same enclosure, occupying a maximum of 10U rack height and it should support minimum 8 blade servers		
22.	Enclosure should be populated fully with power supplies of the highest capacity and energy efficiency of Platinum rating		
23.	Power subsystem should support N+N, N+1 power redundancy where N is greater than 1 for a fully populated chassis with all servers configured with the highest CPU configuration (150 W and above)		
24.	Each blade enclosure should have a cooling subsystem consisting of redundant hot pluggable fans or blowers enabled with technologies for improved power consumption and acoustics.		

S. No.	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
25.	Enclosure should support all Intel Xeon scalable processors based 2 CPU and 4 CPU blades		
26.	Should support built-in management software in redundancy		
27.	Should support single management console for all the blade servers across multiple chassis.		
28.	Solution should support templates to quickly make changes to the infrastructure, server BIOS version, MAC ID, NIC firmware version, WWPN, FC-HBA firmware version, Adapter QoS, Management module firmware version, UUIDs, Server Boot Policies, KVM IP, etc. of the infrastructure required for workload.		
29.	Requires 5 year OEM Warranty		

6.2.4 Next Generation Firewall (NGFW)

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Physical attributes	• Should be mountable on 19” Rack • Should act in high availability mode • Modular Chassis /Appliance Design • Internal redundant power supply		
5.	Interfaces	• Should have minimum 4X1GE ports and 2X10G port with necessary SFP loaded from day one. Should be scalable to add 2 or more 10G ports in future.		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		• Console Port 1 number		
6.	Performance and Availability	• Encrypted throughput: minimum 2 Gbps • Concurrent connections: up to 100,000 • Simultaneous VPN tunnels: 2000		
7.	Routing Protocols	• Static Routes • RIPv1, RIPv2 • OSPF		
8.	Protocols	• TCP/IP, PPTP • RTP, L2TP • IPSec, GRE, DES/3DES/AES • PPPoE, EAP-TLS, RTP • FTP, HTTP, HTTPS • SNMP, SMTP • DHCP, DNS • Support for Ipv6 • IPSEC		
9.	Other support	802.1Q, NAT, PAT, IP Multicast support, Remote Access VPN, Time based Access control lists, URL Filtering, support VLAN, Radius/ TACACS, Support multilayer firewall protection, Traffic shaping, Bandwidth monitoring		
10.	QoS	QoS features like traffic prioritization, differentiated services, committed access rate. Should support for QoS		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		features for defining the QoS policies.		
11.	Management	• Console, Telnet, SSHv2, Browser based configuration • SNMPv1, SNMPv2 , SNMPv3		
12.	Additional Features	• Should have inbuilt HDD of minimum 64 GB • Should support DDoS protection		
13.	Certifications	ICSA/NDPP/EAL4		

6.2.5 HIPS (Host Intrusion Prevention System)

#	Minimum Requirements	Bidder Compliance(Yes/No)	Product Documentation Reference
1	**Make**	<to be provided by the bidder>	
2	**Model**	<to be provided by the bidder>	
3	Proposed solution should protect against Distributed DoS attack and Solution should have the ability to lock down a computer (prevent all communication) except with management server.		
4	It should provide automatic recommendations against existing vulnerabilities		
5	Solution should support any pre-defined lists of critical system files for various operating systems and/or applications (web servers, dns, etc.) and support custom rules as well.		
6	Solution should have feature to take backup of infected files and restoring the same.		
7	Host IPS should be capable of recommending rules based on vulnerabilities with the help of virtual patching and should have capabilities to schedule recommendation scan and entire features of solution should be agentless.		

#	Minimum Requirements	Bidder Compliance(Yes/No)	Product Documentation Reference
8	Performance : Should have an aggregate throughput of no less than 200Mbps. Total Simultaneous Sessions – 10,000		
9	Features ✓ IPS should have Dual Power Supply ✓ IPS system should be transparent to network, not default gateway to Network ✓ IPS system should have Separate interface for secure management ✓ IPS system should be able to protect Multi Segment in the network, should be able to protect 4 segments.		
10	Real Time Protection • Web Protection • Mail Server Protection • Cross Site Scripting • SNMP Vulnerability • Worms and Viruses • Brute Force Protection • SQL Injection • Backdoor and Trojans • DoS/DDoS attack		
11	Stateful Operations • TCP Reassembly • IP Defragmentation • Bi-directional Inspection • Forensic Data Collection • Access Lists		
12	Signature Detection: Should have provision for Real Time Updates of Signatures, IPS Should support Automatic signature synchronization from database server on web Device should have capability to define User Defined Signatures		
13	Block attacks in Real Time • Drop Attack Packets • Reset Connections • Packet Logging		

#	Minimum Requirements	Bidder Compliance(Yes/No)	Product Documentation Reference
	• Action per Attack		
14	Alerts • Alerting SNMP • Log File • Syslog • E-mail		
15	Management • SNMP V1, V2, V3 • HTTP, HTTPS • SSHv2, Telnet, Console		
16	Security Maintenance • IPS Should support 24/7 Security Update Service • IPS Should support Real Time signature update • IPS Should support Provision to add static own attack signatures • System should show real-time and History reports of Bandwidth		

6.2.6 Network Switch

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Ports	• 24 or 48 (as per requirements) 10/100/1000 Base-TX Ethernet ports and extra 2 nos of Base-SX/LX ports All ports can auto-negotiate between 10Mbps/ 100Mbps/ 1000Mbps, half-duplex or full duplex and flow control for half-duplex ports.		
5.	Switch type	Layer 3		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
6.	MAC	Support 8K MAC address.		
7.	Backplane	56 Gbps or more Switching fabric capacity (as per network configuration to meet performance requirements)		
8.	Forwarding rate	Packet Forwarding Rate should be 70.0 Mpps or better		
9.	Port Features	Must support Port Mirroring, Port Trunking and 802.3ad LACP Link Aggregation port trunks		
10.	Flow Control	Support IEEE 802.3x flow control for full-duplex mode ports.		
11.	Protocols	• Support 802.1D, 802.1S, 802.1w, Rate limiting • Support 802.1Q VLAN encapsulation, IGMP v1, v2 and v3 snooping • 802.1p Priority Queues, port mirroring, DiffServ • Support based on 802.1p priority bits with at least 8 queues • DHCP support & DHCP snooping/relay/optional 82/ server support • Shaped Round Robin (SRR) or WRR scheduling support. • Support for Strict priority queuing & Sflow • Support for IPV6 ready features with dual stack • Support upto 255 VLANs and upto 4K VLAN IDs		
12.	Access Control	• Support port security • Support 802.1x (Port		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		based network access control). • Support for MAC filtering. • Should support TACACS+ and RADIUS authentication		
13.	VLAN	• Support 802.1Q Tagged VLAN and port based VLANs and Private VLAN • The switch must support dynamic VLAN Registration or equivalent Dynamic Trunking protocol or equivalent		
14.	Protocol and Traffic	• Network Time Protocol or equivalent Simple Network Time Protocol support • Switch should support traffic segmentation • Traffic classification should be based on user-definable application types: TOS, DSCP, Port based, TCP/UDP port number		
15.	Management	• Switch needs to have RS-232 console port for management via a console terminal or PC • Must have support SNMP v1,v2 and v3 • Should support 4 groups of RMON • Should have accessibility using Telnet, SSH, Console access, easier software upgrade through network using TFTP etc.		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		Configuration management through CLI, GUI based software utility and using web interface		

6.2.7 Storage

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Capacity	500+ TB		
5.	Solution/ Type	IP Based/iSCSI/FC/NFS/CIFS		
6.	Storage	• Storage Capacity should be as per Overall Solution Requirement (usable, after configuring in offered RAID configuration) • RAID solution offered must protect against double disc failure. • Disks should be preferably minimum of 3 TB capacity • To store all types of data (Data, Voice, Images, Video, etc) • Storage system capable of scaling vertically and horizontally		
7.	Hardware Platform	• Rack mounted form-factor • Modular design to		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		support controllers and disk drives expansion		
8.	Controllers	• At least 2 Controllers in active/active mode • The controllers / Storage nodes should be upgradable seamlessly, without any disruptions / downtime to production workflow for performance, capacity enhancement and software / firmware upgrades. • Storage should support non-disruptive online firmware upgrade for both Controllers and disk drives.		
9.	RAID support	RAID 0, 1, 1+0, 5+0, 6+0 and 10 (Dual Parity or Higher)		
10.	Disk drive support	Storage subsystem shall support 4TB/6TB/8TB or higher NLSAS/SATA/equivalent 7.2K drives in the same device array.		
11.	Cache	Minimum 128 GB of useable cache across all controllers. If cache is provided in additional hardware for unified storage solution, then cache must be over and above 128 GB.		
12.	Redundancy and High Availability	The Storage System should be able to protect the data against single point of failure with respect to hard disks, connectivity interfaces, fans and power		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		supplies		
13.	Management software	• All the necessary software (GUI Based) to configure and manage the storage space, RAID configuration, logical drives allocation, snapshots etc. are to be provided for the entire system proposed. • Licenses for the storage management software should include disc capacity/count of the complete solution and any additional disks to be plugged in in the future, upto max capacity of the existing controller/units. • A single command console for entire storage system. • Should also include storage performance monitoring and management software • Should provide the functionality of proactive monitoring of Disk drive and Storage system for all possible disk failures • Should be able to take "snapshots" of the stored data to another logical drive for backup		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		purposes		
14.	Data Protection	The storage array must have complete cache protection mechanism either by de-staging data to disk or providing complete cache data protection with battery backup for up to 4 hours		
15.	Converge	Storage converge solution with NSPoF (No Single Point of Failure) Architecture. The storage solution should support NAS and SAN as an integrated offering with high availability at each level. The architecture should allow upgrades of hardware and software for investment protection.		
16.	Protocols	Solution should be configured with required protocols for the solution CIFS / SMB 3 / NFS4 / iSCSI / FCoE / FC. All required protocols required for the solution to be enabled.		
17.	Operating System	The storage array should support operating system platforms and clustering on Windows / Linux		
18.	Cache Memory	Each controller / node should be provided with appropriate ARM scalable to 512 GB RAM with usable protected data cache for disk IO operations. If NAS controller with separate controllers is provided then additional RAM cache to be provided. The storage array must have complete cache protection mechanism either by de-staging data to disk / flash or protected with NVRAM.		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
19.	Global Hot Spare	System should have the capability to designate global hot spares that can automatically be used to replace a failed drive anywhere in the system. Storage system should be configured with required Global Hot-Spares for the different type and number of disks configured, as per system architecture best practices.		
20.	Thin Provisioning	Proposed array must be supplied with Thin provisioning for the configured capacity.		
21.	De-Duplication	Should provide de-duplication functionalities for the configured capacity.		
22.	Snapshots	Should be able to take snapshots of the stored data. Offered storage shall have support to make the snapshot in scheduled or auto snaps. Snapshot should support both block and file..		
23.	Replication	Storage array must have the capability to do remote replication using IP Technology.		
24.	Software Licenses	All necessary software and licenses to configure and manage storage space, RAID configuration, Logical Drive allocation, Snapshots, compression, de-duplication, replication, auto-tiering for the configured capacity to be provided from day 1.		

6.2.8 SAN Switch

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
25.	**Make**		<to be provided by the bidder>	
26.	**Model**		<to be provided by the bidder>	
27.	**Key Features:**			
28.	Converge	Fibre switch should be quoted with minimum 48 FC ports of 16 Gbps speed with all supported licenses from day one.		
29.	Protocols	Switch should have support for 8 / 16 Gbps HBA		
30.	Controllers	Switch should have auto sensing, zoning, integrate Ethernet and serial port for communication		
31.	Operating System	Switch should be rack mountable 1U size and should be supplied with mounting kit		
32.	Cache Memory	Switch should be equipped with redundant hot swap power supply and fan and allow hot swap ability with resetting the switch or affecting the operations of the switch		
33.	Host	Switch should be backward compatible		
34.	Connectivity	Switch should be capable for non-disruptive firmware upgrade and hot code activation		
35.	RAID Supports	Switch should be capable of end to end performance monitoring		
36.	Redundancy	Switch should have support for POST and online / offline diagnostics, non-disruptive daemon restart FC ping and path info (FC trace route)		
37.	Disk Drive Support	Switch should be capable to interface with host based adapters (HBA) of multiple OEM, supporting multiple		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		operating systems		
38.	Global Hot Spare	Switch should have zoning and security features – hardware & software ACL and Policy based security & centralized fabric management		
39.	Support	✓ Secure access ✓ FC based authentication ✓ RADIUS, SSH, SNMP ✓ Port Binding ✓ Port Masking ✓ Hardware based inter switch linking / trunking ✓ Dynamic load balancing of links with no overhead ✓ Web based management and should support CLI ✓ Alert based on threshold value for temperature, fan status, power supply status and port status ✓ Shall support different port type such as FL port, F Port, M Port (mirror port), E Port ✓ Self-discovery based on switch type (U port) ✓ Optional port type control in access gateway mode F		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		port and NPIV enabled N port		
40.	Licenses	• All relevant licenses for all the defined features and scales		

6.2.9 Fire proof enclosure

The overall design of the safe should be suitable for safe storage of computer diskettes, tapes, smart cards and similar devices and other magnetic media, paper documents, etc. the safe should have adequate fire protection.

Capacity	300 Litres
Capacity	300 Litres
Temperature to Withstand	1000° C for at least 1 hour
Internal Temperature	30° C after exposure to high temperature For 1 hour
Locking	2 IO-lever high security cylindrical / Electronic lock

6.2.10 Core Router

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Multi-Services	Should deliver multiple IP services over a flexible combination of interfaces		
5.	Ports	As per overall network architecture proposed by the bidder, the router should be populated with required number of LAN/WAN ports/modules, with cable for connectivity to other network elements.		
6.	Speed	As per requirement, to cater to entire bandwidth		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		requirement of the project.		
7.	Interface modules	Must support upto 10G interfaces. Must have capability to interface with variety interfaces.		
8.	Protocol Support	Must have support for TCP/IP, PPP Frame relay and HDLC Must support VPN Must have support for integration of data and voice services Routing protocols of RIP, OSPF, and BGP. Support IPV4 & IPV6		
9.	Manageability	Must be SNMP manageable		
10.	Scalable	• The router should be scalable. For each slot multiple modules should be available. The chassis offered must have free slots to meet the scalability requirement of expansion of the project in the future.		
11.	Traffic control	Traffic Control and Filtering features for flexible user control policies		
12.	Bandwidth	Bandwidth on demand for cost effective connection performance enhancement		
13.	Remote Access	Remote access features		
14.	Redundancy	• Redundancy in terms of Power supply(s). Power supply should be able to support fully loaded chassis All interface modules, power supplies should be		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		hot-swappable		
15.	Security features	• MD5 encryption for routing protocol • NAT • URL based Filtering • RADIUS Authentication • Management Access policy • IPSec / Encryption L2TP		
16.	QOS Features	• RSVP • Priority Queuing • Policy based routing • Traffic shaping • Time-based QoS Policy Bandwidth Reservation / Committed Information Rate		

6.2.11 Internet Router

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Multi-Services	Should deliver multiple IP services over a flexible combination of interfaces		
5.	Ports	As per overall network architecture proposed by the bidder, the router should be populated with required number of LAN/WAN ports/modules, with cable for connectivity to other network elements.		
6.	Interface modules	Must support up to 10G interfaces as per the design.		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		Must have capability to connect with variety of interfaces.		
7.	Protocol Support	• Must have support for TCP/IP, PPP, X.25, Frame relay and HDLC • Must support VPN • Must have support for integration of data and voice services • Routing protocols of RIP, OSPF, and BGP. • Support IPV4, IPV6 • Support load balancing		
8.	Manageability	Must be SNMP manageable		
9.	Traffic control	Traffic Control and Filtering features for flexible user control policies		
10.	Bandwidth	Bandwidth on demand for cost effective connection performance enhancement		
11.	Remote Access	Remote access features		
12.	Redundancy	• Redundancy in terms of Power supply(s). Power supply should be able to support fully loaded chassis All interface modules, power supplies should be hot-swappable		
13.	Security features	• MD5 encryption for routing protocol • NAT • URL based Filtering • RADIUS/AAA Authentication • Management Access policy • IPSec / Encryption		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		• L2TP		
14.	Security Feature	• RSVP • Priority Queuing • Policy based routing • Traffic shaping • Time-based QoS Policy • Bandwidth Reservation / Committed Information Rate		

6.2.12 L3 Switch

S. No.	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**	<to be provided by the bidder>	
2.	**Model**	<to be provided by the bidder>	
3.	**Key Features:**		
4.	✓ 24 or 48 (as per requirements) 10/100/1000 Base-TX Ethernet ports / FX Ports (splits as needed) and extra 2 number of Base-SX / LX ports ✓ All ports can auto-negotiate between 10 Mbps / 100 Mbps / 1000 Mbps, half duplex or full duplex and flow control for half duplex ports		
5.	Switch Type : Layer 3		
6.	MAC - Support 8K MAC Address		
7.	Backplane ✓ 56 Gbps or more switching fabric capacity for 24 ports ✓ 104 Gbps or more switching fabric capacity for 48 ports		
8.	Forwarding Rate- Packet forwarding rate should be 70 Mbps or better		

S. No.	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
9.	Port Features - Must support Port Mirroring, Port Trunking and 802.3ad LACP Link Aggregation port trunks		
10.	Flow Control - Support IEEE 802.3x flow control for full duplex mode ports		
11.	Protocols ✓ Support 802.1D, 802.1S, 802.1w, Rate limiting ✓ Support 802.1X Security standards ✓ Support 802.1Q VLAN encapsulation, IGMP v1, v2 and v3 snooping ✓ 802.1p Priority Queues, port mirroring, DiffServ ✓ Support based on 802.1p priority bits with at least 8 queues ✓ DHCP support and DHCP snooping / relay / optional 82 / server support ✓ Shaped Round Robin (SRR) or WRR scheduling support ✓ Support for IPV6 ready features with dual stack ✓ Support up to 255 VLANs and up to 4K VLAN IDs ✓ Support IGMP snooping and IGMP Querying ✓ Support Multicasting ✓ Should support lip protection and Loop detection ✓ Should support ring protection		
12.	Access Control ✓ Support port security ✓ Support 802.1x (Port based network access control) ✓ Support for MAC filtering ✓ Should support TACACS+ and		

S. No.	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
	RADIUS authentication		
13.	VLAN ✓ Support 802.1Q Tagged VLAN and port based VLAN and Private VLAN ✓ Switch must support dynamic VLAN Registration or equivalent ✓ Dynamic Trunking protocol or equivalent		
14.	Protocol & Traffic ✓ Network Time Protocol or equivalent Simple Network Time Protocol support ✓ Switch should support traffic segmentation ✓ Traffic classification should be based on user definable application types : TOS, DSCP, Port based, TCP/UDP port number		
15.	Management ✓ Switch needs to have RS-232/USB console port for management via a console terminal or PC ✓ Must have support SNMP v1, v2 and v3 ✓ Should support 4 groups of RMON ✓ Should have accessibility using Telnet, SSH, Console Access, easier software upgrade through network using TFTP, etc. Configuration management through CLI, GUI based software utility and using web interface.		

6.2.13 L2 Switch

S. No.	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**	<to be provided by the bidder>	
2.	**Model**	<to be provided by the bidder>	
3.	**Key Features:**		
4.	19" Rack Mountable stackable switch with min 24 Nos. 10/100/1000 copper input POE/PoE+ (15.4W) ports and additional support of 4x1G SFP, support for external/internal redundant power supply.		
5.	Switch should support for minimum 96 Gbps of forwarding throughput & minimum 70 mbps forwarding rate		
6.	The switch should support dedicated stacking port separate from uplink ports with 80 Gbps of stacking bandwidth to put minimum 8 switches into a single stack group.		
7.	Switch should have static, default IP routing enabled from day one.		
8.	Switch shall have IEEE 802.3ad Link Aggregation Control Protocol (LACP) with up to 8 links (ports) per trunk.		
9.	It shall have IEEE 802.1s Multiple Spanning Tree Protocol and provide legacy support for IEEE 802.1d STP and IEEE 802.1w RSTP or equivalent technology and static routes.		
10.	Switch should have feature to protect access ports using port security, TACACS/TACACS+, Radius, storm control, Access Control List both port, VLAN based.		
11.	Switch should have queuing as per IEEE 802.1P standard on all ports with mechanism for traffic shaping and rate limiting features for specified Host, network, Applications etc.		
12.	Should have Power supply 230 Volt 50Hz input		
13.	The switch should support IPv6 Guard, IPv6 RA-Guard, IPv6 DHCP-Guard, Source-Guard features		

S. No.	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
14.	Switch should support automated image installation, configuration & automatic configuration of per port QoS to reduce switch provisioning time & effort.		
15.	Must have SNMP v1, v2, v3 from day one		
16.	Should have CLI and GUI based management console port.		
17.	The switch should support IEEE 802.3az from day-1		
18.	The switch should be IPv6 ready		
19.	The proposed switch should be EAL2/ NDPP certified by common Criteria body at the time of delivery.		

6.2.14 Tape Drive

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Technology	LTO 6		
5.	Number Drives	Two LTO 6 Drives		
6.	Media Slots	Minimum 45		
7.	Interface	Minimum 4 Gbps FC Interface		
8.	Power Supplies	Redundant Hot Swap Power supply		
9.	Fans	Redundant Hot Swap cooling fans		
10.	Software	Security and Remote Management Software		
11.	Supported Backup Software	Should support industry leading backup software		
12.	Accessories	With all required cables and accessories to install and configure in standard 19" rack and to connect to Server/SAN switch		

6.2.15 Server Load Balancer

S. No.	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**	<to be provided by the bidder>	
2.	**Model**	<to be provided by the bidder>	
3.	**Key Features:**		
4.	Device should support load balancing of both TCP and UDP based traffic using algorithms like round robin, weighted round-robin, least connections, persistent connects, etc.		
5.	Device should provide minimum throughput of 10Gbps		
6.	Device should provide 4x10G ports scalable to additional 4x10G ports		
7.	Should support Client availability (Heartbeat) monitoring		
8.	Should be support High Availability in Active-Active, Active-Passive mode.		
9.	Should be Manageable using CLI(SSH), WebUI(SSL), SNMP (V1, V2, V3), etc.		
10.	The management option should allow configuration, operation, firmware upgrade, traffic reporting, error logs, status logs		
11.	Should support IPv6 from day one		
12.	Should support static and dynamic routing		
13.	Should support Global Server Load balancing, URL based Load balancing, HTTP, HTTP redirection, HTTP Layer 7 redirection, DNS redirection, DNS Fallback redirection,		
14.	Should be able to create and load http/SSL certificates		
15.	Should be Rack mountable & should be supplied with Indian standard AC power cord.		
16.	Should support multiple instances having dedicated CPU, memory, SSL & I/O for guaranteed performance.		

6.2.16 Internet Router

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Technology	LTO 6		
5.	Number Drives	Two LTO 6 Drives		
6.	Media Slots	Minimum 45		
7.	Interface	Minimum 4 Gbps FC Interface		
8.	Power Supplies	Redundant Hot Swap Power supply		
9.	Fans	Redundant Hot Swap cooling fans		
10.	Software	Security and Remote Management Software		
11.	Supported Backup Software	Should support industry leading backup software such as Symatec Net Backup		
12.	Accessories	With all required cables and accessories to install and configure in standard 19" rack and to connect to Server/SAN switch		

6.2.17 Backup software

S. No.	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**	<to be provided by the bidder>	
2.	**Model**	<to be provided by the bidder>	
3.	**Key Features:**		
4.	The software shall be able to back up the necessary and relevant video feeds from storage, various databases, etc.		
5.	Should support file level backup/recovery		
6.	Should perform Scheduled unattended backup using policy-based management for all Server and OS platforms		
7.	The software should support on-line backup and restore of various applications and Databases		
8.	Should support database platforms like Microsoft Exchange Server, Oracle,		

S. No.	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
	Microsoft SQL Server, Microsoft SharePoint, Sybase, MySQL, Informix, IBM Domino (Lotus), SAP, IBM DB2, etc		
9.	Should support backup hardware like tape, virtual tape, optical, disk, interface hardware, etc.		
10.	The backup software should be capable of having multiple back-up sessions simultaneously		
11.	The backup software should support different types of backup such as Full back up, Incremental back up, Differential back up, Selective back up, Point in Time back up and Progressive Incremental back up and snapshots		
12.	The backup software should support different types of user interface such as GUI, Web-based interface		
13.	Should have logging and reporting features		

6.2.18 Centralised Antivirus software

S. No.	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**	<to be provided by the bidder>	
2.	**Model**	<to be provided by the bidder>	
3.	**Key Features:**		
4.	Shall be able to scan through several types of compression formats.		
5.	Must update itself over internet for virus definitions, program updates etc. (periodically as well as in push-updates in case of outbreaks)		
6.	Able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)		
7.	Shall be able to scan only those file types which are potential virus carriers (based on true file type)		
8.	Shall be able to scan for HTML, VBScript Viruses, malicious applets and ActiveX controls		
9.	Shall provide Real-time product Performance Monitor and Built-in		

S. No.	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
	Debug and Diagnostic tools, and context- sensitive help.		
10.	The solution must support multiple remote installations		
11.	Shall provide for virus notification options for Virus Outbreak Alert and other configurable Conditional Notification.		
12.	Should be capable of providing multiple layers of defence.		
13.	Shall have facility to clean, delete and quarantine the virus affected files.		
14.	Should support in-memory scanning so as to minimize Disk IO.		
15.	Should support heuristic scanning to allow rule-based detection of unknown viruses		
16.	Updates to the scan engines should be automated and should not require manual intervention		
17.	All binaries from the vendor that are downloaded and distributed must be signed and the signature verified during runtime for enhanced security		
18.	Updates should be capable of being rolled back in case required		
19.	Should support various types of reporting formats such as CSV, HTML and text files		
20.	Shall be able to automatically push any updates, patches, fixes to all client machines to ensure up-to-date antivirus protection for all IT devices and systems.		

6.2.19 Directory service

S. No.	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**	<to be provided by the bidder>	
2.	**Model**	<to be provided by the bidder>	
3.	**Key Features:**		
4.	Should be compliant with LDAP v3		
5.	Support for integrated LDAP compliant directory services to record information for users and system		

S. No.	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
	resources		
6.	Should provide authentication mechanism across different client devices / PCs		
7.	Should provide support for Group policies and software restriction policies		
8.	Should support security features, such as Kerberos, Smart Cards, Public Key Infrastructure (PKI), etc.		
9.	Should provide support for X.500 naming standards		
10.	Should support that password reset capabilities for a given group or groups of users can be delegated to any nominated user		
11.	Should support that user account creation/deletion rights within a group or groups can be delegated to any nominated user		
12.	Should support directory services integrated DNS zones for ease of management and administration/replication.		

6.2.20 KVM Module

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	KVM Requirement	Keyboard, Video Display Unit and Mouse Unit (KVM) for the IT Infrastructure Management at Data Center		
5.	Form Factor	19” rack mountable		
6.	Ports	minimum 8 ports		
7.	Server Connections	USB or KVM over IP.		
8.	Auto-Scan	It should be capable to auto scan servers		
9.	Rack Access	It should support local user port for rack access		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
10.	SNMP	The KVM switch should be SNMP enabled. It should be operable from remote locations		
11.	OS Support	It should support multiple operating system		
12.	Power Supply	It should have dual power with failover and built-in surge protection		
13.	Multi-User support	It should support multi-user access and collaboration		

6.3 Network Bandwidth – Technical Specifications & Functional Specifications

6.3.1 Internet Bandwidth (for edge equipments)

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Connectivity Type	MPLS L2/L3 , MPLS Cloud Should Support IP Multicast, PIM, BGP and OSPF protocol		
5.	Bandwidth	1680 Mbps (Total)		
6.	Physical Connectivity	Wired Underground		
7.	SLA	99.99 Uptime		

6.3.2 Primary & Secondary Internet Bandwidth (for CCC to Safe City)

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Connectivity Type	MPLS L2/L3 , MPLS Cloud Should Support IP Multicast, PIM, BGP and OSPF protocol		
5.	Bandwidth	1 Gbps		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
6.	Physical Connectivity	Wired Underground		
7.	SLA	99.99 Uptime		

6.3.3 Primary & Secondary Internet Bandwidth at ICCC (DC to DR)

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Connectivity Type	MPLS L2/L3 , MPLS Cloud Should Support IP Multicast, PIM, BGP and OSPF protocol		
5.	Bandwidth	500 Mbps		
6.	Physical Connectivity	Wired Underground		
7.	SLA	99.99 Uptime		

Field Elements & Accessories

6.4 Surveillance System

6.4.1 Functional Specifications – Surveillance System

Functional Requirement of the overall Surveillance System can be categorized into following components:

1. Information to be Captured by Edge Devices
2. Information to be analysed at CCCs/ICCC
3. Role Based Access to the Entire System
4. Storage / Recording Requirements
5. Other General Requirements

6.4.1.1 Information to be captured by Edge Devices

Surveillance Cameras being one of the core sub modules of ICCC project, it is important that their selection and placement is carefully done to ensure the full coverage of the traffic junction along with all associated junction arms, accuracy of the information captured on the field and they are rugged, durable & compact. These cameras need to work on 24 X 7 basis and transmit quality video feeds to the CCCs & ICCC. However, Ludhiana Police may take the regular review of the requirements for video resolution, FPS and may change these numbers to suit certain specific requirements (for example, there could be a situation when certain cameras are required to be viewed at higher FPS for specific period. It is estimated that not more than 5% of the cameras would be required to be viewed at higher FPS at a given point of time).

6.4.1.2 Information to be analyzed at CCCs/ICCC

The proposed Video Management System should provide a complete end-to-end solution for security surveillance application. The control center shall allow an operator to view live / recorded video from any surveillance camera on the IP network. The combination of control center and the IP network would create a virtual matrix, which would allow switching of video streams around the system.

It has been envisaged that all surveillance cameras would not be simultaneously viewed at Integrated Command & Control Center. The viewing shall vary from time to time which shall help to manage traffic at the junctions and coordinate with the field police officers.

6.4.1.3 Role-Based Access to the Entire System

Various users should have access to the system using single sign on and should be role based. Different roles which could be defined (to be finalized at the stage of implementation) could be Administrator, Supervisor, Officer, Operator, etc. Apart from role based access, the system should also be able to define access based on location. Other minimum features required in the role based authentication systems are as follows:

a. The management module should be able to capture basic details (including mobile number & email id) of the Police Personnel & other personnel requiring Viewing / Administration rights to the system. There should be interface to change these details, after proper authentication.
b. Rights to different modules / sub-modules / functionalities should be role based and proper log report should be maintained by the system for such access.
c. The system should be with login name & password enabled to ensure that only the concerned personnel are able to login into the system
d. There should be provision to specify hierarchy of operators / officers for control of the cameras from various locations.
e. The number of users shall increase as per phase wise implementation. MSI is expected to estimate and provision the same based on the phase wise requirements.
f. Windows Active Directory/LDAP or any such system can be used to design role based access.

6.4.1.4 Storage/Recording Requirements

It is proposed that the storage solution shall be modular enough to ensure compliance to the changes in storage / recording policy, to be evolved upon initial deployment of the system. The following storage requirements shall be fulfilled by the MSI as scope for the project:

a. The Data Center (DC) shall be co-located at Integrated Command & Control Center (ICCC)
b. The storage estimation shall be done basis of following requirements:

System	Number of Days for recording	Primary Storage Requirement	Secondary Storage Requirement
Surveillance System	30 days	7	30 Days and 90 days for Flagged data (critical incidents) for 10% of total number of cameras

c. Data on storage would be over-written automatically by newer data after the stipulated time period. If some data is flagged by police personnel (or by designated personnel) as important data / evidence data due to some reporting of crime or accident in the area or due to court order or due to suspicious activity, it would need to be stored for longer duration, as per requirements. Ludhiana Police would analyse such flagged data every 3months to take such decisions for preservation of the flagged data beyond 90 days.
d. Full audit trail of reports to be maintained for 90 days.
e. Archival/Backup to be done on NAS / Scale-out NAS / SAN / Unified/ Tape or equivalent storage solution

f. Retrieval time for any data stored on secondary storage should be max. 4 hours for critical data & 8 hours for other data.

g. The recording servers / system, once configured, shall run independently of the Video Management system and continue to operate in the event that the Management system is off-line.

h. The system shall support the use of separate networks, VLANs or switches for connecting the cameras to the recording servers to provide physical network separation from the clients and facilitate the use of static IP addresses for the devices.

i. The system shall support H.265, MPEG-4 and MJPEG compression formats for all analog cameras connected to encoders and all IP cameras connected to the system.

j. The system shall record the native frame rate and resolution supplied by the camera or as configured by the operator from the system administration server.

k. The system should not limit amount of storage to be allocated for each connected device.

l. The on-line archiving capability shall be transparent and allow Ludhiana Police to browse and archive recordings. Required additional space on primary storage or additional media to be provided along with solution by the MSI

m. The system shall allow for the frame rate, bit rate and resolution of each camera to be configured independently for recording. The system shall allow the user to configure groups of cameras with the same frame rate, bit rate and resolution for efficient set-up of multiple cameras simultaneously.

n. The system shall support archiving or the automatic transfer of recordings from a camera's default database to another location on a time-programmable basis without the need for user action or initiation of the archiving process. Archiving shall allow the duration of the camera's recordings to exceed the camera's default database capacity. Archives shall be located on either the recording server or on a connected network drive. If the storage area on a network drive becomes unavailable for recording the system should have the ability to trigger actions such as the automatic sending of email alerts and sound alerts to necessary personnel.

o. Bandwidth optimisation

- The Recording Server / System shall offer different codec (H.265, MJPEG, MPEG-4, etc.) and frame rate (CIF, 4CIF, QCIF or higher) options for managing the bandwidth utilization for live viewing on the Client systems. (through use of multiple systems such as transcoding server)
- From the Ludhiana Police, the user shall have the option of having video images continually streamed or only updated on motion to conserve bandwidth between the Client systems and the Recording Server.

p. The Recording Server / System shall support camera (analogue and IP cameras) devices from various manufacturers.

q. The Recording Server / System shall support the PTZ protocols of the supported devices listed by the camera OEMs.

r. The system shall support full two-way audio between Client systems and remote devices. (Audio from certain set of cameras can be recorded in future).

s. Failover Support

- The system shall support automatic failover for recording servers. This functionality shall be accomplished by failover server as a standby unit that shall take over in the event that one of a group of designated recording servers fails. Recordings shall be synchronized back to the original recording server once it is back online.
- The system shall support multiple failover servers for a group of recording servers.

t. SNMP Support

- The system shall support Simple Network Management Protocol (SNMP) in order for third-party software systems to monitor and configure the system.
- The system shall act as an SNMP agent which can generate an SNMP trap as a result of rule activation in addition to other existing rule actions.

6.4.1.5 Other General Requirements

1. Management/Integration functionality

a. The Surveillance System shall offer centralised management of all devices, servers and users.

b. The Surveillance System should not have any limit on the number of cameras to be connected for Surveillance, Monitoring and Recording. Any increase in the no. of cameras should be possible by augmentation of Hardware and software licenses components with additional cost as per RFP conditions for any additional requirements.

c. The Surveillance System should have ability to knit the video streams from multiple cameras, based on the date/time stamp. Every video stream shall have date, time, source camera location, FPS etc. water-marked. These attributes shall be finalised at the System Design time. There shall be a centralised NTP server, from which all devices shall synchronise the date and time.

d. The Surveillance System shall support distributed viewing of any camera in the system using Video walls or big screen displays.

e. The Surveillance System shall support alarm management. The alarm management shall allow for the continuous monitoring of the operational status and event-triggered alarms from system servers, cameras and other external devices.

f. It should be possible to integrate the Surveillance System with 3rd-party software, to enable the users to develop customized applications for enhancing the use of video surveillance solution. For e.g., integrating alarm management to initiate SMS, E-Mail, VoIP call etc.

g. It should be possible to integrate social media platforms to Surveillance System to enable Ludhiana Police to track and monitor certain trending incident or crime.

h. The Management system shall store the overall network elements configuration in central database, either on the management server computer or on a separate DB Server on the network.

i. System should be able to be integrated with Event Management / Incident Management System, if implemented by Ludhiana Police in future.

2. System Administration functionality

a. The System Administration Server shall provide a feature-rich administration client for system configuration and day-to-day administration of the system

b. The System Administration Server shall support different logs related to the Management Server

- The System Log
- The Audit Log
- The Alert Log
- The Event Log

3. Rules

The system shall support the use of rules to determine when specific actions occur. Rules shall define what actions shall be carried out under specific conditions. The system shall support rule initiated actions such as:

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

4. Client System

a. The Client system shall provide remote users with rich functionality and features as described below.

- Viewing live video from cameras on the surveillance system
- Browsing recordings from storage systems
- Creating and switching between multiple of views.

- Viewing video from selected cameras in greater magnification and/or higher quality in a designated hotspot.
- Controlling PTZ cameras.
- Using digital zoom on live as well as recorded video.
- Using sound notifications for attracting attention to detected motion or events.
- Getting quick overview of sequences with detected motion.
- Getting quick overviews of detected alerts or events.
- Quickly searching selected areas of video recording for motion (also known as Smart Search).

5. Remote Web Client

The web-based remote client shall offer live view from field cameras, including PTZ control and event / output activation. The Playback function shall give the user concurrent playback of multiple recorded videos with date, alert sequence or time searching.

a. User Authentication – The Remote Client shall support logon using the user name and password credentials

6. Matrix Monitor

a. Matrix Monitor – The Matrix Monitor feature shall allow distributed viewing of multiple camera on the system on any monitor

b. The Matrix Monitor feature shall access the H.265/MJPEG/MPEG4 stream from the connected camera directly and not sourced through the recording server

7. Alarm Management Module

a. The alarm management module shall allow for continuous monitoring of the operational status and event-triggered alarms from various system servers, cameras and other devices. The alarm management module shall provide a real-time overview of alarm status or technical problems while allowing for immediate visual verification and troubleshooting.

b. The alarm management module shall provide interface and navigational tools through the client including;

- Graphical overview of the operational status and alarms from servers, network cameras and external devices including motion detectors and access control systems.
- Intuitive navigation using a map-based, hierarchical structure with hyperlinks to other maps, servers and devices or through a tree-view format.

c. The module shall include flexible access rights and allow each user to be assigned several roles where each shall define access rights to cameras.

d. VMS should be capable to accept third party generated events / triggers

e. Based on alarms/alerts, customised/standard alert messages should be published on VMD/PA, after authorisation by a supervisor/operator.

8. Other Miscellaneous Requirements

a. System should have a facility to create CDs or other storage media for submission to Judiciary, which can be treated evidence for legal matters. Such storage media creation should be tamper proof and MSI to provide appropriate technology so that integrity and quality of evidence is maintained as per requirements of the judiciary. Bidder is required to specify any additional hardware / software required for this purpose & the same can be listed in miscellaneous section of the commercial bid. MSI shall also prepare the guideline document to be followed by the Police Personnel for the retrieval of Video / images from the CCTV System so as to maintain integrity of the evidence. Such a guideline document should include methods of retrieval of data, check-list to be followed and flowchart of the entire process to be followed.

b. All the systems proposed and operationalisation of Video Management System should comply with requirements of IT Acts.

c. Any hardware or software required to achieve the functional requirement and technical solution of the overall Project (may not be not specified in the schedule) is to be proposed in the Bid and the applicable cost shall be borne by the MSI.

d. Bidder shall be required to provide a standardized Mobile Application to integrate smart phones and tablets for 2-way communication with the Surveillance System in a secure manner. LudhianaPolice may provide such tablets / smart phones to the designated Police Personnel. It shall be responsibility of MSI to configure such tablets / Smartphone, for the Surveillance System being implemented a part of this project, and ensure that all the necessary access is given to these mobile users. Functionalities to be provided through mobile application: Viewing of any video steam from Central VMS, uploading of video / pictures central VMS, Location based GIS Map access, tagging of mobile device/location information for all relevant functionalities.

e. There would be the provision for Third party audit periodically, paid by LSCL separately. LSCL reserves the right to appoint any Independent Evaluation Agency at any time during the phases of the project.

6.4.2 Technical Specifications – Surveillance System

6.4.2.1 PTZ Camera out-door

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Video Compression	H.265		
5.	Video Resolution	1920 X 1080		
6.	Frame rate	Min 25 fps		
7.	Operating frequency	50 Hz		
8.	Image Sensor	1/3" OR ¼" Progressive Scan CCD / CMOS		
9.	Lens	Auto-focus, 4.3 – 129 mm (corresponding to 30 X) PIRIS Lens		
10.	Multiple Streams	Dual streaming with 2nd stream at minimum 720P at 30fps at H.265 individually configurable		
11.	Minimum Illumination	Colour: 0.05 lux, B/W: 0.01 lux (at 30 IRE, F 1.2) or better		
12.	Day/Night Mode	Colour, Mono, Auto		
13.	Wide Dynamic Range	True WDR 120 db or better		
14.	S/N Ratio	≥ 50dB		
15.	PTZ	Pan: 360° endless/continuous, 0.2 to 300°/s (auto), 0.2 to 100°/s (Manual) Tilt: 90°, 0.2 to 100°/s (Auto), 0.2 to 40°/s (Manual) 30 optical zoom and 10x digital zoom Pre-set tour 256 preset positions, Tour recording, Guard tour		
16.	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control,		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		backlight compensation, Gain Control, , Electronic Image Stabilization		
17.	Protocol	HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, ONVIF Profile S & preferably G		
18.	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption		
19.	Local Storage	Minimum 64 GB Memory card in a Memory card slot. In the event of failure of connectivity to the central server the camera shall record video locally on the SD card automatically. After the connectivity is restored these recordings shall be automatically merged with the server recording such that no manual intervention is required to transfer the SD card based recordings to server.		
20.	Intelligent Video	Motion Detection & Tampering alert		
21.	Alarm I/O	Minimum 1 Input & Output contact for 3rd part interface		
22.	Operating conditions	0 to 50°C		
23.	Casing	NEMA 4X / IP-66 rated & IK10		
24.	Power	802.3af PoE (Class 0) and 12VDC/24AC/ / POE+ IEEE 902.3at Compliant		
25.	Physical security	Detection of camera tampering and Detection of Motion should be possible using either camera or VMS		
26.	Certifications	UL/EN,CE,FCC, ONVIF		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
27.	IR Illumination	Internal > 150 meters		

6.4.2.2 Fixed OutDoor Box/Bullet Camera

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Video Compression	H.265		
5.	Video Resolution	1920 X 1080		
6.	Frame rate	50 FPS at all resolutions with Controllable Bit Rate/ Bandwidth and Frame Rate		
7.	Operating frequency	50 Hz		
8.	Image Sensor	1/3" Progressive Scan CCD / CMOS		
9.	Lens Type	Varifocal, C/CS Mount, IR Correction Full HD lens compatible to camera imager		
10.	Lens	5-50mm IR corrected, CS-mount lens, P-Iris		
11.	Electronic Shutter	1/28000 s to 2 s or better		
12.	Multiple Streams	The camera shall be able to setup and stream out minimum three (3) stream profiles. Each stream profile can have its own compression resolution, frame rate and quality independently up to Full HD @ 30 FPS		
13.	Minimum Illumination	Colour: 0.2 Lux @ 30 IRE B/W: 0.01 @ 30 IRE 0 Lux with Built in or External IR, IR Range 50 m		
14.	IR Cut Filter	Automatically Removable IR-cut filter		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
15.	Day/Night Mode	Yes with IR Cut Filter		
16.	S/N Ratio	≥ 50 dB		
17.	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, Auto back focus		
18.	Wide Dynamic Range	True WDR 120 db or better		
19.	Privacy Masks	Minimum 20 configurable 3D zones		
20.	Audio	Full duplex, line in and line out, G.711, G.726		
21.	Local storage	microSDXC up to 64GB (Class 10) In the event of failure of connectivity to the central server the camera shall record video locally on the SD card automatically. After the connectivity is restored these recordings shall be automatically merged with the server recording such that no manual intervention is required to transfer the SD card based recordings to server.		
22.	Edge Storage	SD Card Slot with minimum 64GB Support Class 10 speed		
23.	Protocol	HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, ONVIF Profile S & preferably G		
24.	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption, IEEE 802.1Xa network access control, Digest authentication, User access log		
25.	Intelligent Video	Motion Detection & Tampering alert		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
26.	Alarm I/O	Minimum 1 Input & Output contact for 3rd part interface		
27.	Operating conditions	-10 degree C to 65 degree C		
28.	Interface	RJ 45, 100 Base TX		
29.	Humidity	Humidity 10–95% RH (condensing)		
30.	Casing	NEMA 4X / IP-66 rated & IK 09		
31.	Certification	UL2802 / EN, CE ,FCC, IEC		
32.	Power	802.3af PoE (Class 0) and 12VDC/24AC/ / POE+ IEEE 902.3at Compliant		
33.	Physical security	Detection of camera tampering and Detection of Motion should be possible using either camera or VMS		

6.5 Environmental sensors

- The environment sensors shall be integrated with ICCC to capture and display/ provide feed on Temperature, Humidity, Pollutants like SoX, NoX, CoX, etc PM2.5, PM10, Noise Pollution. The data it collects is location-marked.
- Various environment sensors shall sense the prevailing environment conditions and send the data to ICCC where real time data resides and the same shall be made available to various other departments and applications for decision making.
- Then this information is relayed instantaneously to signage – large, clear, digital display screens which communicates to the citizens the prevalent environmental conditions.
- The data should be collected in a software platform that allows third party software applications to read that data..
- MSI can also make use of Variable messaging displays wherever possible.
- The sensor management platform should allow the configuration of the sensor to the network and location details etc.

6.5.1 Functional Specification – Environmental Sensors

#	Functional Specifications
1.	The environment sensors should be have the following capabilities

2.	They should be ruggedized enough to be deployed in open air areas on streets and parks
3.	They should be able to read and report at least the following parameters • Temperature • Relative Humidity • Ambient Light • Noise • CO • NO2 • So2 • O3 • PM 2.5 • PM 10 • UVa • UVb • CO2
4.	Sensor should be able to communicate its data using wireless technology (GSM/WIFI)
5.	Data should be collected in a software platform that allows third party software applications to read that data. Data Buffer Capacity up to 3 years
6.	Data Capture Frequency – 30 seconds
7.	Li-Ion Battery Backup of 4 hours
8.	Aesthetic & Elegant Aerodynamic design
9.	Stabilization Time on power outages < 10 minutes
10.	LEDs on the enclosure for easy visual indications
11.	Software Solution • Solution to enable APIs for mobile & Web services • APIs to provide • Status of Devices • NAQI Colour Schema as per NAQI, India • Lead pollutant contributing to NAQI • Architecture to support computation of new parameters such as o Now Cast NAQI o Zonal Limits of pollutants if any
12.	Data Analytics • Lead pollutants, trends & Source level apportionments • Integration and analysis of various northbound API's including traffic / parking & Environment to derive insights. • ICCC shall have provision to displayof feed / analytics for the temporarily installed cameras. The number of cameras cannot be anticipated now.
13.	The sensor management platform should allow the configuration of the sensor to the network and also location details etc.
14.	One of the most important requirement is that the display panel should display the optimum/accepted/recommended level of all the pollutant along with their live status. This will

	help the citizens as well as authority to compare and analyse the status of air pollutant in their respective area and thereby take corrective measures

6.5.2 Technical Specifications – Environmental Sensor

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	General	• They should be ruggedized enough to be deployed in open air areas such as Traffic Junctions, Streets, Parks, Parking Lots etc. • The sensor should be able to communicate its data using wireless technology • The data should be collected in a software platform that allows third party software applications to read that data. • The sensor management platform should allow the configuration of the sensor to the network and also location details etc.		
5.	Measurement component	Temperature, Humidity, Ambient Light, Sound, CO, NO2, NOX, CO2, SO2		
6.	Measurement range	• NO2: 0 to 10 ppm • NOX : 0 to 50ppm , 5000ppm • SO2 : 0 to 500 ppm • CO : 0 to 1000 ppm • O3: up to 1000 ppb • CO2 : 0 to 5% (5000 ppm) • PM 2.5: 0 to 230 micro gms / cu.m • PM 10: 0 to 450 micro gms / cu.m		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		• Light: up to 10,000 Lux • UV: up to 15 mW/ cm2 • Noise: up to 120 dB (A) • Temperature : 0 to 100° C		
7.	Repeatability	±0.5% FS		
8.	Zero Drift	±1.0% FS max./week ±2.0% FS/week max. if range is less than 200ppm ±2.0% FS max./month for O2 Meter		
9.	Temperature and Humidity Sensor	• Real-time Temperature Range: 0ºC ~ 70ºC • Real-time in Air Humidity Level Display (up to 100%)		
10.	Span drift	±2.0% FS max./week ±2.0% FS max./month for O2 meter		
11.	Response speed	60 seconds max. for 90% response from the analyzer Inlet		
12.	Connectivity & Data Interface	USB / Ethernet /Wireless (GPS ,GSM, Wi-Fi- 802.11 n/ac)		
13.	Operating Temperature	0 to 55 °C		

6.6 Public Address system – Technical & Functional Specification

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	PAS System	Should have the capability to control individual PAS i.e. to make an announcement at select location (1:1) and all locations (1: many) simultaneously. The PAS should also support both, Live and Recorded inputs		
5.	Speaker	Minimum 2 speakers, To be used for Public Address		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		System		
6.	Connectivity	IP based		
7.	Access Control	Access control mechanism would be also required to establish so that the usage is regulated.		
8.	Integration	with VMS and Command and Control Centre		
9.	Construction	Cast Iron Foundation and M.S. Pole, Sturdy Body for equipment		
10.	Battery	Internal Battery with different charging options (Solar/Mains)		
11.	Power	Automatic on/off operation		
12.	Casing	IP-66 rated for housing		
13.	Operating Conditions	-10° to 65°C		

6.7 Panic Button and Emergency Call Box - Technical & Functional Specification

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Construction	Cast Iron/Steel Foundation, Sturdy Body for equipment		
5.	Call Button	Watertight Push Button, Visual Feedback for button press		
6.	Speaker	To be used for Public Address System		
7.	Connectivity	GSM/PSTN/Ethernet as per solution offered		
8.	Sensors	For tempering/Vandalism		
9.	Battery	Internal Battery with different charging options (Solar/Mains)		
10.	Power	Automatic on/off operation		
11.	Casing	IP-66 rated for housing		
12.	Operating	-10° to 65°C		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
	conditions			

6.8 Digital Variable Message Display (VMD)

The MSI shall presently install IP based VMS boards at identified locations in the city of Ludhiana. These VMD boards shall have different characteristics depending upon the location and purpose of installation. VMD board displays are to be controlled by personnel from the ICCC. The purpose of the VMD boards is to provide the commuters with information about traffic conditions and alternate routes in case of high traffic on roads

6.8.1 Functional Specifications – Variable Message Display

#	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
1	**Make**	<to be provided by the bidder>	
2	**Model**	<to be provided by the bidder>	
3	**System Requirements**		
a.	The system should be capable to display warnings, traffic advice, route guidance and emergency messages to motorists from the ICCC in real time.		
b.	The system should also be capable to display warnings, traffic advice, route guidance and emergency messages to motorist by using local PC/Laptops.		
c.	The VMD should display text and graphic messages using Light Emitting Diode (LED) arrays.		
d.	The System should able to display failure status of any LED at ICCC.		
e.	The System should support Display characters in true type fonts and adjustable based on the Operating system requirement.		
f.	The VMD workstation at the ICCC should communicate with the VMD controller through the network. It should send out command data to the variable message display controller and to confirm normal operation of the signboard. In return, the VMD workstation should receive status data from the VMD controller.		
g.	VMD controllers should continuously monitor the operation of the VMD via the provided		

#	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
	communication network.		
h.	Operating status of the variable message display should be checked periodically from the ICCC		
i.	It shall be capable of setting an individual VMD or group of VMD's to display either one of the pre-set messages or symbols entered into the computer via the control computer keyboard or by another means.		
j.	It shall be capable of being programmed to display an individual message to a VMD or a group of VMD's at a pre-set date and time.		
k.	A sequence of a minimum of 10 messages/pictures/ pre-decided sign or group of signs shall be possible to assign for individual VMD or group of VMD's.		
l.	It shall also store information about the time log of message displayed on each VMD. The information stored shall contain the identification number of the VMD, content of the message, date and time at which displayed message/picture starts and ends.		
m.	The central control computer shall perform regular tests (pre-set basis) for each individual VMD. Data communication shall be provided with sufficient security check to avoid unauthorized access.		
4	**Variable Message Displays (VMD) application**		
a.	Central Control Software allows controlling multiple VMD from one console.		
b.	Capable of programming to display all types of Message/ advertisement having alphanumeric character in English, Hindi, Punjabi (any other language asked by LSCL) and combination of text with pictograms signs. The system should have feature to manage video / still content for VMD. The system should have capability to divide VMD screen into multi-parts to display diverse form of information like video, text, still images,		

#	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
	advertisements, weather info, city info etc. The system should also provide airtime management and billing system for paid content management		
c.	Capable of controlling and displaying messages on VMD boards as individual/ group.		
d.	Capable of controlling and displaying multiple font types with flexible size and picture sizes suitable as per the size of the VMD.		
e.	Capable of controlling brightness & contrast through software.		
f.	Capable to continuously monitor the operation of the Variable Message Display board, implemented control commands and communicate information to the ICCC via communication network.		
g.	Real-time log facility – log file documenting the actual sequence of display to be available at central control system.		
h.	Multilevel event log with time & date stamp.		
i.	Access to system only after the authentication and acceptance of authentication based on hardware dongle with its log.		
j.	Location of each VMD will be plotted on GIS Map with their functioning status which can be automatically updated.		
k.	Report generation facility for individual/group/all VMDs with date and time which includes summary of messages, dynamic changes, fault/repair report and system accessed logs, link breakage logs, down time reports or any other customized report.		
l.	Configurable scheduler on date/day of week basis for transmitting pre-programmed message to any VMD unit.		
m.	Various users should access the system using single sign on and should be role based. Different roles which could be defined (to be finalized at the stage of SRS) could be Administrator, Supervisor, Officer, Operator, etc.		

#	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
n.	Apart from role based access, the system should also be able to define access based on location.		
o.	Rights to different modules / Sub-Modules / Functionalities should be role based and proper log report should be maintained by the system for such access		
p.	Components of the architecture should provide redundancy and ensure that there are no single points of failure in the key project components. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage.		
q.	The architecture should adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc. provisions for security of field equipment as well as protection of the software system from hackers and other threats shall be a part of the proposed system. Using Firewalls and Intrusion detection systems such attacks and theft shall be controlled and well supported (and implemented) with the security policy. The virus and worms attacks shall be well defended with Gateway level Anti-virus system, along with workstation level Anti-virus mechanism. There shall also be an endeavour to make use of the SSL/VPN technologies to have secured communication between Applications and its end users. Furthermore, all the system logs shall be properly stored & archived for future analysis and forensics whenever desired.		
r.	Ease of configuration, ongoing health monitoring, and failure detection are vital to the goals of scalability, availability, and security and should be able to match the growth of the environment.		
s.	System shall use open standards and protocols to the extent possible		
t.	Facility to export reports to excel and PDF formats.		

#	Minimum Specifications	Bidder Compliance (Yes/No)	Product Documentation Reference
3.	**Remote Monitoring**		
a.	All VMD shall be connected/configured to ICCC for remote monitoring through network for two way communication between VMD and control Room to check system failure, power failure & link breakage.		
b.	Remote Diagnostics to allow identifying failure up to the level of failed individual LED.		

6.8.2 Technical Specifications – Variable Message Display

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Location	To be installed at locations identified by Authority and the text on the sign must be readable even in broad daylight		
5.	LED Type	DIP		
6.	Pixel Configuration	1R/1G/1B		
7.	Pixel Density	10000 dots/m2		
8.	Environmental Grade	UV Resistant		
9.	Colour	True Colour		
10.	Brightness & Legibility	○ To be read even in broad daylight without any shade ○ The displayed image shall not appear to flicker to the normal human eye >6000 cd/m2		
11.	Luminance Class	L-3 as per EN 12966		
12.	Contrast Ratio	R2-R3 as per EN 12966		
13.	Beam Width	B6+ : Viewing angle shall ensure message readability		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		for citizens, motorists, pedestrians, etc. on the respective locations		
14.	Best Viewing Distance	10m – 100m		
15.	Display capability	○ Fully programmable, full colour, full matrix, LED displays Alpha-numeric, Pictorials, Graphical & video		
16.	Display Language	To support both pictograms and bilingual (English and Punjabi) text		
17.	Display Front Panel	It shall utilize a front face that is smooth, flat, scratch-resistant, wipe-clean 100% anti-glare		
18.	Message Creation	Through both a Central Control Room Application and a local Laptop/Device loaded with relevant software		
19.	Language	Multilingual (Punjabi/English/Hindi) and all fonts supported by windows		
20.	Auto Dimming	Auto dimming adjusts to ambient light level.		
21.	In built Sensor	Photoelectric sensor		
22.	Storage capacity	Minimum 60 GB		
23.	Display Area	Customized (2.88m x 1.96m with 5-10% tolerance)		
24.	Number of Lines & Characters	The number of lines and characters can be customized as per the requirement (Min 3 Lines & 10 Characters)		
25.	Brightness & contrast	Controlled through software		
26.	Display Driving method	Direct current control driving circuit. Driver card of display applies Direct		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		Current Technology		
27.	Display Style	Steady, flash, partial flash, right entry, left entry, top entry, bottom entry, canter spread, blank, and dimming		
28.	Connectivity	IP Based		
29.	Access Control	Access control mechanism would be also required to establish so that the usage is regulated.		
30.	Integration	○ Interface with GPRS or Ethernet ○ Integration with Command and Communications Center and service providers for offering G2C and B2C services		
31.	Construction	Mounting structure shall use minimum 6 Mtrs. high hexagonal/octagonal MS Pole or suitable structure with 5.5 mtr. Minimum vertical clearance under the VMS sign from the Road surface.		
32.	Battery	○ 230VAC+ 15%, 50Hz, Single Phase (automatically re-start in the event of an electricity supply failure) ○ Batteries with solar charging options can also be recommended as back up		
33.	Power	Automatic on/off operation		
34.	Casing	○ Weather-proof		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		Display for VMS o IP-66 rated for housing all control equipment		
35.	Operating conditions	-10° to 65°C		
36.	Message Validity	If the controller is unable to connect to the server for the next message, it shall not display the old message, which has passed its expiry time. Instead it shall be programmed to display a default message.		

6.8.3 Application Software for VMD (Control Messaging Application at Data Center)

The Application System for Controlling Messaging for VMD shall:

1) Be deployable over multiple (3 to 4) workstations.
2) Ensure that provision for feeding/updating the following information:
   a. VMD messages and information
   b. Types of possible scenarios per VMD
   c. Types of possible messages to be displayed on each VMD during various scenarios
3) Ensure that the normal operator users are not able to publish any custom message and shall only display predefined sets of messages.
4) The application shall have an option for Supervisor (someone with appropriate authority) to bypass the control during certain situations and to write in free-text mode.
5) Ensure that users can publish specific messages for managing traffic and also general informative messages.
6) Allow an operator to seamlessly toggle between multiple VMD points at each workstation in order to send specific messages to specific locations.
7) Accommodate different access rights to various control unit functionalities depending on operator status and as agreed with the client.

6.9 VMS (Video Management Software)

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	General	• The VMS should be built on "Open Platform" i.e. should be able to support any ONVIF compliant IP cameras without any limitation to any kind of licensing. • VMS server shall be deployed in a clustered server environment/Support in built for high availability and failover for directory & recording servers • VMS shall be capable of being deployed in a virtualized server environment without loss of any functionality. • All CCTV cameras locations shall be overlaid in graphical map in the VMS Graphical User Interface (GUI). • The cameras selection for viewing shall be possible via clicking on the camera location on the graphical map • The graphical map shall be of high resolution enabling operator to zoom-in for specific location while selecting a camera for viewing.		
5.	Scalability	The VMS shall have ability to connect and integrate other technologies and		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		third party software systems (e.g. ANPR, RLVD, Face Detection, Speed Violation Detection, Environmental Sensors etc.) and act as a singular platform for entire surveillance and security system. The system should be able to bi-directionally and dynamically exchange data between various software applications in real-time as well as schedule transfer. It should Support for unlimited cameras, servers, sites and clients. Support for storage expandability.		
6.	User Management	Centrally controlled user management - Users, roles, rules and privileges should be stored on the central VMS server allowing any authorized user to log into any workstation.		
7.	Device Discovery	The VMS shall have ability to easily install, configure, modify, search and remove surveillance devices with automatic discovery of IP devices.		
8.	Event Management	The VMS shall have ability to enforce custom settings for event detection, alarm notification, recording, input/out (I/O) control, and other features in response to events. The alarm management module shall support graphical displays with interactive icons to display the status of the cameras & other inputs.		
9.	Software/Patch Upgrade	• The VMS shall have ability to enforce custom settings for event		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		detection, alarm notification, recording, input/out (I/O) control, and other features in response to events. • The alarm management module shall support graphical displays with interactive icons to display the status of the cameras & other inputs. • For future requirement, migration to h.265 should happen with a simple firmware upgrade		
10.	Recording & Transfer	• Should support dual streaming • Should allow each stream to be viewed independently by client viewer. • Recording from connected cameras Should be stored in individual databases. • Should support multiple storage formats • Should support recording in all resolution at desired FPS • Should support video cum audio recording • shall support automatic failover for recording • shall be capable of transferring recorded images to recordable media (such as CD/DVD and/or tapes) • or Video Exports with VMS's Native Format along with Watermark and Encrypted with SSL / TSL technology, one can protect the video		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		tampering and prove that the video is not tampered		
11.	Motion Zone Masking	VMS should Support Exclusion of Motion /Masked Zones to enhances optimized recordings and storage.		
12.	Customized Record Retention	Should support Customized recording retention period for specific camera, group, area etc.		
13.	Remote User Support	Should support multiple remote users via network/web browser/client software		
14.	Device Grouping	• The VMS shall have ability to logically group devices based on installation location, device type, configuration type or any other predefined rules. • Individual cameras/ devices should have the capability to inherent rules from parent group/ subgroup.		
15.	Parameter Configuration	The VMS shall have ability to configure multiple streams with different quality parameters e.g. Codec (H.264, H.265 MPEG, JEPG) , resolution, frame & bit rate etc.		
16.	Image Stabilization	The VMS shall have Electronic Image Stabilization feature		
17.	Device Search	The VMS shall have ability to search and view device(s) based on standard criteria like ID, Name, Location, Group, Type etc.		
18.	Storage Indexing	VMS should store video feeds in a standard folder tree structure so that it		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		becomes easy for system admin to browse videos categories based on year, month, date and time wise. Also the file name should indicate important attributes like camera location, date, time etc.		
19.	Video Wall /Monitor Support	• Multiple monitor support: The system should allow connecting multiple monitors on single client workstation and display different contents on each of the connected monitor. • All panes / tiles should indicate mode (live or recoded), source (camera name/location) and date/time and applied quality information (FPS, CODEC). • The font color shall be changed automatically in sync with the video/image to have a clear text reading at any point of time. • A matrix view should support multiple formats on video wall and any number of multiple screen divisions.		
20.	PTZ Control	PTZ configuration and control including presets, patterns, patrolling, priority, Zoom in/out and permissions.		
21.	Shortcut Keys	Along with menu-driven interface, a VMS should also support custom shortcut keys to helps operators quickly switch between different modules/screens, change views or panes/tiles		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		and to carry out playback functions.		
22.	Image Snapshot	System should allow creating a still image from live or recorded feed and storing it into a workstation.		
23.	Digital Zoom	Digital zoom to enlarge portion of an image to provide superior zooming capability.		
24.	Display Interface	Option to view surrounding cameras: The system should enable operators to select master camera feed and based on group/subgroup details, its surrounding cameras should be automatically displayed on separate panes. These panes/tiles should be dynamically generated so that operator does not need to manually pull the feeds from desired cameras.		
25.	Video Search and retrieval	The VMS shall have ability to quickly search and retrieve recordings: Search methods should include search by camera(s), group, date/time, alarm/event / bookmark list, smart (motion) search by creating motion index or by generating thumbnail summary of a video archive to locate specific event.		
26.	Playback Control	The system should offer following playback controls like Play/Pause, Lock speed, Forward playback (1x, 2x, 4x), Reverse playback (-1x, -2x, -4x), Slow forward playback (frame by frame, 1/8x, 1/4x,1/3x, 1/2x, 1x), Slow reverse playback		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
27.	Camera Tempering	The VMS should provide a centralized camera tampering detection solution in real-time by automatically identifying tampering to ensure video image capture and integrity. The solution sends an alert when the following potential tampering is detected: • Scene too bright — e.g. flash light, direct sun, laser pointer that is pointed at the camera, causing it to become over saturated. • Scene too dark — not enough light to see a clear image, if camera is covered. • Camera is covered or blocked — if something is blocking or partially blocking most of the camera's field of view. • Camera redirection detection — if camera is redirected from its' initial position of field of view (FOV). • Unfocused or blurred view — if the camera was sprayed with rain or its focus changed. The System should be able to detect tampering on any IP camera that has been discovered in the VMS		
28.	Mobile App	The bidder needs to provide a Mobile App and integrate it with the VMS system for 2-way communication with the 10000 in a secure manner. The App should be able to		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		provide Role-based access to the users		
29.	Reports	The system should provide interactive reporting interface with standard and user-defined custom reports and filtering options to: • Review currently logged in users and functions being performed. • Retrieve audit trails - user activities, errors and system logs. • View list of hardware units and selected configuration options. • List down configured users and corresponding roles & permissions. • View details of bookmarks, event/alarm history and exported evidences.		
30.	SDK	The VMS must be supplied along with its well documented Software Development Kit (SDK): The SDK should include a rich, easy-to-use Application Programming Interface (API) that supports the most common programming languages.		

6.10 VAS (Video Analytics Software)

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	**General**	✓ The Video Analytics		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
	requirements	shall be designed to provide Intelligent Video Analysis for 24/7 surveillance with support for devices from different vendors ✓ Support any architecture namely distributed, centralized and hybrid ✓ Support system openness without using any proprietary format ✓ Support commercial-off-the-shelf computing hardware without the need of any proprietary hardware ✓ Able to produce reliable analytics at lower resolutions like 4CIF resolution in order to save the computation ✓ Able to process at variable resolution and frame rate when if necessary ✓ It shall support open platform Video Management System (VMS). ✓ It shall provide ONVIF device discovery ✓ It shall get video from camera or VMS and send alarms to VMS to be viewed in VMS client ✓ It shall stream the Analytics Video to VMS using open interface protocol like ONVIF. ✓ It shall support multiple regions of analytics on single		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		video feed ✓ It shall support multiple features to be enabled for each of the regions ✓ It shall support feature based scheduling so that that alarms can be enabled or disabled for a certain period of time ✓ It shall support both Virtual line and Virtual area based features. The virtual area can be of any shape and can be bound by at least 10 end points. ✓ It shall support both indoor and outdoor environment. ✓ It shall support setting of minimum and maximum object size for detection. ✓ It shall support masking of area in a view ✓ It shall support object masking. ✓ It shall support color detection for vehicle & Object. ✓ It shall support alarms to filter based on object color, size, speed and aspect ratio. ✓ It shall support analytics capability to run both on server as well as edge (on camera). ✓ It shall support simultaneous running of different features both on edge as well as server for same camera ✓ It shall support		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		camera independent licensing ✓ The System Should be capable to do the analytics on Live Video Cameras as well as Stored Video records from such cameras		
5.	Suspicious incident /Object detection	✓ It shall detect person loitering in a virtual area for more than a pre-defined period. ✓ It shall detect crowd assembling in a pre-defined area. The count for the crowd determination should be pre-defined. It shall be able to provide live crowd count. ✓ The VA shall support dense and sparse crowds for crowd counting and crowd flow detection ✓ The VA shall detect object left out or abandoned in a virtual area by a person beyond a certain pre-defined period. ✓ The VA shall detect object removed by a person beyond a certain pre-defined period. ✓ The VA shall detect counter flow of people (such as people moving in a wrong way) ✓ Should be able to track a Person/ moving Object till the last point of the camera view		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		✓ The applications should also be able to do People search based on a given description/attributed/Sketch/Full length photograph ✓ Should have an interface to Create sketches, Composite (Human like Figure) of the suspect based on description. There Shall be different options available for describing hair color and style, Facial Attributes, shirts, trousers, patterns, etc.		
6.	Traffic Management Features	✓ It shall detect vehicle or group of vehicle moving in a wrong way. ✓ It shall detect a vehicle parked in an area for a pre-defined period. ✓ It shall detect congestion due to vehicles		
7.	Other Features	It shall be able to stitch up to 4 camera videos with overlapped view and provide the stitched view. It shall be able to stabilize the video when camera is shaking (such as, due to wind) and shall be able to stream the stabilized video to VMS. Ability such that alerts can be searched and categorized based on this information. i. Timestamp (date & time) ii. Alert Name		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		iii. Alert Type iv. Alert Location v. Text Description vi. Associated Region It shall provide video summary of all the alarms. It shall provide reporting option to export reports of alarms in PDF, EXCEL and Image formats and also option to schedule it. It shall support email and FTP of alarm data and also option to schedule it. It shall be able to provide comparison reports for different months and year		

6.11 Industrial Grade 8 Port PoE+ Switch

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Enclosure Type	Desktop, rack-mountable 1U		
5.	Subtype	Gigabit Ethernet		
6.	Ports	4 x 10/100/1000 (PoE+) + 4 x 10/100/1000 (PoE) + 2 x combo Gigabit SFP		
7.	Power Over Ethernet (PoE)	PoE+		
8.	PoE Budget	180 W		
9.	Performance	Forwarding performance (64-byte packet size): 38.69 Mpps Switching capacity: 52 Gbps		
10.	Remote Management	SNMP 1,2,3, RMON 1,2,3,9 Telnet, HTTP, HTTPS		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
	Protocol			
11.	Authentication Method	RADIUS, TACACS+		
12.	Features	Flow control, layer 2 switching, BOOTP support, VLAN support, IGMP snooping, Syslog support, DoS attack prevention, port mirroring, DiffServ support, Weighted Round Robin (WRR) queuing, MAC address filtering, Broadcast Storm Control, IPv6 support, Multicast Storm Control, Unicast Storm Control, firmware upgradable, SNTP support, Spanning Tree Protocol (STP) support, Rapid Spanning Tree Protocol (RSTP) support, Multiple Spanning Tree Protocol (MSTP) support, Trivial File Transfer Protocol (TFTP) support, Access Control List (ACL) support, Quality of Service (QoS), MLD snooping, reset button, LLDP support, DHCP relay, DHCP client, Energy Efficient Ethernet, Generic Attribute Registration Protocol (GARP), Generic VLAN Registration Protocol (GVRP), Type of Service (ToS), 2 fans, 4.1MB packet buffer		
13.	Compliant Standards	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3af, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3at, IEEE 802.3az		
14.	RAM	128 MB		
15.	Flash Memory	32 MB		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
16.	Status Indicators	Port transmission speed, system, PoE, link/activity		
17.	**Expansion / Connectivity**			
18.	Interfaces	4 x 1000Base-T - RJ-45 - PoE+ - 30 W		
19.		4 x 1000Base-T - RJ-45 - PoE - 15.4 W		
20.		2 x 1000Base-T - RJ-45		
21.		2 x - SFP		
22.	**Power**			
23.	Power Device	Internal power supply		
24.	Voltage Required	AC 120/230 V (50/60 Hz)		
25.	**Environmental Parameters**			
26.	Min Operating Temperature	-10 Degree C		
27.	Max Operating Temperature	65 Degree C		
28.	Humidity Range Operating	10 - 90% (non-condensing)		

6.12 Online UPS for Field components

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Capacity	1KV or more Line Interactive		
5.	Technology	Automatic Voltage Regulation		
6.	Input Frequency Range	50 Hz +/- 5%		
7.	Output Frequency Range	50 Hz +/- 5%		
8.	Output Voltage	180V AC - 280V AC Single Phase		
9.	Input Voltage	230 VAC		
10.	Voltage	+/-5% (or better)		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
	Regulation			
11.	Output Waveform	True Sine Wave		
12.	Output Power Factor	0.6 or more		
13.	Battery Backup	Minimum backup of 1 Hour on full load		
14.	Battery Type	VRLA (Valve-regulated Lead Acid battery)		
15.	General Operating Temperature	-10 to 65 Degree Celsius		
16.	Alarms & Indications	All necessary alarms & indications essential for performance monitoring of UPS like mains fail, low battery		
17.	Bypass	Automatic, Manual Bypass Switch		
18.	Optional SMPS	Power Management from SNMP manager and Web browser		

6.13 Poles for mounting cameras and other SMART components

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Pole type	Hot Dip Galvanized after Fabrication with Silver coating of 86 micron as per IS:2629; Fabrication in accordance with IS-2713		
5.	Height	5 Meter OR higher, As-per-requirements for different types of cameras & Site conditions.		
6.	Pole Diameter	Bottom section : 97.9mm Middle Section : 76.2mm Top Section : 65.2mm		
7.	Bottom base plate	Minimum base plate of size 30 x 30 x 15 cms		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
8.	Mounting facilities	Capable to Mount 3-4 Cameras, Environmental Sensors, PA Systems, ECB, and Digital Display boards with related Junction box.		
9.	Foundation	Casting of Civil Foundation with foundation bolts, to ensure vibration free erection (basic aim is to ensure that video feed quality is not impacted due to winds in different climatic conditions). Expected foundation depth of min. 100cms. Please refer to Earthing standards mentioned in RFP		
10.	Protection	Lightning arrestors with proper grounding		
11.	Sign-Board and Number-Plate	A sign board describing words such as "This area under surveillance" and with serial number of the pole.		

6.14 Junction Box

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Built	• The Outdoor Utility Cabinet will be constructed with a front sheet steel door with 3 point Locking system to ensure the security of the cabinet. Side and Wall Panels shall be double wall constructed, with fixing bolts internal to the cabinet. • The Cabinet should have the required frames to mount the required components like, network device, power, edge router,		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
		UPS, LIU, battery, etc.		
5.	Utility & IP rating	Should be Made for 24/7/365 Outdoor Applications; The Utility Cabinet shall be IP 66 rated (Regulatory Standard Compliance) for ingress protection.		
6.	Size	The cabinet has to be provided of size suitable for the mounting of the associated network devices, power, and UPS, LPU/mini T server and Battery components securely and safely within the cabinet.		
7.	Power Slot	3 x 5 way Indian Standard PDU's has to be provided to support the site equipment. PDU type should be as per actual requirement.		
8.	Installation	Each Cabinet will be mounted on a raised height Plinth, 600 - 1000 mm high, as per site requirements. FAN Cooling unit shall be inherent in the design.		
9.	Cable Management	Proper cable management should be provided		
10.	Cable Routing	Power connection cable shall be provided from the nearest access point to the Outdoor Utility Cabinet through Power meter enclosure.		

6.15 Body Camera

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Dimensions	95.9 mm x 52.2 mm x 27.6 mm (3.78" x 2.06" x 1.09") ±5%		
5.	Weight	100-150 Grams		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
6.	Lens	f/2.0 , 130° wide angle		
7.	Connection Interface	USB 2.0		
8.	Storage	64 Gb or Higher		
9.	Wi-Fi	Yes		
10.	Bluetooth	Yes		
11.	Microphone	Yes		
12.	Battery Life (Fully Charged)	12 Hours or more		
13.	Resolution	Full HD 1080P		
14.	Frame Rate	30 FPS		
15.	Video Compression	H.264/H.265		
16.	Operating Temperature	-20°C (-4°F) ~ 65°C (149°F)		
17.	Storage Temperature	-25°C (-13°F) ~ 70°C (158°F)		
18.	IP Rating	IP67		
19.	Viewing Angel	130° (diagonal)		
20.	InfraRed	Built-in		
21.	Required Accessories	USB cable/360° rotatable clip/Adapter/Velcro holder		

6.16 Body Camera docking station

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
1.	**Make**		<to be provided by the bidder>	
2.	**Model**		<to be provided by the bidder>	
3.	**Key Features:**			
4.	Dimensions	(Max.)423 mm x 105 mm x 54 mm +/- 10%		
5.	Weight (Max.)	1000 Gram +/- 10%		
6.	Connection Interface	USB 3.0		
7.	Network Port	WAN: 10/100/1000 Mbps Ethernet LAN: 10/100 Mbps Ethernet		
8.	Operating Temperature	0°C (32°F) ~ 40°C (104°F)		

S. No.	Parameters	Minimum Specifications	Bidder Compliance(Yes/No)	Product Documentation Reference
9.	Storage Temperature	-20°C (-4°F) ~ 70°C (158°F)		
10.	Power Supply (Max.)	19V / 3.42A		
11.	Certificate	CE/FCC		
12.	Operating System	Microsoft Windows 7, 8, 10		
13.	Camera docking capacity	6 or higher		

7 Annexure II: Detailed Scope of Work and Considerations

7.1 Scope of Work

7.1.1 Inception Phase

The MSI will be responsible for preparation of detailed project plan. The plan shall address at the minimum the following:

i. Define an organized set of activities for the project and identify the interdependence between them.

ii. Resource planning and loading for each phase/activity. This must also indicate where each resource would be based during that phase, i.e. onsite at the LSCL office or off site at MSI premises.

iii. Establish and measure resource assignments and responsibilities

iv. Highlight the milestones and associated risks

v. Communicate the project plan to stakeholders with meaningful reports.

vi. Measure project deadlines and performance objectives.

vii. Project Progress Reporting. During the implementation of the project, the MSI should present weekly reports. This report will be presented in the steering committiee meeting to LSCL. The report should contain at the minimum the under mentioned:

   a. Results accomplished during the period (weekly)

   b. Cumulative deviations from the schedule date as specified in the finalized Project Plan

   c. Corrective actions to be taken to return to planned schedule of progress

   d. Plan for the next week

   e. Proposed revision to planned schedule provided such revision is necessitated by reasons beyond the control of MSI

   f. Support needed

   g. Highlights/lowlights

   h. Issues/Concerns

   i. Risks/Show stoppers along with mitigation

viii. Identify the activities that require the participation of client personnel (including LSCL, the Program Management Unit etc.) and communicate their time requirements and schedule early enough to ensure their full participation at the required time.

7.1.2 Requirement Phase

The MSI must perform the detailed assessment of the business requirements and IT Solution

requirements as mentioned in this RFP. Based on the understanding and its own individual assessment, MSI shall develop & finalize the System Requirement Specifications (SRS) in consultation with LSCL and its representatives. While doing so, MSI at least is expected to do following:

i. MSI shall study and revalidate the requirements given in the RFP with LSCL and submit as an exhaustive FRS document.

ii. MSI shall develop the FRS and SRS documents.

iii. MSI shall develop and follow standardized template for requirements capturing and system documentation.

iv. MSI must maintain traceability matrix from SRS stage for the entire implementation.

v. MSI must get the sign off from user groups formed by LSCL.

vi. For all the discussion with LSCL team, MSI shall be required to be present at LSCL office with the requisite team members.

vii. Prior to starting the site clearance, the MSI shall carry out survey of field locations as specified in Annexure IX, for buildings, structures, fences, trees, existing installations, etc.

viii. The infrastructure of existing traffic signal and other street ICT infrastructure may need to be dismantled and replaced with the new systems which are proposed and required under the scope of the project. The infrastructure like poles, cantilevers, cabling, aspects etc. should be reused to derive economies for the project with prior approval of LSCL. The dismantled infrastructure shall be delivered at the LSCL designated location without damage at no extra cost.

ix. All existing road signs which are likely to be effected by the works are to be carefully taken down and stored. Signs to be re-commissioned shall be cleaned, provided with new fixings where necessary and the posts re-painted in accordance with LSCL 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.

x. The MSI shall directly interact with electricity boards for provision of mains power supply at all desired locations for field solution. LSCL shall facilitate the same. The recurring electricity charges will be borne by LSCL as per actual consumption.

7.1.3 Design Phase

The MSI shall build the solution as per the Design Considerations detailed in Section 5. The solution proposed by MSI should comply with the design considerations requirements as mentioned therein.

7.1.4 Development Phase

The MSI shall carefully consider the scope of work and provide a solution that best meets the project's requirements. Considering the scope set in this RFP, the MSI shall carefully consider the solutions it proposes and explicitly mention the same in the technical proposal. The

implementation of the application software will follow the procedure mentioned below:

a. Software Products (Configuration and Customization): In case MSI proposes software products the following need to be adhered:

   i. MSI will be responsible for supplying the application and licenses of related software products and installing the same so as to meet project requirements.

   ii. MSI shall have provision for procurement of licenses in a staggered manner as per the actual requirement of the project.

   iii. The MSI shall perform periodic audits to measure license compliance against the number of valid End User software licenses consistent with the terms and conditions of license agreements, volume purchase agreements, and other mutually agreed upon licensed software terms and conditions. The MSI shall report any exceptions to license terms and conditions at the right time to LSCL. However, the responsibility of license compliance solely lies with the MSI. Any financial penalty imposed on LSCL during the contract period due to license non-compliance shall be borne by MSI.

   iv. MSI shall also supply any other tools & accessories required to make the integrated solution complete as per requirements. For the integrated solution, the MSI shall supply:

      a) Software & licenses.

      b) Supply tools, accessories, documentation and provide a list of the same. Tools and accessories shall be part of the solution.

      c) System Documentation: System Documentation both in hard copy and soft copy to be supplied along with licenses and shall include but not limited to following. Documentation to be maintained, updated and submitted to LSCL regularly :

         - Functional Requirement Specification (FRS)
         - High level design of whole system
         - Low Level design for whole system / Module design level
         - System Requirements Specifications (SyRS)
         - Any other explanatory notes about system
         - Traceability matrix
         - Technical and product related manuals
         - Installation guides
         - User manuals
         - System administrator manuals
         - Toolkit guides and troubleshooting guides
         - Other documents as prescribed by LSCL

- Quality assurance procedures
- Change management histories
- Version control data
- SOPs, procedures, policies, processes, etc developed for LSCL
- Programs :
  - Entire source codes
  - All programs must have explanatory notes for understanding
  - Version control mechanism
  - All old versions to be maintained
- Test Environment :
  - Detailed Test methodology document
  - Module level testing
  - Overall System Testing
  - Acceptance test cases

These documents need to be updated after each phase of project and to be maintained updated during entire project duration. The entire documentation will be the property of LSCL.

7.1.5 Integration Phase

The Command and control center should be integrated with feeds of all tracks/component under the ICCC Project. The MSI shall provide the testing strategy including traceability matrix, test cases and shall conduct the testing of various components of the software developed/customized and the solution as a whole. The testing should be comprehensive and should be done at each stage of development and implementation.

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

S. No.	Departments/Systems	Minimum Integration Requirements
1)	City Surveillance & ITMS	• Integrates with existing cameras and new cameras. Should support multiple video sources from multiple locations. Platform should have no limitation in displaying the number of CCTV video sources • Integrate and assess inputs from different sources such as CCTV, ANPR, RLVD, Speed detection systems, Traffic Violation cameras, Emergency Call Box/Panic Buttons, PA Systems, Video Analytics, and other sensors further to assist with actionable intelligence.

S. No.	Departments/Systems	Minimum Integration Requirements
		• CCTV, Video Analytics, and sensors further to assist with actionable intelligence. • Should use dynamic channel coverage specifically for video stream function for efficient bandwidth usage for multiple Remote Control center • Display module should have capability to control multi-screened display wall in sync with operator console • Should support Fixed type and PTZ camera. Control PTZ function from the screen to control the camera But with changing tile configuration each camera should be viewed with much lower resolution. • The system should dynamically reduce the bit rate and bandwidth for each stream based on the viewing resolution at the remote location. • Integration with GIS map
2)	Public Wi-fi	• ICCC should integrate with Wi-Fi solution and project real time user information on city dashboard • Integration with GIS map
3)	Environmental Monitoring (sensor based/ hosted on Intelligent Pole)	• Monitor key inputs from city environmental sensors like Temperature, Humidity, CO, CO2, NO2, SO2, PM10, PM2.5, • Create awareness within the city based on dynamic inputs received from sensors and display output to various interfaces including city application, multi-services • Integration with GIS map
4)	Smart Governance(ERP) Birth & Death Module, Assets Managemen, Vanue Booking etc.. (for future integration)	• Integrate the portal for displaying birth and death data via APIs • Integrate with master data and other modules for information validity • MIS Reports on Birth/Death information per location/age/gender etc. viz., ▪ Online Birth Certificates printed today ▪ Online Death Certificates printed today ▪ Total Birth Certificates printed ▪ Total Death Certificates printed ▪ Birth Registrations – Today ▪ Birth Registrations – Total ▪ Death Registrations – Today ▪ Death Registrations – Total ▪ Re-print requests per day/month ▪ Verification requests per day/month

S. No.	Departments/Systems	Minimum Integration Requirements
		▪ Pending Certificates issuance ▪ Location/Hospital wise birth/death registrations ▪ Age group wise death registrations ▪ Gender wise birth/death registrations • Analytics on Population vs Birth/Death • KPI's on birth and death certificate issuance by location per location • Integration with GIS map
5)	Smart LED Street Lights (for future integration)	• The ICCC should aggregate various data feeds from light sensors and systems further process information out of these data feeds to provide interface /dashboards for generating alert and notifications in real time. • Provide single dashboard of various brand of lighting solution. • ICCC should support lighting control like diming, switch on/off, group control etc. • ICCC should provide reports of various brand of lighting solution • Integration with GIS map
6)	GPS	• ICCC should integrate with Vehicle tracking • ICCC should Garbage vehicles, C&D Waste, Municipal sweepers, water tankers etc. • Actionable alerts • Summary of distance travelled by each vehicle. • Violations • Integration with GIS map
7)	GIS Based Property Tax (for future integration)	• The Property Tax module should be integrated into ICCC • ICCC uses an ESB or IoT API Adapter for consuming the web services from Property Tax application • ICCC Integration Engine stores auth and other historic data for generating reports • ICCC initially makes call to get the authentication tokens for calling web services • ICCC makes calls to get the required data from Urban Local Bodies (ULB) viz., City Corporation, City Municipal Council, Town Municipal etc., • ICCC expects the following services viz., Property Details per Location, • ICCC displays the analytical information of property tax collections across the in a GIS map

S. No.	Departments/Systems	Minimum Integration Requirements
		▪ All the below services can be integrated into ICCC ▪ Create New Property ▪ Get Property details ▪ Get Property Bill ▪ Make Payment ▪ Get Receipt • Following reports can be displayed on ICCC, if required ▪ Demand / Collection Register ▪ Assessment Register ▪ Ward-wise / Zone-wise Recovery reports ▪ Top Defaulters Report ▪ Occupancy wise / Flat wise report' ▪ Tax-wise Recovery Details ▪ Tax-wise Demand Details ▪ Advance Payment Reports ▪ Objection / Hearing Details • Integration with GIS map
8)	Mobile App (for future integration)	• Provides unified northbound API to abstract diverse sensors and its attributes by single northbound API to allow interfacing and integration with existing systems. • The platform should be able to normalize the data coming from different devices of same type (i.e. Different lighting sensor from different OEMs, different energy meters from different OEMs etc.) and provide secure access to that data using data API(s) to application developers. • Provides Query-based language to access sensor parameter from sensor cloud • Provides mechanism to translate and map business logic to sensor functionality • Integration with GIS map

Following are the minimum use cases identified for integration for above mentioned integrations. The bidder is expected to propose more use cases based on the global leading practices and project experiences:

S. No.	Departments/ Systems	Relevant ICCC Use Cases	Data Feed Frequency	Dataset Required
1.	Solid Waste	Display type of fleet vehicle (LMC garbage	Batch	Categorized information of

S. No.	Departments/ Systems	Relevant ICCC Use Cases	Data Feed Frequency	Dataset Required
	Management	Collector)		various fleet types available in the city
2.		Receive and Display Surveillance Feed	Real-time	Real-time/Near real-time feed of Surveillance Cameras
3.	Transit Management System	Show position of Buses, vehicles on the route	Batch	Documentation of Bus Routes
4.			Real-time	Real-time/Near real-time location of the Buses
5.	ITMS & City Surveillance	Show location of traffic lights	Batch	Location coordinates of traffic light installations at junctions
6.		Show Status of Traffic Lights	Real-time	Real-time/Near real-time status of traffic lights downtime
7.		Show location of CCTV Cameras	Batch	Location coordinates of CCTV Cameras installations at junctions
8.		Show Status of CCTV Cameras	Real-time	Real-time/Near real-time status of CCTV Cameras downtime
9.		Show location of Enforcement System	Batch	Location coordinates of Enforcement System installations at junctions

S. No.	Departments/ Systems	Relevant ICCC Use Cases	Data Feed Frequency	Dataset Required
10.		Show Status of Enforcement System	Real-time	Real-time/Near real-time status of Enforcement System downtime
11.		Show location of VMD Boards	Batch	Location coordinates of VMD Boards installations at junctions
12.		Show Status of VMD Boards	Real-time	Real-time/Near real-time status of VMD Boards downtime
13.		Forecast Demand	Batch	Energy usage across 5 previous years
14.	Street Lights	Identify location of Street Lights	Batch	Location coordinates of Street Lights
15.		Control Street Lights status	Real-time	Real-time/Near real-time status of street lights functioning
16.		Show Status of Street Lights	Real-time	Real-time/Near real-time status of street lights functioning
17.	Property Tax	Show the Properties on GIS map	Batch	Location geo-fenced coordinates of Properties
18.		Display heat map of tax collections by each ward	Batch	Tax collections data by each ward
19.	E-Governance	Show Population by	Batch	Base Population data based on

S. No.	Departments/ Systems	Relevant ICCC Use Cases	Data Feed Frequency	Dataset Required
		each ward		latest census
20.			Batch	Birth and Death data at a regular frequency
21.		Transmit information to citizens	Real-time	Data/Information that has to be broadcast to citizens
22.		Show status of Grievances by Ward	Batch	Details of Grievances received
23.		Show location of Public Advertisement Boards	Batch	Location coordinates of Public Advertisements
24.		Show Public Advertisements availability status	Batch	Booking status of Public Advertisements
25.		Display heat map of advertisement tax collections by each ward	Batch	Tax collections data by each ward
26.	Disaster Management	Identify Disaster Impact Area on map	Real-time	Coordinates to Geo-fence the Disaster Zone
27.		Respond to Disaster Situation	Real-time	Documented Standard Operating Procedures
28.	Emergency Management	Identify Location of Fire Hydrants	Batch	Location coordinates of Fire Hydrants
29.		Show position of Fleet on the city map	Real-time	Real-time/Near real-time location of the Fleet
30.		Display type of fleet	Batch	Categorized

S. No.	Departments/ Systems	Relevant ICCC Use Cases	Data Feed Frequency	Dataset Required
		vehicle		information of various fleet types available in the city
31.		Respond to Emergency Situation	Real-time	Documented Standard Operating Procedures
32.	Smart Poles	Identify location of Smart Poles	Batch	Location coordinates of Smart Poles
33.		Show Status of Smart Poles – Wi-Fi Hotspots	Real-time	Real-time/Near real-time status of Wi-Fi Hotspots functioning
34.		Show Status of Smart Poles - Panic Button/Emergency Call Box	Real-time	Real-time/Near real-time status of Panic Button/Emergency Call Box functioning
35.		Show Status of Smart Poles - Public Address System	Real-time	Real-time/Near real-time status of PAS functioning
36.		Show Status of Smart Poles - Environmental sensors	Real-time	Real-time/Near real-time status of Environmental Sensors functioning
37.		Show Status of Smart Poles - Smart Billboards	Real-time	Real-time/Near real-time status of Smart Billboards functioning
38.		Show Status of Smart Poles - Surveillance	Real-time	Real-time/Near real-time status of Surveillance Cameras functioning
39.		Show Status of Smart Poles - LED Lights	Real-time	Real-time/Near real-time status of

S. No.	Departments/ Systems	Relevant ICCC Use Cases	Data Feed Frequency	Dataset Required
				LED Lights functioning
40.		Show Status of Smart Poles - Solar Panel	Real-time	Real-time/Near real-time status of Solar Panel functioning
41.		Receive and Display Surveillance Feed	Real-time	Real-time/Near real-time feed of Surveillance Cameras
42.		Receive and Display Environmental Sensor Feed	Real-time	Real-time/Near real-time feed of Environmental Sensors
43.		Broadcast message on PAS	Real-time	Message to be broadcast on PAS
44.		Play music on PAS	Real-time	Music tracks to be played on PAS
45.		Receive and Send messages through Panic Button/Emergency Call Box	Real-time	Not Applicable

7.1.6 Go-Live Preparedness and Go-Live

a. MSI shall prepare and agree with LSCL, the detailed plan for Go-Live (in-line with LSCL's implementation plan as mentioned in RFP).

b. The MSI shall define and agree with LSCL, the criteria for Go-Live.

c. The MSI shall ensure that all the data migration is done from existing systems.

d. MSI shall submit signed-off UAT report (issue closure report) ensuring all issues raised during UAT are being resolved prior to Go-Live.

e. MSI shall ensure that Go –Live criteria as mentioned in User acceptance testing of Project is met and MSI needs to take approval from LSCL team on the same.

f. Go-live of the application shall be done as per the finalized and agreed upon Go-Live plan.

7.1.7 Revenue Generation Phase

a. ICCC along with its elements is a critical project under smart cities, and it is imperative that the ICCC should be made sustainable to ensure its continuity. Keeping this in mind it shall be the responsibility of the MSI to build and implement a revenue generation strategy for smart solutions and ICCC such as data monetization, Information products etc.

b. The MSI will be free to choose the options for revenue strategy, prepare a Business plan, which will include revenue generation models based on the feasibility and viability, continuity strategy and timelines. The Business Plan shall be vetted and approved by the PMC for the SPV.

c. Once approved, the MSI shall prepare the RFP in consultation of PMC for hiring an agency to Generate revenue from various models and deliver it to SPV

d. The RFP shall also be approved by the PMC for SPV and assist in the hiring the agency through bid process management.

e. The MSI is expected to develop a strategy for revenue generation options from the Integrated Command and Control Center and implemented smart solutions such as information product.

f. The MSI is expected to study the various options for revenue generation from the scope and elements defined for smart solutions implemented.

g. The MSI may introduce new innovative products or solutions by which revenue can be generated at it's own cost.

h. The following key options for revenue generation may be explored (as applicable):

- Information Products for public and institutions
- Data Monetization
- Advertisement
- Laid network monetization
- Wi-Fi data
- Data Centre as IaaS, PaaS, SaaS for city startups

7.1.8 Operations and Maintenance

Success of the Project would lie on how professionally and methodically the entire Project is managed once the implementation is completed. From the MSI perspective too this is a critical phase since the quarterly payments are linked to the SLA's in the post implementation phases. MSI thus is required to depute a dedicated team of professionals to manage the Project and ensure adherence to the required SLAs. MSI shall provide operations and maintenance services for the software, hardware and other IT and Non-IT infrastructure installed as part of the project after Go-Live for a period of 5 years. Warranty period of the product supplied under project i.e hardware, software,

IT/Non-IT etc., will be considered after phase wise Go-Live. The scope of work for the Operations & Maintenance Phase can be categorized under 8 service categories.

7.1.8.1 Project Management & Facilities Management Services

The MSI will be required to provide facilities management services to support the LSCL and stakeholder department officials in performing their day-to-day functions related to this system.

MSI is required to depute a dedicated, centralised project management and technical team for the overall project management and interaction with LSCL and stakeholder departments.

7.1.8.2 Provision of the Operational Manpower & Contact Center Manpower to view the various data feeds and call center operations at ICCC

The MSI is required to provide suitable manpower to monitor the data feeds ICCC and support LSCL, Traffic Police and other stakeholder departments for operationalization of smart solutions of the project. The exact role of these personnel and their responsibilities would be defined and monitored by LSCL and respective departmental personnel. MSI shall be required to provide such manpower meeting following requirements:

1. All such manpower shall be minimum graduate pass
2. All such manpower shall be without any criminal background / record.
3. LSCL reserves the right to carry out background check of the personnel proposed on the Project for verification of criminal record, at the beginning of deployment or during deployment.
4. MSI shall have to replace any person, if not found suitable for the job.
5. All the manpower shall have to undergo training from the MSI for at least 15 working days on the working of project. Training should also cover dos & don'ts and will have few sessions from LSCL and Stakeholders/End User Department officers on right approaches for monitoring the feeds & providing feedback to LSCL, Stakeholders/End User Department officers and other associated government agencies.
6. Each person shall have to undergo compulsory 1 day training every month
7. Operational Manpower shall work in 3 shifts, with no person being made to see the data feeds for more than 8 hours at a stretch.

Detail operational guideline document shall be prepared during implementation which shall specify detail responsibilities of these resources and their do's & don'ts.

The Current estimation of the man-power required from the MSI is as follows:

#	Description	Quantity
1.	Contact Centre Manpower for operationalization of the systems (12 resources in normal working shift & 4 resources each in two shifts)	20

The remaining operational manpower and supervisors required for operationalization of the project will be provided by LSCL, as per requirements.

7.1.8.3 Basic Infrastructure Services

Following services shall be provided by the MSI under the basic infrastructure services:

1. Ensure availability of the infrastructure (both physical and IT) including but not limited to Power, Cooling, Racks, Storage and other peripheral equipment installed at the time of Project commissioning as per the SLAs.
2. Ensure scalability in terms of availability of racks and supporting infrastructure.
3. Proactive and reactive maintenance, repair and replacement of defective components (physical and other peripheral IT infrastructure) installed for the Project through this RFP. The cost for repair and replacement shall be borne by the MSI.
4. Any component (Physical & IT installed at the time of Project commissioning) that is reported to be faulty / non-functional on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame agreed upon in the Service Level Agreement (SLA).
5. Proactive monitoring of the entire basic infrastructure installed.
6. MSI shall maintain records of the maintenance of the basic infrastructure and shall maintain a logbook on-site that may be inspected by the LSCL, Police department and other stakeholder departments/end users at any time.

7.1.8.4 Network Monitoring Services

The activities shall include:

1. MSI shall provide services for management of ICCC Project to maintain performance at optimum levels on a 24 x 7 basis.
2. MSI shall monitor and administer the network.
3. MSI shall create and modify VLAN, assignment of ports to appropriate applications and segmentation of traffic.
4. MSI shall carry out break fix maintenance of the LAN cabling or maintenance work requiring civil work.

7.1.8.5 Integration Testing

This shall be a black-box testing role primarily to ensure that the application to be deployed does not disrupt the Ludhiana operations and affect other Ludhiana infrastructure in terms of performance and security. The technical tasks to be carried out shall be as follows:

1. Functional Testing: Ensuring that the application functionality as described by the LSCL, Police department and other stakeholder departments/end users. The functional testing of application will necessarily be minimal as this is a core responsibility of the Supplier.

2. Performance Testing: Ensuring that the application meets expressed performance requirements on the Ludhiana servers by using performance test tools and performance monitoring tools.
3. Security Testing: Testing for exploitable application security weaknesses that undermine the application security or the security of the infrastructure.

7.1.8.6 Vendor Management Services

The activities shall include:

1. Coordination with all the project stakeholders to ensure that all Ludhiana activities are carried out in a timely manner.
2. MSI shall coordinate and follow-up with all the relevant vendors to ensure that the issues are resolved in accordance with the SLAs agreed upon with them.
3. MSI shall also ensure that unresolved issues are escalated to respective departments.
4. MSI shall maintain database of the various vendors with details like contact person, telephone nos., escalation matrix, response time and resolution time commitments etc.
5. MSI shall draw a consolidated quarterly SLA performance report across vendors for consideration of the LSCL, Police department and other stakeholder departments/end users.

7.1.8.7 Network Management

The objective of this service is to ensure continuous operation and upkeep of the Network infrastructure of the project including all active and passive components. The selected MSI shall be responsible to coordinate with Network Service Provider for network related issues between ICCC, DC, DR and other sub systems. The services to be provided for Network Management include:

1. Ensuring that the network is available 24x7x365 as per the prescribed SLAs for the 6 years of operations
2. Attending to and resolving network failures and snags.
3. Support and maintain the overall network infrastructure including but not limited to LAN passive components, routers, switches etc.
4. Configuration and backup of network devices including documentation of all configurations.
5. 24x7x365 monitoring of the network to spot the problems immediately.
6. Provide information on performance of Ethernet segments, including capacity utilization and error statistics for the segment and the top-contributing hosts, WAN links and routers.
7. Ensuring timely information to the LSCL, Police department and other stakeholder departments/end users pertaining to issues of Network Backbone

7.1.8.8 Physical Infrastructure Management and Maintenance Services

All the devices that will be installed in the Project as part of the physical infrastructure should be SNMP enabled and shall be centrally and remotely monitored and managed on a 24x7x365 basis. Industry leading infrastructure management solution should be deployed to facilitate monitoring and management of the Infrastructure on one integrated console. The physical infrastructure management and maintenance services shall include:

1. Proactive and reactive maintenance, repair and replacement of defective components (IT and Non-IT/ Hardware and Software). The cost for repair and replacement shall be borne by the MSI.
2. The MSI shall have to stock and provide adequate onsite and offsite spare parts and spare component to ensure that the uptime commitment as per SLA is met. To provide this service it is important for the MSI to have back to back arrangement with the OEMs. The MSI needs to provide a copy of the service level agreement signed with the respective OEMs.
3. Component that is reported to be down on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame indicated in the Service Level Agreement (SLA). In case the selected MSI fails to meet the above standards of maintenance, there will be a penalty as specified in the SLA.
4. The selected MSI shall also maintain records of all maintenance of the system and shall maintain a logbook on-site that may be inspected by the LSCL, Police department and other stakeholder departments/end users at any time.

7.1.9 Exit Management

a. This sets out the provisions, which will apply on expiry or termination of the Master Service Agreement, the Project Implementation, Operation and Management SLA.

b. In the case of termination of the Project Implementation and/or Operation and Management, the Parties shall agree at that time whether, and if so during what period, the provisions of this Schedule shall apply.

c. The Parties shall ensure that their respective associated entities carry out their respective obligations set out in this Exit Management Schedule.

7.1.9.1 Cooperation and Provision of Information

During the exit management period:

a. The MSI will allow the LSCL or its nominated agency access to information reasonably required to define the current mode of operation associated with the provision of the services to enable the LSCL to assess the existing services being delivered;

b. Promptly on reasonable request by the LSCL, the MSI shall provide access to and copies of all information held or controlled by them which they have prepared or maintained in accordance with this agreement relating to any material aspect of the services (whether provided by the MSI or sub-contractors appointed by the MSI). The LSCL shall be entitled to

copy of all such information. Such information shall include details pertaining to the services rendered and other performance data. The MSI shall permit the LSCL or its nominated agencies to have reasonable access to its employees and facilities, to understand the methods of delivery of the services employed by the MSI and to assist appropriate knowledge transfer.

7.1.9.2 Confidential Information, Security and Data

a. The MSI will promptly on the commencement of the exit management period supply to the LSCL or its nominated agency the following:

- information relating to the current services rendered and customer and performance data relating to the performance of sub-contractors in relation to the services;
- documentation relating to Intellectual Property Rights;
- documentation relating to sub-contractors;
- all current and updated data as is reasonably required for purposes of LSCL or its nominated agencies transitioning the services to its Replacement MSI in a readily available format nominated by the LSCL, its nominated agency;
- all other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable LSCL or its nominated agencies, or its Replacement MSI to carry out due diligence in order to transition the provision of the Services to LSCL or its nominated agencies, or its Replacement MSI (as the case may be).

b. Before the expiry of the exit management period, the MSI shall deliver to the LSCL or its nominated agency all new or up-dated materials from the categories set out in Schedule above and shall not retain any copies thereof, except that the MSI shall be permitted to retain one copy of such materials for archival purposes only.

7.1.9.3 Transfer of Certain Agreements

On request by the LSCL or its nominated agency the MSI shall effect such assignments, transfers, licences and sub-licences LSCL, or its Replacement MSI in relation to any equipment lease, maintenance or service provision agreement between MSI and third party lessors, vendors, and which are related to the services and reasonably necessary for the carrying out of replacement services by the LSCL or its nominated agency or its Replacement MSI.

7.1.9.4 General Obligations of the MSI

a. The MSI shall provide all such information as may reasonably be necessary to effect as seamless handover as practicable in the circumstances to the LSCL or its nominated agency or its Replacement MSI and which the MSI has in its possession or control at any time during the exit management period.

b. For the purposes of this Schedule, anything in the possession or control of any MSI, associated entity, or sub-contractor is deemed to be in the possession or control of the MSI.

c. The MSI shall commit adequate resources to comply with its obligations under this Exit Management Schedule.

7.1.9.5 Exit Management Plan

a. The MSI shall provide the LSCL or its nominated agency with a recommended exit management plan ("Exit Management Plan") which shall deal with at least the following aspects of exit management in relation to the MSA as a whole and in relation to the Project Implementation, and the Operation and Management SLA.

- A detailed program of the transfer process that could be used in conjunction with a Replacement MSI including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer;
- plans for the communication with such of the MSI's sub-contractors, staff, suppliers, customers and any related third party as are necessary to avoid any material detrimental impact on the LSCL's operations as a result of undertaking the transfer;
- (if applicable) proposed arrangements for the segregation of the MSI's networks from the networks employed by LSCL and identification of specific security tasks necessary at termination;
- Plans for provision of contingent support to LSCL, and Replacement MSI for a reasonable period after transfer.

b. The MSI shall re-draft the Exit Management Plan annually thereafter to ensure that it is kept relevant and up to date.

c. Each Exit Management Plan shall be presented by the MSI to and approved by the LSCL or its nominated agencies.

d. The terms of payment as stated in the Terms of Payment Schedule include the costs of the MSI complying with its obligations under this Schedule.

e. In the event of termination or expiry of MSA, and Project Implementation, each Party shall comply with the Exit Management Plan.

f. During the exit management period, the MSI shall use its best efforts to deliver the services.

g. Payments during the Exit Management period shall be made in accordance with the Terms of Payment Schedule.

h. This Exit Management plan shall be furnished in writing to the LSCL or its nominated agencies within 90 days from the Effective Date of this Agreement.

7.1.10 Compliance to Standards & Certifications

a. For a large and complex set up such as the Project, it is imperative that the highest standards applicable are adhered to. In this context, the MSI will ensure that the entire Project is developed in compliance with the applicable standards.

b. During project duration, the MSI will ensure adherence to prescribed standards as provided below:

Sl. No.	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

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

- The Information Technology Act, 2000" and amendments thereof and
- Guidelines and advisories for information security published by Cert-In/DeitY (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.

d. 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:

- The name of the module
- The date when module was created
- A description of what the module does
- A list of the calling arguments, their types, and brief explanations of what they do
- A list of required files and/or database tables needed by the module
- Error codes/Exceptions
- Operating System (OS) specific assumptions
- A list of locally defined variables, their types, and how they are used
- Modification history indicating who made modifications, when the modifications were made, and what was done.

e. 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 -

- Proper and consistent indentation
- Inline comments

- Structured programming
- Meaningful variable names
- Appropriate spacing
- Declaration of variable names
- Meaningful error messages

f. Quality Audits

- LSCL, at its discretion, may also engage independent auditors to audit any/some/all standards/processes. The MSI shall support all such audits as per calendar agreed in advance. The result of the audit shall be shared with the MSI who has to provide an effective action plan for mitigations of observations/non-compliances, if any.

7.1.11 Project Management and Governance

7.1.11.1 Project Management Office (PMO)

A Project Management office will be set up during the start of the project. The PMO will, at the minimum, include a designated full time Project Manager from MSI. It will also include key persons from other relevant stakeholders including members of LSCL and other officials/representatives by invitation. The operational aspects of the PMO need to be handled by the MSI including maintaining weekly status, minutes of the meetings, weekly/monthly/project plans, etc.

PMO will meet formally on a weekly basis covering, at a minimum, the following agenda items:

i. Project Progress
ii. Delays, if any – Reasons thereof and ways to make-up lost time
iii. Issues and concerns
iv. Performance and SLA compliance reports;
v. Unresolved and escalated issues;
vi. Project risks and their proposed mitigation plan
vii. Discussion on submitted deliverable
viii. Timelines and anticipated delay in deliverable if any
ix. Any other issues that either party wishes to add to the agenda.

During the development and implementation phase, there may be a need for more frequent meetings and the agenda would also include:

i. Module development status
ii. Testing results
iii. IT infrastructure procurement and deployment status

iv. Status of setting up/procuring of the Helpdesk, DC hosting

v. Any other issues that either party wishes to add to the agenda.

Bidder shall recommend PMO structure for the project implementation phase and operations and maintenance phase.

7.1.11.2 Helpdesk and Facilities Management Services

The MSI shall be required to establish the helpdesk and provide facilities management services to support the LSCL and stakeholder department officials in performing their day-to-day functions related to this system.

The MSI shall setup a central helpdesk dedicated (i.e. on premise) for the Project, which shall be supported by individual smart city command centres, implemented and proposed to be setup under Ludhiana Smart City Programme. This helpdesk would be operational upon implementation of the Project. Providing helpdesk/support services from a shared facility of any other party/provider is not permitted.

Functional requirements of the helpdesk management system, fully integrated with the enterprise monitoring and network management system. The system will be accessed by the stakeholder department officials for raising their incidents and logging calls for support. The detailed service levels and response time, which the MSI is required to maintain for provisioning of the FMS services are described in the Service Level Agreement of this Tender.

MSI shall deploy Manpower during implementation and O&M phases. The deployed resource shall report to LSCL's Project In-charge for Smart City Project and work closely with Program Management Office of the project. Following are the minimum resources required to be deployed in the Project, however MSI may deploy additional resources based on the need of the Project and to meet the defined SLAs in this RFP:

#	Type of Resource	Minimum Quantity	Minimum Deployment during Operation and Maintenance phase
1.	Project Manager	1	100% (8*5)
2.	Solution Architect	1	Onsite Support to Project team on need basis
3.	Integrated Traffic Management Expert	1	100% (24*7)
4.	Network & Security – Infrastructure Expert	1	100% (24*7)
5.	Server and Storage Expert	1	100% (24*7)
6.	Technical Expert-GIS	1	100% (24*7)
7.	Technical Expert-ICCC	1	100% (24*7)

#	Type of Resource	Minimum Quantity	Minimum Deployment during Operation and Maintenance phase
8.	Command Center Operators	24	100% (24*7 – 16 resources in normal shift & 4 resource each in two shifts)

Note:

1. Numbers provided for staff providing 24*7 support is excluding relievers.
2. Qualification of the operator shall also be submitted even if not evaluated for the bids.

7.1.11.3 Steering Committee

The Steering Committee will consist of senior stakeholders from LSCL, its nominated agencies and MSI. MSI will nominate its Smart City vertical head to be a part of the Project Steering Committee

The MSI shall participate in monthly Steering Committee meetings and update Steering Committee on Project progress, Risk parameters (if any), Resource deployment and plan, immediate tasks, and any obstacles in project. The Steering committee meeting will be a forum for seeking and getting approval for project decisions on major changes etc.

All relevant records of proceedings of Steering Committee should be maintained, updated, tracked and shared with the Steering Committee and Project Management Office by MSI.

During the development and implementation phase of the project, it is expected that there will be at least fortnightly Steering Committee meetings. During the O&M phase, the meetings will be held at least once a quarter.

Other than the planned meetings, in exceptional cases, LSCL may call for a Steering Committee meeting with prior notice to the MSI.

7.1.11.4 Project Monitoring and Reporting

The MSI shall circulate written progress reports at agreed intervals to LSCL and other stakeholders. Project status report shall include Progress against the Project Management Plan, status of all risks and issues, exceptions and issues along with recommended resolution etc.

Other than the planned meetings, in exceptional cases, project status meeting may be called with prior notice to the Bidder. LSCL reserves the right to ask the bidder for the project review reports other than the standard weekly review reports.

7.1.11.5 Risk and Issue management

The MSI shall develop a Risk Management Plan and shall identify, analyse and evaluate the project risks, and shall develop cost effective strategies and action plans to mitigate those risks.

The MSI shall carry out a Risk Assessment and document the Risk profile of LSCL based on the risk appetite and shall prepare and share the LSCL Enterprise Risk Register. The MSI shall develop an issues management procedure to identify, track, and resolve all issues confronting the project. The risk management plan and issue management procedure shall be done in consultation with LSCL.

The MSI shall monitor, report, and update the project risk profile. The risks should be discussed with LSCL and a mitigation plan be identified during the project review/status meetings. The Risk

and Issue management should form an agenda for the Project Steering Committee meetings as and when required.

7.1.11.6 Governance procedures

MSI shall document the agreed structures in a procedures manual.

7.1.11.7 Planning and Scheduling

The MSI will prepare a detailed schedule and plan for the entire project covering all tasks and sub tasks required for successful execution of the project. The MSI has to get the plan approved from LSCL at the start of the project and it should be updated every week to ensure tracking of the progress of the project.

The project plan should include the following:

1. The project break up into logical phases and sub-phases;
2. Activities making up the sub-phases and phases;
3. Components in each phase with milestones;
4. The milestone dates are decided by LSCL in this RFP. MSI cannot change any of the milestone completion dates. MSI can only propose the internal task deadlines while keeping the overall end dates the same. MSI may suggest improvement in project dates without changing the end dates of each activity.
5. Key milestones and deliverables along with their dates including those related to delivery and installation of hardware and software;
6. Start date and end date for each activity;
7. The dependencies among activities;
8. Resources to be assigned to each activity;
9. Dependency on LSCL

7.1.11.8 License Metering / Management

The MSI shall track software usage throughout the IT setup so as to effectively manage the risk of unauthorized usage or under-licensing of software installed at the ICCC. This may be carried out through the use of standard license metering tools.

7.1.12 Change Management & Control

7.1.12.1 Change Orders / Alterations / Variations

a. The MSI agrees that the requirements given in the Bidding Documents are minimum requirements and are only indicative. The MSI would need to fetch out the details at the time of preparing the design document prior to actual implementation. It shall be the responsibility of the MSI to meet all the requirements of technical specifications contained in the RFP and any upward revisions and/or additions of quantities, specifications sizes given in the Bidding Documents required to be made during execution of the works, shall

not constitute a change order and shall be carried out without a change order and shall be carried out without any time and cost effect to Purchaser.

b. Further upward revisions and or additions required to make MSI's selected equipment and installation procedures to meet Bidding Documents requirements expressed and to make entire facilities safe, operable and as per specified codes and standards shall not constitute a change order and shall be carried out without any time and cost effect to Purchaser.

c. Any upward revision and/or additions consequent to errors, omissions, ambiguities, discrepancies in the Bidding Documents which the MSI had not brought out to the Purchaser's notice in his bid shall not constitute a change order and such upward revisions and/or addition shall be carried out by MSI without any time and cost effect to Purchaser.

7.1.12.2 Change Order

a. The Change Order will be initiated only in case (i) the Purchaser directs in writing the MSI to include any addition to the scope of work covered under this Contract or delete any part of the scope of the work under the Contract, (ii) MSI requests to delete any part of the work which will not adversely affect the operational capabilities of the facilities and if the deletions proposed are agreed to by the Purchaser and for which cost and time benefits shall be passed on to the Purchaser, (iii) the Purchaser directs in writing the MSI to incorporate changes or additions to the technical specifications already covered in the Contract.

b. Any changes required by the Purchaser over and above the minimum requirements given in the specifications and drawings etc. included in the Bidding Documents before giving its approval to detailed design or Engineering requirements for complying with technical specifications and changes required to ensure systems compatibility and reliability for safe operation (As per codes, standards and recommended practices referred in the Bidding Documents) and trouble free operation shall not be construed to be change in the Scope of work under the Contract.

c. Any change order as stated in Clause 2 a. comprising an alteration which involves change in the cost of the works (which sort of alteration is hereinafter called a "Variation") shall be the Subject of an amendment to the Contract by way of an increase or decrease in the schedule of Contract Prices and adjustment of the implementation schedule if any.

d. If parties agree that the Contract does not contain applicable rates or that the said rates are inappropriate or the said rates are not precisely applicable to the variation in question, then the parties shall negotiate a revision of the Contract Price which shall represent the change in cost of the works caused by the Variations. Any change order shall be duly approved by the Purchaser in writing.

e. Within ten (10) working days of receiving the comments from the Purchaser or the drawings, specification, purchase requisitions and other documents submitted by the MSI for approval, the MSI shall respond in writing, which item(s) of the Comments is/are

potential changes(s) in the Scope of work of the RFP document covered in the Contract and shall advise a date by which change order (if applicable) will be submitted to the Purchaser.

7.1.13 Testing and Acceptance Criteria

a. MSI shall demonstrate the following mentioned acceptance criteria prior to acceptance of the solution as well as during project operations phase, in respect of scalability and performance etc. The MSI may propose further detailed Acceptance criteria which the LSCL will review. Once LSCL provides its approval, the Acceptance criteria can be finalized. In case required, parameters might be revised by LSCL in mutual agreement with bidder and the revised parameters shall be considered for acceptance criteria. A comprehensive system should be set up that would have the capability to log & track the testing results, upload & maintain the test cases and log & track issues/bugs identified.

b. The following table depicts the details for the various kinds of testing envisaged for the project:

Type of Testing	Responsibility	Scope of Work
System Testing	MSI	1. MSI to perform System testing 2. MSI to prepare test plan and test cases and maintain it. LSCL may request the MSI to share the test cases and results 3. Should be performed through manual as well as automated methods 4. Automation testing tools to be provided by MSI. LSCL doesn't intend to own these tools
Integration Testing	MSI	1. MSI to perform Integration testing 2. MSI to prepare and share with LSCL the Integration test plans and test cases 3. MSI to perform Integration testing as per the approved plan 4. Integration testing to be performed through manual as well as automated methods 5. Automation testing tools to be provided by MSI. LSCL doesn't intend to own these tools
Performance and load Testing	• MSI • LSCL / Third Party Auditor (to monitor the performance testing)	1. MSI to do performance and load testing. 2. Various performance parameters such as transaction response time, throughput, page loading time should be taken into account. 3. Load and stress testing of the Project to be performed on business transaction volume 4. Test cases and test results to be shared with LSCL. 5. Performance testing to be carried out in the exact same architecture that would be set up for

Type of Testing	Responsibility	Scope of Work
		production. 6. MSI need to use performance and load testing tool for testing. LSCL doesn't intend to own these tools. LSCL if required, could involve third party auditors to monitor/validate the performance testing. Cost for such audits to be paid by LSCL.
Security Testing (including Penetration and Vulnerability testing)	• MSI • LSCL / Third Party Auditor (to monitor the security testing)	1. The solution should demonstrate the compliance with security requirements as mentioned in the RFP including but not limited to security controls in the application, at the network layer, network, data centre(s), security monitoring system deployed by the MSI 2. The solution shall pass vulnerability and penetration testing for rollout of each phase. The solution should pass web application security testing for the portal, mobile app and other systems and security configuration review of the infrastructure. 3. MSI should carry out security and vulnerability testing on the developed solution. 4. Security testing to be carried out in the exact same environment/architecture that would be set up for production. 5. Security test report and test cases should be shared with LSCL 6. Testing tools if required, to be provided by MSI. LSCL doesn't intend to own these tools 7. During O&M phase, penetration testing to be conducted on yearly basis and vulnerability assessment to be conducted on half-yearly basis. 8. LSCL will also involve third party auditors to perform the audit/review/monitor the security testing carried out by MSI. Cost for such auditors to be paid by LSCL.
User Acceptance Testing of Project	• LSCL or LSCL appointed third party auditor	1. LSCL / LSCL appointed third party auditor to perform User Acceptance Testing 2. MSI to prepare User Acceptance Testing test cases 3. UAT to be carried out in the exact same environment/architecture that would be set up for production 4. MSI should fix bugs and issues raised during UAT

Type of Testing	Responsibility	Scope of Work
		and get approval on the fixes from LSCL / third party auditor before production deployment 5. Changes in the application as an outcome of UAT shall not be considered as Change Request. MSI has to rectify the observations.

Note:

a. Bidder needs to provide the details of the testing strategy and approach including details of intended tools/environment to be used by MSI for testing in its technical proposal. LSCL does not intend to own the tools.

b. The MSI shall work in a manner to satisfy all the testing requirements and adhere to the testing strategy outlined. The MSI must ensure deployment of necessary resources and tools during the testing phases. The MSI shall perform the testing of the solution based on the approved test plan, document the results and shall fix the bugs found during the testing. It is the responsibility of MSI to ensure that the end product delivered by the MSI meets all the requirements specified in the RFP. The MSI shall take remedial action based on outcome of the tests.

c. The MSI shall arrange for environments and tools for testing and for training as envisaged. Post Go-Live; the production environment should not be used for testing and training purpose. If any production data is used for testing, it should be masked and it should be protected. Detailed process in this regard including security requirement should be provided by the MSI in its technical proposal. The process will be finalized with the selected bidder.

d. All the Third Party Auditors (TPA) as mentioned above will be appointed and paid by LSCL directly. All tools/environment required for testing shall be provided by the MSI.

e. STQC/Other agencies appointed by LSCL shall perform the role of TPA. MSI needs to engage with the TPA at the requirement formulation stage itself. This is important so that unnecessary re-work is avoided and the audit is completed in time. The audit needs to be completed before Go-Live of different phases. MSI needs to prepare and provide all requisite information/documents to third party auditor and ensure that there is no delay in overall schedule.

f. The cost of rectification of non-compliances shall be borne by the MSI.

7.1.13.1 Factory Testing

Success MSI shall have to submit Factory Test Certificate for the below mentioned materials before the actual supply of the items.

1. Cable
2. Pole
3. Signal Aspects

Authorized representative from LSCL will visit the manufacturing plant of the product subject to present in India. Authorized representative will check the testing process.

7.1.13.2 Final Acceptance Testing

The final acceptance shall cover 100% of the I Project, after successful testing by the LSCL, Police Department, other stakeholders/end user department or its PMU; a Final Acceptance Test Certificate (FAT) shall be issued by the LSCL to the MSI.

Prerequisite for Carrying out FAT activity:

1. Detailed test plan shall be developed by the MSI and approved by LSCL. This shall be submitted by MSI before FAT activity to be carried out.
2. All documentation related to ICCC Project and relevant acceptance test document (including IT Components, Non IT Components etc.) should be completed & submitted before the final acceptance test to the LSCL.
3. The training requirements as mentioned should be completed before the final acceptance test.
4. Successful hosting of Application, NMS and MIS Software.
5. For both IT & Non-IT equipment's / software manuals / brochures / Data Sheets / CD / DVD / media for all the Ludhiana Project supplied components.

The FAT shall include the following:

1. All hardware and software items must be installed at respective sites as per the specification.
2. Availability of all the defined services shall be verified.
3. The MSI shall be required to demonstrate all the features / facilities / functionalities as mentioned in the RFP.
4. The MSI shall arrange the test equipment required for performance verification, and will also provide documented test results.
5. The MSI shall be responsible for the security audit of the establishes system to be carried out by a certified third party as agreed by LSCL.

Any delay by the MSI in the Final Acceptance Testing shall render him liable to the imposition of appropriate Penalties. However, delays identified beyond the control of MSI shall be considered appropriately and as per mutual agreement between LSCL and MSI. In the event the MSI is not able to complete the installation due to non-availability of bandwidth from the bandwidth service providers, the Supplier and LSCL may mutually agree to redefine the Network so the MSI can complete installation and conduct the Final Acceptance Test within the specified time.

8. Annexure III: Payment Schedule and Milestones

The payment schedule and milestones are divided into four phases:

1. Implementation & Integration Phase-1
2. Integration Phase
3. Operations and Maintenance Phase

LSCL shall issue a "Request Order" in writing, indicating the number of units of Hardware and Software to be supplied along with the location (Project Site). The LSCL shall continue to issue such request until the full quantities of Hardware and Software specified in volume 1 within the variation limits of RFP is exhausted. Upon getting the Request Order, the MSI shall promptly and as soon as possible within the lead time specified in the request order, supply, install and implement specified numbers of hardware and software at stated project site and commissioned the same. LSCL shall specify the Lead Time in Request Order. The Lead Time of Request Order shall be decided in discussion with the Service Provider before the Request Order is placed. LSCL's decision in this regard shall be final but reasonable time shall be provided to the MSI. Delay or non-performance will form the basis for application of Liquidated Damages. Tentative time line is specified below.

Sr. No.	Deliverables	Time Schedule
1	Completion of Scoping and feasibility study (Inception Phase)	D+ 1 Month
2	Installation, Integration, Commissioning and Go-Live of ICCC (Phase I) 1. ICCC - IT hardware 2. ICCC - Non-IT equipment 3. ICCC – software 4. Data Center Cloud – Hardware 5. Data Center Cloud- Software 6. Data Center (DC) – Hardware 7. Data Center (DC) – Software 8. Data Center (DC) – Non-IT equipment 9. DR – Hardware 10. DR – Software 11. DC-DR link 12. Implementation and Integration of City Surveillance System – 300 Cameras 13. Implementation and Integration of 10 Variable Message Display (VMD) Boards at different identified Locations 14. Implementation and integraton of 50 ECB/Panic Button 15. Implementation and integration of 50 Public Address System	D+ 6 Months

Sr. No.	Deliverables	Time Schedule
	16. Implementation and Integration of 10 Environmental Sensors 17. DR Services 18. Integeration with other phase I components such as city surveillance, smart governance, smart LED light, smart traffic and SWM	
3	Integration of Smart elements of Phase II	D + 9 Months

8.1 Milestones and Payment Schedules for Implementation Phase

Based on findings of the site survey activity done by the MSI, the MSI may propose a change in the number of sites or individual units to be deployed in each phase as well as overall scope and a consequent change in phasing. LSCL also retains the right to suo-moto change the number of sites or individual units to be deployed for each scope item. The final decision on change in phasing and related change in payment schedules shall be at the discretion of LSCL.

MSI should complete all the activities within the defined timelines as indicated above. The timeline will be reviewed regularly during implementation phase and may be extended incase LSCL feels that extension in a particular Request Order/Integration or any track is imperative, for the reason beyond the control of the bidder. In all such cases LSCL's decision shall be final and binding. The MSI will be eligible for the payment based on the completion of activities and approval of the relevant deliverables.

D = Effective Date of Contract Agreement

D1= Date of Issue of Request Order 1

Milestones	Payment Milestones for the Implementation % Payment of Time Schedule Phase	Payment Schedule	Time Schedule	Deliverable
M1	Project Kickoff	Value commensurate to the discovered quote for site survey activity as per commercial format	D	NA
M2	Request Order – Site Survey of Locations	10% of Request Order Value (Capex Cost) post issuance of Request	D1 + 1 Month	1. Inception Report 2. Project Plan 3. Risk Management and

Milestones	Payment Milestones for the Implementation % Payment of Time Schedule Phase	Payment Schedule	Time Schedule	Deliverable
		Order		Mitigation Plan 4. Site Survey report 5. Final BoQ 6. Project tracebility matrix
M3	Requirement Phase Completion Design Phase Completion	10% of Request Order Value (Capex Cost)	D1 + 2 Month	1. Functional Requirement Specification document 2. System Requirement Specification document 3.System Architecture document 4.Test strategy 5. Updated Traceability Matrix
M4	Request Order – Delivery and Receipt of Hardware and Software at site and after Verification of such items by LSCL/LSCL authorized agency	13% of Request Order Value (Capex Cost)	D1 + 3 Months	1. HLD documents 2. LLD documents 3. Application architecture documents. 4. Technical Architecture documents. 5. Network Architecture documents. 6. Interface specification (for all the integeration modules) 7. GUI design (screen design, navigation, etc.). 8. Test Plans 9. Security Plan 10. Training Plan 11. SoPs and KPIs 12. Change management Plan

Milestones	Payment Milestones for the Implementation % Payment of Time Schedule Phase	Payment Schedule	Time Schedule	Deliverable
				13. Updated tracebility matrix
M5	Power-up (for hardware), Installation, configuration and Application deployment	13% of Request Order Value (Capex Cost)	D1 + 4 Months	1. IT and Non IT Infrastructure Installation Report 2. Integration testing report 3. Training Completion report 4. Application deployment and configuration report 5. Updated tracebility matrix
M6	Installation, integration, Commissioning and Go-Live of ICCC (Phase I)	15% of Request Order Value (Capex Cost)	D1 + 6 Months	1. Completion of UAT and closure of observations report 2. Go-Live Report 3. Updated tracebility matrix
M7	Integration of smart element of Phase II	15% of Request Order Value (Capex Cost)	D1 + 9 Months	1. Integration Testing Report 2. Updated tracebility matrix
The remaining part of the 24% of the Project Cost shall be paid a rate of 1.5% per Quarter. The Payment shall be made along with the Opex Invoice per Quarter during the O&M Period.				

Note:

- All payments to the Master Systems Integrator (MSI) shall be made upon submission of invoices along with necessary approval certificates from concerned Authorities.
- The above payments are subject to meeting of SLA's failing which the appropriate deductions as mentioned in the SLA document of this RFP.
- Payment for Integration with Individual sub system can be released after 3 months of given timeline of each phase in case of the any of the sub systems of that phase is not ready

8.2 Milestones and Payment Schedules for Operations and Maintenance Phase

The Operations and maintenance phase will start as soon as Go-Live for the each phase occurs. The MSI will be required to adhere to the SLA and provide post implementations support of warranty and O&M for a period of 4 years after implementation/Phase wise Go-Live.

Milestones	Payment Milestones for the Implementation % Payment of Time Schedule Phase	Payment Schedule	Time Schedule
M5	Year 1 payment for O&M after Go-Live	Equal Quarterly O&M Payments	Payment of Year 1
M6	Year 2 payment for O&M after Go-Live	Equal Quarterly O&M Payments	Payment of Year 2
M7	Year 3 payment for O&M after Go-Live	Equal Quarterly O&M Payments	Payment of Year 3
M8	Year 4 payment for O&M after Go-Live	Equal Quarterly O&M Payments	Payment of Year 4

Payment of Operations and maintenance phase will be made on quarterly basis (at completion of each quarter) based on the adherence to SLA, for the amount quoted for each respective year.

9. Annexure IV- Common guidelines regarding compliance of systems/equipment

1. The specifications mentioned for various IT / Non-IT components are indicative requirements and should be treated for benchmarking purpose only. MSIs are required to undertake their own requirement analysis and may propose higher specifications that are better suited to the requirements.
2. Any manufacturer and product name mentioned in the Tender should not be treated as a recommendation of the manufacturer / product.
3. All IT Components should support IPv4 and IPv6
4. All IT/Electronics components shall be in compliance to the IEC/ISI/BSI standards as applicable
5. All systems will be designed to ensure accessibility to the disabled hence all the components related to IT, electronics and/or digital technology should be in accordance to the latest version of WCAG and the European Standards - EN 301 549 or an equivalent standard as approved
6. MSI should adhere with the open standard oneM2M wherever applicable during solution design and implementation
7. The specifications provided in this RFP are indicative and carry guiding rule. The MSI is free to offer products and solutions which meet requirements of the RFP focussing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards & best practices adopted in the industry. The MSI is encouraged to design an Optimised solution which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical requirement in the RFP may be considered if it is required for meeting current & future requirements during the contract period. Necessary justification should be given in Technical solution accordingly.The MSI is fully responsible for the specified outcome to be achieved.
8. Technical Bid should be accompanied by OEM's product brochure / datasheet. Bidders should provide complete make, model, for all equipment/software quoted, in the Technical Bid.
9. Bidder should ensure that only one make and model is proposed for one component in Technical Bid for example all PTZ cameras must belong to a single OEM and must be of the same model etc.
10. Bidders should ensure warranty and support for all equipment from OEMs during the contract period. All the back-to-back service agreements should be submitted along with the Technical Bid.
11. All equipment, parts should be original and new.
12. The user interface of the system should be a user friendly Graphical User Interface (GUI).

13. Critical core components of the system should not have any requirements to have proprietary platforms and should conform to open standards.

14. For custom made modules, industry standards and norms should be adhered to for coding during application development to make debugging and maintenance easier. Object oriented programming methodology must be followed to facilitate sharing, componentizing and multiple-use of standard code. Before hosting the application, it shall be subjected to application security audit (by any of the CERTIN empanelled vendors) to ensure that the application is free from any vulnerability; and approved by the LSCL.

15. All the Clients Machines / Servers shall support static assigned IP addresses or shall obtain IP addresses from a DNS/DHCP server.

16. The indicative architecture of the system is given in this volume. The Successful Bidder must provide the architecture of the solution it is proposing.

17. The system servers and software applications will be hosted in Data Centers as specified in the Bid. It is important that the entire set of Data Center equipment are in safe custody and have access from only the authorized personnel and should be in line with the requirements & SLAs defined in the RFP .

18. The Servers provided should meet industry standard performance parameters (such as CPU Utilisation of 60 percent or less, disk utilisation of 75 percent or less). In case any non-standard computing environment is proposed (such as cloud), detail clarification needs to be provided in form of supporting documents, to confirm (a) how the sizing has been arrived at and (b) how SLAs would be met.

19. MSI is required to ensure that there is no choking point / bottleneck anywhere in the system (end-to-end) and enforce performance and adherence to SLAs. SLA reports must be submitted as specified in the Bid without fail.

20. All the hardware and software supplied should be from the reputed Original Equipment Manufacturers (OEMs). LSCL/or any other authorized agency as nominated by the Authority reserves the right to ask replacement of any hardware / software if it is not from a reputed brand and conforms to all the requirements specified in the RFP documents.

21. Cameras and the Video Management / Video Analytics Software should be ONVIF Core Specification '2.X' or 'S', 'G' compliant and provide support for ONVIF profiles such as Streaming, Storage, Recording, Playback, retrieval of local stored video and Access Control.

22. **ICCC hence established by MSI shall have provision to display of feed / analytics for the temporarily installed cameras. The number of cameras cannot be anticipated now.**

23. System Integrator shall place orders on various OEMs directly and not through any sub-contractor / partner.

24. All licenses should be in the name of the Ludhiana Smart City Limited (LSCL).

NOTE: For all supply equipment's, registered service/support center of the respective OEM should be existing or established in India within 30 days of award of contract. The Bidder should submit an undertaking from the OEM to that effect.

10. Annexure V - Status of the Systems to be integrated in ICCC in Ludhiana City

S.No.	ICT Systems	Status of current Automation	Future Roadmap
1	Smart Lighting	No	Yes
3	Integrated Traffic Management System (ITMS)	No	Yes
4	Environment Sensors	No	Yes
5	City Surveillance	Partial	Yes
6	Smart Governance	No	Yes
7	Smart Parking/ MLCP	No	Yes
10	GIS	No	Yes
13	Transit Management System for City Buses	No	Yes

11. Annexure VI – Smart City Guidelines for ensuring Universal Access IT Systems to empower citizens with disability to access ICT systems with ease

Sl. No.	Parameters	Minimum Requirements
1	Text Alternatives	Provide text alternatives for any non-text content so that it can be changed into other forms people need, such as large print, braille, speech, symbols or simpler language.
2	Non-text Content	All images, form image buttons, and image map hot spots have appropriate, equivalent alternative text. Images that do not convey content, are decorative, or contain content that is already conveyed in text are given null alt text (alt="") or implemented as CSS backgrounds. All linked images have descriptive alternative text. Equivalent alternatives to complex images are provided in context or on a separate (linked and/or referenced via longdesc) page.
3	Time-based Media	Provide alternatives for time-based media.
4	Audio Description or Media Alternative (Prerecorded)	A descriptive text transcript OR audio description audio track is provided for non-live, web-based video
5	Adaptable	Create content that can be presented in different ways (for example simpler layout) without losing information or structure.
6	Info and Relationships	Semantic markup is used to designate headings (<h1>), lists (, , and <dl>), emphasized or special text (, <code>, <abbr>, <blockquote>, for example), etc. Semantic markup is used appropriately. Tables are used for tabular data. Where necessary, data cells are associated with their headers. Data table captions and summaries are used where appropriate. Text labels are associated with form input elements. Related form elements are grouped with fieldset/legend.
7	Meaningful Sequence	The reading and navigation order (determined by code order) is logical and intuitive.
8	Use of Color	Color is not used as the sole method of conveying content or distinguishing visual elements. Color alone is not used to distinguish links from surrounding text unless the luminance contrast between the link and the surrounding text is at least 3:1 and an additional differentiation (e.g., it becomes underlined) is provided when the link is hovered over or receives focus.

9	Audio Control	A mechanism is provided to stop, pause, mute, or adjust volume for audio that automatically plays on a page for more than 3 seconds.
10	Resize text	The page is readable and functional when the text size is doubled.
11	Images of Text	If the same visual presentation can be made using text alone, an image is not used to present that text.
12	Keyboard Accessible	Make all functionality available from a keyboard.
13	Keyboard	All page functionality is available using the keyboard, unless the functionality cannot be accomplished in any known way using a keyboard (e.g., free hand drawing). Page-specified shortcut keys and accesskeys (accesskey should typically be avoided) do not conflict with existing browser and screen reader shortcuts.
14	No Keyboard Trap	Keyboard focus is never locked or trapped at one particular page element. The user can navigate to and from all navigable page elements using only a keyboard.
15	Pause, Stop, Hide	Automatically moving, blinking, or scrolling content that lasts longer than 5 seconds can be paused, stopped, or hidden by the user. Moving, blinking, or scrolling can be used to draw attention to or highlight content as long as it lasts less than 5 seconds. Automatically updating content (e.g., automatically redirecting or refreshing a page, a news ticker, AJAX updated field, a notification alert, etc.) can be paused, stopped, or hidden by the user or the user can manually control the timing of the updates.
16	Seizures	Do not design content in a way that is known to cause seizures.
17	Three Flashes or Below Threshold	No page content flashes more than 3 times per second.
18	Navigable	Provide ways to help users navigate, find content, and determine where they are
19	Bypass Blocks	A link is provided to skip navigation and other page elements that are repeated across web pages. If a page has a proper heading structure, this may be considered a sufficient technique instead of a "Skip to main content" link. Note that navigating by headings is not yet supported in all browsers. If a page uses frames and the frames are appropriately titled, this is a sufficient technique for bypassing individual frames.
20	Page Titled	The web page has a descriptive and informative page title.

21	Focus Order	The navigation order of links, form elements, etc. is logical and intuitive.
22	Headings and Labels	Page headings and labels for form and interactive controls are informative. Avoid duplicating heading (e.g., "More Details") or label text (e.g., "First Name") unless the structure provides adequate differentiation between them.
23	Focus Visible	It is visually apparent which page element has the current keyboard focus (i.e., as you tab through the page, you can see where you are).
24	Readable	Make text content readable and understandable
25	Language of Page	The language of the page is identified using the HTML lang attribute
26	Language of Parts	The language of page content that is in a different language is identified using the lang attribute.
27	Predictable	Make Web pages appear and operate in predictable ways.
28	On Input	When a user inputs information or interacts with a control, it does not result in a substantial change to the page, the spawning of a pop-up window, an additional change of keyboard focus, or any other change that could confuse or disorient the user unless the user is informed of the change ahead of time.
29	Compatible	Maximize compatibility with current and future user agents, including assistive technologies.
30	Parsing	Significant HTML/XHTML validation/parsing errors are avoided. In content implemented using markup languages, elements have complete start and end tags, elements are nested according to their specifications, elements do not contain duplicate attributes, and any IDs are unique, except where the specifications allow these features.
31	Name, Role, Value	Markup is used in a way that facilitates accessibility. This includes following the HTML/XHTML specifications and using forms, form labels, frame titles, etc. appropriately. For all user interface components, the name and role can be programmatically determined; states, properties, and values that can be set by the user can be programmatically set; and notification of changes to these items is available to user agents, including assistive technologies.
32	Audio-only and Video-only (Prerecorded)	A descriptive text transcript (including all relevant visual and auditory clues and indicators) is provided for non-live, web-based audio (audio podcasts, MP3 files, etc.). A text or audio description is provided for non-live, web-based video-only (e.g., video that has no audio track).

33	Captions (Prerecorded)	Synchronized captions are provided for non-live, web-based video (YouTube videos, etc.)
34	Captions (Live)	Synchronized captions are provided for all live multimedia that contains audio (audio-only broadcasts, web casts, video conferences, Flash animations, etc.)
35	Audio Description (Prerecorded)	Audio descriptions are provided for all video content NOTE: Only required if the video conveys content visually that is not available in the default audio track.
36	Sensory Characteristics	Instructions do not rely upon shape, size, or visual location (e.g., "Click the square icon to continue" or "Instructions are in the right-hand column"). Instructions do not rely upon sound (e.g., "A beeping sound indicates you may continue.").
37	Distinguishable	Make it easier for users to see and hear content including separating foreground from background.
38	Contrast (Minimum)	Text and images of text have a contrast ratio of at least 4.5:1. Large text - at least 18 point (typically 24px) or 14 point (typically 18.66px) bold has a contrast ratio of at least 3:1.
39	Enough Time	Provide users enough time to read and use content.
40	Timing Adjustable	If a page or application has a time limit, the user is given options to turn off, adjust, or extend that time limit. This is not a requirement for real-time events (e.g., an auction), where the time limit is absolutely required, or if the time limit is longer than 20 hours.
41	Link Purpose (In Context)	The purpose of each link (or form image button or image map hotspot) can be determined from the link text alone, or from the link text and its context (e.g., surrounding paragraph, list item, table cell, or table headers). Links (or form image buttons) with the same text that go to different locations are readily distinguishable.
42	Multiple Ways	Multiple ways are available to find other web pages on the site - at least two of: a list of related pages, table of contents, site map, site search, or list of all available web pages.
43	On Focus	When a page element receives focus, it does not result in a substantial change to the page, the spawning of a pop-up window, an additional change of keyboard focus, or any other change that could confuse or disorient the user.
44	Consistent Navigation	Navigation links that are repeated on web pages do not change order when navigating through the site.
45	Consistent Identification	Elements that have the same functionality across multiple web pages are consistently identified. For example, a search box at

		the top of the site should always be labeled the same way.
46	Input Assistance	Help users avoid and correct mistakes.
47	Error Identification	Required form elements or form elements that require a specific format, value, or length provide this information within the element's label. If utilized, form validation errors are presented in an efficient, intuitive, and accessible manner. The error is clearly identified, quick access to the problematic element is provided, and user is allowed to easily fix the error and resubmit the form.
48	Labels or Instructions	Sufficient labels, cues, and instructions for required interactive elements are provided via instructions, examples, properly positioned form labels, and/or fieldsets/legends.
49	Error Suggestion	If an input error is detected (via client-side or server-side validation), provide suggestions for fixing the input in a timely and accessible manner.
50	Error Prevention (Legal, Financial, Data)	If the user can change or delete legal, financial, or test data, the changes/deletions can be reversed, verified, or confirmed.
51	Visual Captcha	Alternative mode of authentication should be offered to inorder to be authenticated
52	Mandatory use of Unicode for regional language	Unicode facilitates assistive technology to access content.

12. Annexure VII – Cyber Security Requirements for Ludhiana Smart City Project

12.1 Cyber Security Framework

The Bidder shall develop Cyber Security Framework aimed at building a secure and resilient cyberspace for citizens and stakeholders of Smart City. 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. Framework shall cover smart city cyber security architecture with reference to the cyber security framework suggested by National Institute of Standards and Technology (NIST), CSA (Cloud Security Alliance) and ISO27001. Framework shall also comply with MoUD guidelines vide circular K- 1s016/6U2016-SC-1.

12.2 Cyber Security Policy

The Bidder shall ensure creation and implementation of Smart City Cyber Security Policy and related procedures in line with relevant international standards. The policy shall address security of hardware and software, along with the connectivity between the field device and the respective application software. The bidder shall ensure to develop and implement Standard Operating Procedures for smooth Operations and Maintenance of IT infrastructure.

12.3 Cyber Security Governance

1. The Bidder shall conduct Risk Assessment and prepare Risk Treatment Plan for the IT applications and infrastructure deployed in smart city ecosystem.
2. The Bidder shall facilitate management reporting in form of dashboard covering Risk Assessment results along with risk treatment plan and timeline to the smart city management.
3. The Bidder shall implement all the controls as identified during the Risk assessment and treatment plan as per the agreed timelines.

12.4 Cyber Security Organization Structure

1. The Bidder shall clearly define Organization structure for Smart City Cyber Security with skilled personnel and adequate representation from Senior Management. The organization structure shall also include the roles and responsibilities of personnel deployed for cyber security of smart city.
2. The smart city cyber security resources shall be deployed as part of the team during the complete contract period i.e. implementation and operation stage.

12.5 Smart City IT Asset Management

1. The Bidder shall utilize automated asset management tools to prepare the information asset register (IAR) for all IT assets deployed in the Smart city. The IAR shall capture criticality, rating, classification, owner and custodian of the Asset.

2. The Bidder shall develop and implement an appropriate set of procedures for information labeling and handling in accordance with the classification scheme proposed in the cyber security policy of smart city.

12.6 Physical & Environmental Security

1. The bidder shall implement and manage physical security of IT assets of smart city, which shall include, as a minimum: locks, alarms, surveillance equipment, sensors, access control systems (biometrics), etc. The bidder shall also design processes and procedures for same.
2. The Bidder shall ensure that all the equipment, information or software shall not be taken off-site without appropriate authorization.

12.7 Access Control

1. The Bidder shall ensure that users shall be provided single sign on functionality if required for the applications and solutions deployed in Smart City.
2. The smart city solution should support multiple authentication methods such as Username password, two factor authentication, digital certificate and biometric based authentication.
3. 2FA solution should be capable of being deployed on mobile devices deployed for smart city
4. Solution should have the capability to define access based on time of day, day of week or by group or user defined access.
5. The smart city solution should have the functionality to provide authentication based on the role.
6. Remote access to all smart city IT users shall be securely managed.
7. The smart city solution should be able to deploy and configure the approved password policy and should provide the feature to configure the logs.
8. The smart city solution should have the option of blocking multiple sessions for the user.
9. All smart city applications should support role based access control to enforce separation of duties.
10. The application deployed in smart city should display the last login status (successful/unsuccessful, time) to the user and should not store authentication credentials on client computers after a session terminates
11. All smart city solution should be compliant with Indian IT Act, 2000 and Amended IT Act, 2008

12.8 Security Analytics & Forensics

1. System should perform Full Packet Capture of network traffic with zero packet loss. Support the retrieval of relevant packets to a cyber security incident.
2. Support importing archived PCAP files for analysis. Support importing other structured and unstructured content for analysis.

3. Index all the data in the packets to simplify navigation across huge data. Enable search-driven data discovery of packet metadata and content for incident analysis
4. Enable search-driven data discovery of packet metadata AND content for incident analysis. And should allow for retracing the activities of an entity in a chronological order
5. Perform full reconstruction of assets transferred, accessed and transmitted. Should provide a visual representation of relationships between entities (IP, email ids, etc.)
6. The solution should highlight potentially malicious or suspicious content and allow for assigning security analysts to specific security incident investigations. The solution should have capability to integrate with 3rd party SIEM through rest API to have unified visibility.
7. The solution should support - classification from more than 2,800 protocols/applications(natively without writing any custom parsers) and thousands of descriptive, metadata attributes, including content types, file names, and more - for easy analysis and recall without writing any custom parsers
8. Solution should be sized for traffic rate of 1+Gbps
9. The solution must have feature for root cause analysis and while PCAP import the System is performing LIVE packet capture of the network.
10. Should provide Regeneration and Playback functionality: Ability to create shadow networks. Regeneration and Playback: Point and click to instantly regenerate traffic (at configurable speeds) to a chosen NIC on a shadow network for further analysis in 3rd party systems. Without interruption of regular services.
11. Anomaly Detection – find anomalous traffic patterns occurring in your network. Should have ability to filter, view timeline, or readily access Email and IM artifacts in one pane of glass
12. Should be an on-premise appliance-based solution with capability to do packet capture, storage, protocol dissection.
13. Should support 3rd Party Threat Feed integration – add live-feeds, like Snort, quickly and easily. Reputation Services provide added value and threat intelligence. Should be able to remediate Endpoints from the same console
14. Root Cause Explorer Features - Automates tracing of HTTP referrer chains that can significantly reduce time to search for related preceding sessions.
15. Should be able to provide complete packet-by-packet details pertaining to one or more session of interest including voice/video replay, page reconstruction, image views, artifact & raw packet extractions.
16. Security Analytics should be proposed with required SSL visibility solution to enable meticulous network forensics and monitoring across all network traffic, thousands of applications, dozens of file transports, all flows, and all packets—including encrypted traffic.
17. Should provide total visibility into network traffic with actionable intelligence so that department can quickly shut down exposure and mitigate ongoing risk. Should provide:
    a. Detailed insights from all forensic captures
    b. Establish policies to selectively decrypt SSL traffic

c. Share encrypted traffic insight with your security applications

18. Solution must support automatic visibility and interpretation of SSL decrypted traffic regardless of port or protocol. SSL decryption should be provided through the dedicated purpose built appliance based. There has to be integration with SSL decryption and security analytics solution.
19. The provided solution for SSL decryption must support 78+ Ciphers and TLS 1.3.
20. Should include Directly Attached Storage with minimum 40TB capacity and should be scalable to 240 TB.
21. Should have minimum 2 x 1 GbE , 2 x 10GbE interfaces and 256GB RAM.
22. The provided solution must be running in minimum 3+ Indian Government/ PSU organizations and due certification from the client authorities must be submitted.

12.9 Web Application Firewall (WAF) with Reverse Proxy

Web Application Firewall must support the following aspects

1. OWASP Top 10
2. Cross Site Scripting
3. SQL Injection
4. Cross Site Request Forgery
5. Session Hijacking
6. Third-party scanner integration (virtual patching)
7. XML and JSON protocol conformance
8. Malware detection
9. Virtual patching
10. Protocol validation
11. Brute force protection
12. Custom error message and error code handling
13. DoS prevention
14. Advanced correlation protection using multiple security elements
15. Data leak prevention
16. Web Defacement Protection
17. The WAF must be deployable in full reverse proxy mode as well as transparent bridge mode, where all traffic is re- directed to flow through the WAF.
18. The appliance must support Web server and application signatures (black list) as per requirement.
19. It must support reputation and geolocation feature and must be HTTP RFC compliant.

12.10 Proposed Security Solution Features

The proposed security solution must dupport following features

1. Layer 7 server load balancing
2. URL Rewriting
3. HTTPS/SSL Offloading
4. HTTP Compression
5. Caching
6. Authetication Methods
    a. Active and passive authentication
    b. LDAP support and any other available
    c. SSL client certificate support
7. Management feature
    a. Web user interface
    b. Command line interface
    c. Central management for multiple devices
    d. REST API
    e. Centralized logging and reporting
8. High Availability with Config-sync for syncing across multiple active appliances
9. Must have Ability to save resources of the web servers by serving cached static content directly
10. Must support advance signature less engine
11. Must provide HTML rewriting functionality
12. It should be possible to add, delete and edit request and response headers, translate URL spaces, rewrite or redirect the URL in the request, and rewrite the response body.
13. Regular expression like syntax should be available for the required text manipulations.
14. Should allow enforcing the following protocol related restrictions on the requests and these should be specifiable on an individual URL basis
    a. HTTP method length
    b. Request line length
    c. URI length
    d. Query string length
    e. Protocol length
    f. Header name, value, and number
    g. Request body length
    h. Cookie name, value and number.
    i. Parameter name, value and number
    j. Max length (per file) and number for uploaded files (via POST)
15. Should support a negative security model where attacks are detected by performing a regular expression match against incoming URL requests.
16. Should be able to detect an block requests coming from anonymous proxies
17. Must be able to handle IPv4 and IPv6 traffic

18. Client certificates should be applicable granularly at a URL level
19. OCSP and CRL support for should be available for client certificate validation
20. Anti-virus signatures should be automatically updateable to the latest versions
21. SOC should be able to manage logs from all routers, switches, servers, hips, firewalls, ips etc in the data centre.
22. SOC must provide log correlation and data enrichment using global threat intelligence.
23. Solution should be SSAE 16 Type II, ISO27001 and PCI certified.
24. SOC should provide a web interface portal to the users to manage the services.
25. Security solution should have artificial intelligence to provide zero-day protection and stop new and unknown threats by monitoring more than 1000+ file behaviors while they execute in real-time to determine file risk.
26. Security solution should provide protection for critical systems by only allowing whitelisted applications.
27. Security solution should have the feature to investigate whether endpoint is out of compliance and should accomplish remediation, either via self-contained capabilities or integration with external resources.
28. Should have incident investigation and response utilizing the integrated capabilities.
29. Solution should manage single license for all available operating systems from a single system / server.
30. Should detect malware that evades detection by using polymorphic custom packers by unpacking in a light weight virtual environment with no performance over-head.
31. If the security solution detects a network attack, solution must automatically activate active response to block all communication to and from the attacking computer.
32. Solution must have a layer of protection that enables organization to go on the offensive and lure attackers out of hiding using deception and reveal attacker intent and tactics via early visibility, so that the information can be used to enhance security posture.
33. Security solution's EDR should be able expose advanced attacks with precision machine learning, behavioral analytics and threat intelligence minimizing false positives.

12.11 Communications and Operations Management

1. Bidders must ensure that the IT systems in the smart city infrastructure are open, scalable and interoperable. The deployed systems must operate within 4 layers – Sensory layer, communication layer, data layer and application layer adhering to relevant security controls as mandated by the MoUD guidelines.
2. Bidders shall ensure that all the interfaces between IoT devices, field sensors, device applications and storage deployed in smart city are encrypted using appropriate protocols, algorithm and key pairs.
3. All transport link communication must be encrypted and sensitive data both in rest and transit is to be secured using encryption.

4. Bidders must ensure that all the changes made to the smart city infrastructure incl. of IoT field devices, sensors and related applications should be tracked and recorded in order to enable security monitoring of the infrastructure. The maintained logs should be systematically collated, enabling the access of critical information as per date, fortnight, month, quarter, year etc.
5. Bidders should ensure that separate environments are maintained for production, test and development for smart city infrastructure and solutions to reduce the risks of unauthorized access or changes.
6. Bidders must ensure that smart city IT systems are designed in such a way that only authenticated users have access to the smart city database. Also, the provision of access has to be routed only through designated applications.
7. Bidders must ensure that sensitive data is stored in the smart city database in an encrypted format thereby curtailing the database administrator from reading or modifying the stored sensitive data.
8. Bidders must ensure that the smart city architecture should include a VPN solution enabling designated users to access necessary applications and functions from remote applications.
9. Bidders must enable for the maintenance of an audit trail to record all the administrator, user level activities including the failed attempts thereby enabling a robust high level security monitoring of the smart city security infrastructure.
10. Bidders must ensure that the smart city components – Network elements, Operating system, Applications etc. are in sync and adhere to a singular master clock. Thereby ensuring an appropriate logging/ time stamping of incidents and bolstering smooth operation of the smart city.
11. Bidders must ensure that adequate security controls are deployed against the tampering of log information and unauthorized access to the smart city infrastructure such as the data center, IoT device control room etc.
12. Bidders must ensure that platforms hosted in the central data center support multi-tenancy with adequate authentication and role based access. This can be achieved by utilizing Authentication and privilege management technology thereby controlling the access of data as per user privileges.
13. Bidders must ensure that the smart city architecture accounts for latency issues for the flow of data between devices. Suitable protocols should be utilized to minimize data flow latency upon management of heterogeneous data.
14. Bidders must strictly make sure that the communication between IoT field devices and their respective management applications happens only over a data layer (digital platform). Thereby enabling this designated layer to be the one true source of data abstraction, normalization and correlation.

15. Bidders must ensure that the smart city IT infrastructure including the Wi-Fi network adheres to relevant and applicable security standards and protocols. Also, bidders must make sure that the Application Program Interfaces (APIs) are published and the IT systems run on standard protocols.
16. Bidders must ensure that the smart city architecture end-to-end has adequate security controls to enforce safety, privacy and integrity of confidential data. Necessary controls must be deployed to protect the integrity of data flowing into the control systems and other critical infrastructure.
17. Bidders must enable for wireless/ broadband architecture used in the smart city infrastructure to interface with other/citywide wireless networks thereby enabling interoperability.
18. Bidders must ensure that IoT field devices and sensory equipment operating within the smart city periphery connect only to authorize wireless networks. Secure Wi-Fi guidelines as prescribed by the Department of Telecom must be followed.
19. Bidders must make sure that the wireless layer of the smart city network is appropriately segmented, bifurcating the network into various trusted zones. Thereby segregating public and utility networks via VPN (Virtual private networks), ensuring that the traffic from internet users is not routed into sensor networks and vice versa.
20. Bidders must enable for the authentication of the sensory equipment during the provisioning of the sensors and connection into the smart city infrastructure.
21. Bidders must ensure that the data aggregators used for enabling the interoperability between field IoT devices and sensors functioning on different protocols incorporate appropriate authentication and encryption at the aggregator gateway when field devices are not capable of authenticating /encrypting critical information.
22. Bidders must ensure that the IoT field devices and sensory equipment deployed in smart city periphery must not have a physical interface for administration. System and Network monitoring should be only performed remotely thereby ensuring local cyber-attacks/ tampering of field devices is curtailed.
23. Bidders must ensure appropriate network segregation. The smart city data center must be systematically segmented into multiple zones. Each zone must have a dedicated functionality. IoT field devices and sensory equipment must be connected to a completely separate network isolated from public networks and other private networks.
24. Bidders must make sure that the internet facing segment of the data center must incorporate a DMZ (Demilitarized zone), where customer application servers would be located. Predefined ports must be assigned for enabling the communication between the customer application servers and utility application servers to facilitate the access/transfer of data.

25. Bidders must ensure that Smart city data centers are well equipped with adequate security controls to protect the confidentiality, integrity and accessibility of critical data. The center should consider including cyber security systems such as firewalls, Intrusion detection & Intrusion prevention systems, Web Application Firewalls, Behavioral analysis systems for anomaly detection, Correlation engine, Denial of Service prevention device, Advanced Persistent Threat notification mechanism, Federated identity, access management system etc.
26. Bidders must ensure that the Smart city cyber security infrastructure incorporates high level security and monitoring controls such as SIEM (Security Information and Event Management) tools on all networks, field devices and sensors to identify malicious traffic.
27. Bidders must ensure all smart city applications must be hosted within India and must undergo static and dynamic security testing before deployment. Also, the applications must be periodically (at least once a year) tested for adequate security control.
28. Bidders must ensure that the proposed smart city architecture provides for:
    a. Automatic and secure firmware updates
    b. Device logging and auditing capabilities
    c. Vendor self-certification for non-existence of backdoors, undocumented and hard coded accounts.
29. Bidders must ensure that all the information on security incidents is regularly shared with Indian Computer Emergency Response Team (CERT-ln) and NCIIPC (National Critical Information Infrastructure Protection Centre) and their help is sought for appropriate mitigation and recovery from the security incidents.
30. Bidders shall ensure that Data encryption at rest shall be implemented using departments managed keys, which are not stored in the cloud.
31. The bidder shall setup Cyber Security Continuous Monitoring process to monitor - physical environment, External service provider activity etc. to detect potential cyber security incidents.

12.12 Information Systems Acquisition, Development and Maintenance

1. The Bidder shall prepare the detailed technical security requirement as part of the 'Software Requirement Specification' document with secure coding guidelines for development of applications for smart city.
2. The Bidder shall incorporate validation checks into smart city applications to detect any corruption of information through processing errors or deliberate acts.
3. The Bidder shall obtain information about technical vulnerabilities of information systems being used in smart city, evaluate the exposure to such vulnerabilities, and take appropriate measures to address the associated risk.
4. The bidder shall implement maintenance and repair process of smart city IT assets in timely manner, with approved and controlled tools.

12.13 Business Continuity Planning and Disaster Recovery

1. The Bidder shall implement and operate Disaster Recovery site for the Smart city infrastructure and related IT & OT applications. IT & OT applications and processes should be supported from the disaster recovery site.
2. The Bidder shall define Business Continuity and Disaster Recovery plan and will perform the testing on a half yearly basis

12.14 Information Security Audits

The bidder shall ensure Information security audits of the smart city infrastructure and related applications by a CERT-In empaneled vendor. VA/PT (Vulnerability assessment and Penetration Testing) activities, audits and application security testing must be carried out on twice-a-year basis ensuring optimal operation and security of the smart city infrastructure and applications. Teams carrying out the audit exercise must be different from the implementation teams. Systematic actionable need to be derived post audits and necessary changes need to be made periodically.

12.15 Security Operations Center

The bidder shall set up Security Operations Centre to ensure continuous monitoring and manage all kinds of cyber security operations related to smart city such as Incident Management, Logging and Monitoring, Anti-virus Management, Threat Intelligence Support, Secure Technology Disposal and other cyber security support activities to ensure secured smart city ecosystem.

12.16 Awareness Training

The bidder shall deploy appropriate resources to support periodic awareness training based on latest standards of ISMS. The trainings must focus on educating relevant employees (including privileged users, third party, senior management etc.) on necessary security practices and processes to be followed in order to maintain the Confidentiality, Integrity and Availability of critical data.

12.17 Security Controls for Cloud Services

The security controls for creating and managing cloud services shall comply with the following guidelines.

Empanelment of Cloud Service Offerings CSPs facilities/services shall be compliant with regulative directives and industry best practices. The SLA shall be based on the guidelines issued by Government Departments on contractual terms related to Cloud Services (MeitY guideline dated 31/03/17). The security controls should include the following:

a. The CSP should be empaneled by MeitY for providing cloud services. The CSPs facilities/services shall be certified to be compliant to the following standards: ISO 27001, ISO 27017, ISO 27018, ISO 20000-9, ISO/IEC 20000-1 & PCI DSS.

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

setup / recognized by Government of India from time to time and notified to the CSP/Service Providers by MeitY as a mandatory standard.

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.

d. Incident Management shall be managed by CSP / third party.

e. Periodic secure code review shall be performed for cloud applications.

f. Data encryption at rest / transit depending on sensitivity of data shall be implemented using departments managed keys, which are not stored on the cloud.

g. The CSP will undertake to treat information passed on to them as classified. Such Information will not be communicated / published / advertised by the CSP to any person/organization without the express permission of the Department.

h. CSP shall inform all security breach incidents to Smart City management on real time.

i. CSP shall ensure data confidentiality and mention Sub-contractual risk shall be covered by CSP.

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

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

l. CSP must ensure location of all data related to smart cities in India only.

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

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

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

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

q. Change-management process (e.g., changes such as updates or new services) must be defined.

r. Appropriate segregation of Virtual Private Cloud (VPC) security rules defined as part of firewall to restrict access, Role based access management, Logging and monitoring shall be ensured.

s. 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.

t. Digital Certificate shall be implemented for secure access.

u. 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.

v. 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.

w. For SLAs to be used to steer the behavior of a cloud services provider, imposition of financial penalties is to be incorporated.

x. Monitor Vendor Service level agreement for annual end-to-end service availability of 99.999 percent. The end to end service agreement should be in place for minimum period of six years form the date of operations of the system